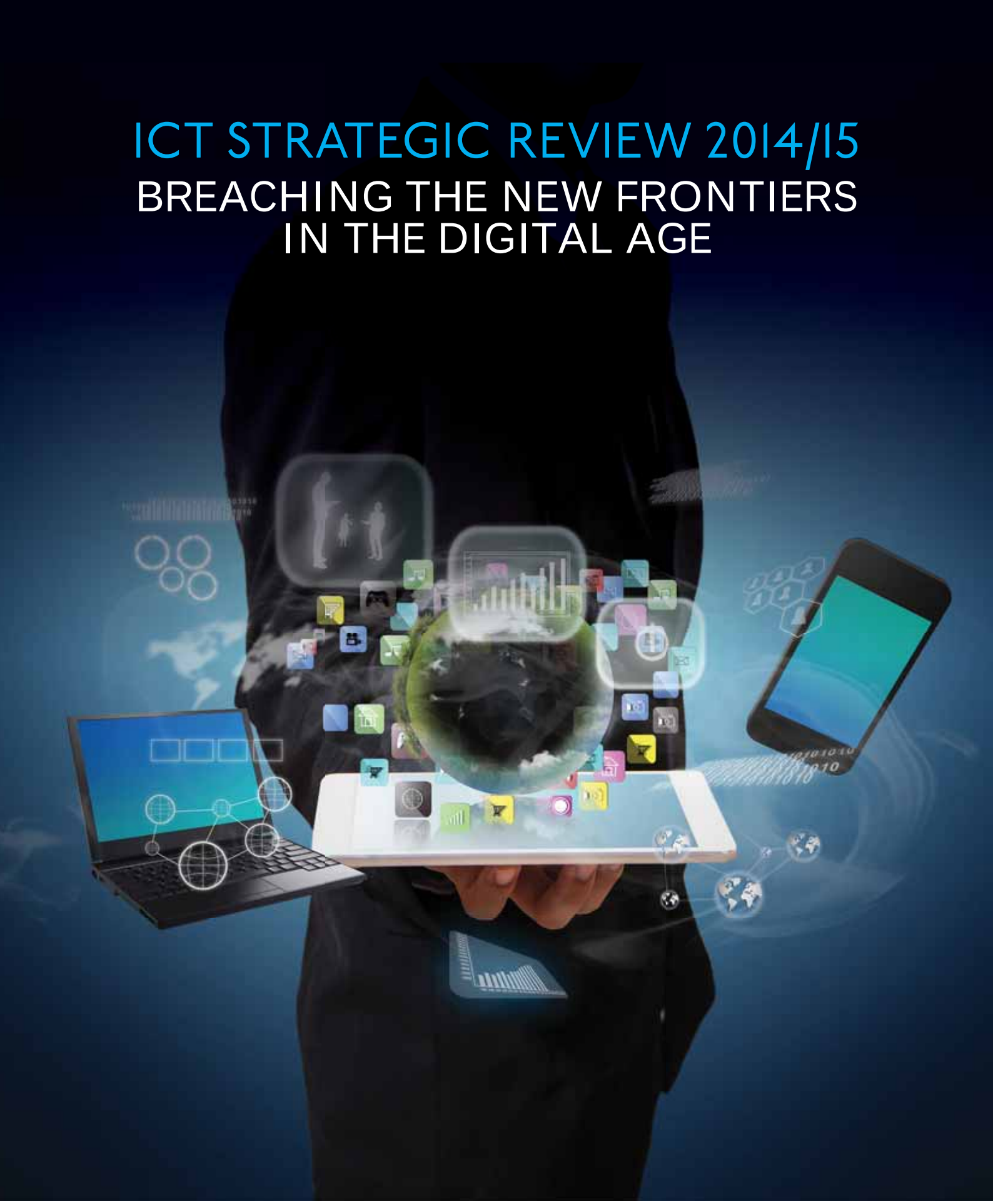
ICT STRATEGIC REVIEW 2014/15

BREACHING THE NEW FRONTIERS IN THE DIGITAL AGE



PIKOM

KKMM
KEMENTERIAN KOMUNIKASI
DAN MULTIMEDIA MALAYSIA

PUBLISHED BY:

Aras 37, Lot 4G9, Persiaran Perdana, Precint 4,Central
Administration of The Federal Government
62100 Putrajaya, Malaysia

T: (603) 8911 5114
F: (603)8911 5124
e: webmaster@kpkk.gov.my
w: www.kkmm.gov.my

E1, Empire Damansara
No 2, Jalan PJU 8/8A Damansara Perdana
47820 Petaling Jaya, Selangor Darul Ehsan

T: (603) 4065 0078
F: (603) 4065 0079
e: info@pikom.my
w: www.pikom.my

PIKOM, the National ICT Association of Malaysia, is a not-for-profit organisation. It is the largest association representing information and communications technology (ICT) players in Malaysia. Since its inception in 1986, PIKOM has come of age as the voice of the ICT industry. It has become an ICT referral centre for government and industry players, as well as international organisations. In this regard, PIKOM takes on the responsibility to publish ICT-relevant information in a periodic manner.

ISSN No:

EDITOR-IN-CHIEF:
Ramachandran Ramasamy
Head of Policy, Capability and Research, PIKOM

DESIGN, PRODUCTION AND PRINTING:
mjlaikc infoworks

RELEASE DATE
September, 2014

Breaching the New Frontiers in the Digital Age

- A C-level event designed to discuss the industry's latest thought leadership, trends and insights to spur innovation, adoption of new technologies and new business models in elevating the ICT growth in Malaysia
- A platform to showcase the industry's best practices and successes in using ICT for business growth, transformation and nation building
- Showcase the diversity of the ICT industry's talents and potentials in the changing business landscape
- A meeting place for industry leaders to network with industry players, share views, best practices and advice on how to stay relevant in the industry that's transforming continuously

An event by

PIKOM

Strategic Partner

DIGITAL MALAYSIA

MSC MALAYSIA

MDEC Driving Transformation

Gold Partners

IBM

FUSIONEX experience.excellence

Microsoft

TM

vmware

worldline e-payment services

Silver Partner

JUNIPER NETWORKS

Media Partners

DSA

DNA DIGITAL NEWS ASIA

Bronze Partners

EPSON EXCEED YOUR VISION

HITACHI Inspire the Next Hitachi Sunway Information Systems

PWS

Supporting Partners

hp

TATA CONSULTANCY SERVICES

CONTENT

FOREWORD BY
THE MINISTER OF COMMUNICATION & MULTIMEDIA

DATO' SRI AHMAD SHABERY CHEEK

On behalf of the Ministry, I would like to congratulate PIKOM's effort in realising the sixth edition of its ICT Strategic Review Series for 2014/2015. Over the years this publication has been very well received by the industry and the contents of the report have becoming richer and aligned with the latest development and global trend of the ICT industry. I am indeed delighted that the Ministry of Communication and Multimedia (MCMM) is a partner in this endeavour.

The theme, "Breaching the Technology Frontiers in the Digital Era" is timely especially when our nation is now at the advance stage of realising our vision to be a developed nation by 2020; and ICT and digital technology being the enabler is a critical platform for this journey. However, the boundary beyond the frontiers may also come with inherent risks as innovations and opportunities are not without threats, especially when borders are becoming more open to facilitate the free flow of information, goods, services and people. Hence, a good presence of mind, alertness, responsiveness as well as prudence are essential for community and business to ensure continuity and relevance; including the appropriate law and regulations.

The Malaysian Government recognises such technological and business evolution, if not revolution. Adequate seeding of thoughts and early planning are crucial, before ideas and concepts can be materialized into actionable programmes. Therefore, we at MCMM, welcome any collaborative effort with both the industry and academia to ensure that Malaysia capitalise on the opportunities and reap the full benefits when the frontiers of the digital era is 'breached'.

On that note, I congratulate PIKOM once again for this effort and I assure you that MCMM will continue its support in realising such thought leadership publication.

DATO' SRI AHMAD SHABERY CHEEK

MESSAGE BY PIKOM CHAIRMAN

CHEAH KOK HOONG

On the surface, 2014 may seem to be a calamitous year on both the local as well as global fronts. Yet, amid the maelstrom of tragic incidents, Malaysians have remained resilient and resolute in moving forward towards our vision of developed nation status by 2020. Indeed, we stand at a crossroads in which our ability to capitalise on opportunities offered by the digital era will determine success or failure in this endeavour.

On this score, I am pleased to note that ICT Services is poised to fuel the growth of the key Services Sector and expand the latter's share of the national economy from 55% in 2013 to a projected 70% by 2020. Growth in the Services Sector is deemed as critical in realising the vision of becoming a high income nation.

As Chairman of PIKOM, I am proud to see the successful completion of the ICT Strategic Review 2014/15 publication, the sixth of this series. This time around, the collection of articles is appropriately centred on the theme "Breaching the Technology Frontiers in the Digital Era". The theme is timely in moving businesses forward to take advantage of the proliferation of ICTs or digital technologies in their various shapes and shades. On that note, I thank all the contributors from industry and academia who have given their unremitting support in making this publication a reality once again.

For a long while now, the impact of digital technologies have cut across all social groups and sectors, irrespective of time, geography, traditions and cultures as witnessed in the ubiquity and pervasiveness of Facebook, Twitter, LinkedIn et cetera. Before businesses and individuals can fully absorb the impact of social web technologies, new advancements and the digitisation of life processes such as the internet of things; wearable technology; miniaturisation of devices replacing desktops, laptops and tablets; information of things driving big data analytics to the next business level; cloud computing customisation for small and medium enterprises; ICT-packaged as services; mobility increasing business agility and demands of YZ generations seeking buy your own devices (BYOD); and tele-working practices; are on the verge of disrupting business continuity and relevance.

As reflected in the theme, it is prudent that we review and realign the way we work, learn, play, perform transactions, build relationships and develop networks. Indeed, regional integration and globalisation processes are taking place at an unprecedented rate, creating plethora of new business opportunities.

I would like to take this opportunity to thank the Ministry of Communication and Multimedia (MCMM), particularly YB Dato' Sri Ahmad Shabery Cheek for his support of PIKOM and its activities. To the readers of this publication, I trust that you will find in this edition many of the queries about moving forward in the digital era.

EXECUTIVE SUMMARY

BREACHING THE NEW FRONTIERS IN THE DIGITAL AGE

WOON TAI HAI
PIKOM Research Committee Chairman

The rate at which digital technologies is evolving requires that we constantly take stock of what is over the horizon so as to put in place the necessary measures to adapt and adopt the new in place of the old. Yet to stay abreast of or better still on top of the constantly shifting parameters impacted by digital technologies, we are forced to engage in predictive exercises not unlike the frivolous practice of crystal-balling. Naturally, this is by no means an exact science. Looking into a digital future, where trends come and go in timeframes measured by a rapidly declining life cycle, comes with its own risks and challenges. That said, this is an essential task for us all as digital citizens, businesses, governments and other entities. After all, every party fear the spectre of obsolescence and irrelevance. For this reason, we have appropriately chosen "Breaching the New Frontiers in the Digital Age" as this year's theme. The discourse and discussion that follows in this publication attempt to build a big picture of what is in store for Malaysia and the world in the years to come even as digital technologies continue to change and transform our way of living and doing business, as it has done since its first iteration.

The advent of commercial Internet three decades ago marked the beginning of the digital age. Since then, the digital realm has crossed over several points of inflexion in becoming the defining phenomenon of our time. Indeed, the ubiquity and pervasiveness of all things digital have suffused all aspects of the world we know today. In essence, digital has become as much a way of life as it is an enabler of our lives. It can be considered an understatement to say that the growth and spread of the digital realm have been phenomenal, revolutionary and unprecedented in human history.

This surge continues today with even more technological advancements and innovation. New shapes and shades of digitization are rapidly coming into the limelight on a breathtakingly rapid rate. As a consequence, mainstream policy institutions are shifting their focus from digital divide to digital opportunity.

The new age opportunities come in varied form. Miniaturization of devices at affordable prices and increased computing power are replacing the PC and desktops that dominated office and individual use. Digital mobility is certainly not an emerging trend any more but part of our lives. Mobile commerce is also becoming more prevalent and prominent than e-commerce for its convenience and ease of use and more pertinently the business opportunities it has created for all of us.

The biggest phenomenon that has 'stormed' the digital era in recent years is the emergence of Big Data Analytics (BDA). It has taken centre stage by becoming the method to cull business, market and policy intelligence, leveraging on real time data arising from internal and external sources. It is pertinent to note that this was not possible technologically and administratively under the preceding business intelligence analytics models.

The scope and coverage of BDA is becoming wider with the Internet of Things (IoT) driving information of things. With Tthe recent announcement that the big data policy framework for Malaysia will be ready for

presentation in the third quarter to the Prime Minister (DNA Sep 10, 2014) is certainly timely and strategic, more so and since the country aspires to be ambition to make the country a regional hub for big data and analytics hub for the region; is certainly strategic and timely. The Ggovernment has realised that the aspiration aspiring to be a fully-developed nation and leverageding on a developed digital economy will also have to rely on the effectiveness of the deployment andcum adoption of data and analytics.

Cloud computing models are now preferred over proprietary computing systems for itheirts ability to drive down costs and achieve improvements in operational efficiency and efficacy. These attributes of cloud technologies have made it tenable for the computerisation of small and medium-sized industries. As most will be aware, that the common deployment models that CIO and C-level decisions maker these days are seriously considering are Public, Private, Community and Hybrid albeit the continuing concern on the security aspect of these models. Cloud computing service models such as SaaS, PaaS and IaaS and their adoptions are also making fast headway into the industry. Suffice to say, the success of these models is not merely based on the fact that they are the flavours of the month. Obviously it will still depend largely on the effectiveness of implementing these models and whether the models fit a specific need or situation. Deployment models as Public, Private, Community and Hybrid becoming a common language used by CIOs and C-level decision makers; and cloud computing service models such as SaaS, PaaS and IaaS become a reality today. The future is all about cloud as the overarching technology that fuels BDA, social technologies and digital phenomena. Although still small, Malaysian companies and other organizations are increasingly capitalising on cloud computing as a means reduce operational costs as well as to focus on their core business activities.

Social technology applications, by its natural progression, has evolved to provide cheaper, faster and wider means for advertisement, marketing and branding that were once the exclusive domain of large corporations.

Social webs are migrating into semantic webs to create new frontiers in social computing and content management activities by connecting data, concepts, applications and people as well as associated procedures and processes. Even now, Malaysian companies are turning to social technologies to add value to their offerings in the form of personalize products and services as well as to reach out to a broader customer base.

With the advent of all these digital trends, practices and expectations, Ttraditional human resource practitioners are increasingly feeling the pressure from Generation Z or Millennials for buy your own device (BYOD) and teleworking practices.

Under such scenarios, the capability of companies is critical in developing strategic leadership, government relations, institutional support and security & risk, quality and process, knowledge management, innovation process, market market globalization, human capital and working motivation. However, the readiness of our present and future workforce in facing these constantly-changing digital trends and practices remains a matter of deep concern. Going forward, the next generation worker or self-employed entrepreneur must depend on learning agility as the base to adapt to the sweeping changes brought on by digital technology. This is an issue our institutions of learning as well as the academia-industry partnership need to pay greater attention on.

Are we breaching the New Frontiers in the Digital Age? The boundaries are moving so fast and often blurred, hence to realistically answer this question is a matter of perspective and where are youdepends on where you are at a certain point in time. Suffice to say, all organisations have to take into cognizance this fluid boundary of the digital era and to seize opportunities to increase their economic values, improve efficiencies, increase satisfactions of their talent workers or inculcate higher level of innovations.

CHAPTER ONE
MALAYSIAN ECONOMIC AND INFORMATION COMMUNICATIONS TECHNOLOGY (ICT) OUTLOOK

PIKOM forecasts that the Malaysian economy will register at least 5.2% growth in 2014, mainly as a result of healthy growth in domestic demand, sound macro-economic conditions and prudent financial management as well as political stability. All economic sectors except mining and quarrying, have been on the upward trajectory over the past three years and such growth is poised to continue this year. Despite fluctuations and challenges, the economies of China, ASEAN and India – economic regions with which Malaysia has long and established trade and cultural ties - remain on the high side and are poised to provide the requisite impetus to the Malaysian economy.

A low unemployment rate and a Malaysian currency gaining strength provide favourable macro-economic conditions for export trade and investment. However, the anticipated increase in the base lending rate due to the upward movement of the overnight policy rate by Central Bank, the subsidy rationalization, introduction of Goods and Services Tax (GST) in April 2015, and fiscal deficit reduction measures, are forecasted to raise the inflation rate to 3.6% by the end of 2014 in comparison with the average 2.0% the year before. Nonetheless, the ICT Services sub-sector is expected to register a double digit growth rate of 13% in 2014, mainly attributed to expected growth in the provision of computer services which are in turn fuelled by increased uptake of cloud computing, big data analytics, mobile computing and Internet of things as well as the rise in the export and import of ICT services.

Despite the predicted good news for this year, the ICT Sector continues to be plagued by challenges such as a declining supply of ICT graduates, quality of ICT graduates not meeting industry demands, the trend of qualified and experienced ones migrating overseas in search of greener pastures, job hopping, low level innovation and R&D, patent registration and new commercialization activities. These challenges are likely to become more acute with ASEAN 2015 when there will not only be a greater flow of goods and services, but also people across borders.

CHAPTER 2:
INTERNET OF THINGS (IoT) DRIVE INFORMATION OF THINGS (IOT): MOBILITY, SECURITY, ANALYTICS AND TALENT PERSPECTIVES

The phrase "Internet of Things (IoT) driving information of Things (IOT)" may sound like a new buzzword in the ICT industry, but it is becoming a rapidly-emerging reality for the business sector. Beginning with the largely-static World Wide Web (WWW) in the early nineties, web technologies have subsequently evolved into social webs by providing connectivity and networking capabilities for people and institutions, with sites proliferated by animated content and videos as in the case of Facebook, Twitter, Instagram, You Tube, blogs et cetera. Incrementally, web technologies are now migrating into the semantics environment, in which embedded data and information are converted into useful knowledge and intelligence.

More so, business intelligence is made available in a pervasive and ubiquitous manner as well as in real time even as miniaturization of devices, trends, Internet of Things and wearable technology are being driven with the support of cloud computing and big data analytics. Indeed, such an ambience intelligence phenomenon is fast gaining the attention of businesses, thus providing a new direction in enhancing customer and business aspirations as well as the bottom line. In fact, Gartner has predicted that there will be nearly 26 billion devices on the Internet of Things by 2020 and importantly, they will be wirelessly connected, likely to give rise to a plethora of business opportunities

either as service providers or users of new technology and practices. Such a phenomenon may still be in its infancy but is likely to be unavoidable for business continuity and relevance. Taking cognizance of this trend, the paper points out that future businesses need to pay special attention to a Mobility, Security, Analytics and Talents (MSAT) Framework that is deemed critical to enhance business agility, pervasiveness and ubiquity as well as ambience intelligence.

CHAPTER 3
LEVERAGING UPON PRIVATE SECTOR BIG DATA: INFORMATION COMMUNICATIONS TECHNOLOGY (ICT) PROFESSIONALS SALARY PERSPECTIVE

This chapter expounds on the collaboration between industry association and the online job recruitment service providers, producing the income profile of information communications technology (ICT) professionals in Malaysia, but viewing the whole exercise as prospective big data analytics (BDA). Currently, the salary compilation activity leverages on the profiles of millions of job registrants in the web-based database of Jobstreet.com and web published information of PayScale.com. The typical data published includes average salary of ICT professionals by industry, job category, employment size and geographical locations; top paying ICT jobs; hot ICT jobs in demand; job sentiment index; and median data for various types of job functions as well as regional data for benchmarking. Being based on a structured database built around a rectangular array of records, in a true sense, the current salary compilation exercise may not fully meet the BDA requirements.

As per current industry understanding, contemporary BDA is characterized by 5 Vs, namely volume depicting amount of data; velocity indicating the rate and frequency at which data is created, processed, analysed and disseminated; variety entailing the complexity of data types and data sources as well as integration of structured, unstructured and semi-structured data streams; veracity dimensions deals with data validity, reliability, security and quality; and values aimed at closing the gap between data and business needs and customer aspirations. The paper notes that the on-going salary compilation activity may not have attained the full-fledged BDA status. However, the chapter acknowledges that the current salary compilation exercise has laid the requisite foundation to move in the envisaged BDA direction if structured database is integrated with other unstructured or semi-structured databases within Jobstreet.com or external records like PIKOM Membership database; by changing frequency of reporting from once a year to real-time reporting to PIKOM; and by culling not only business intelligence but also public policy relevance. It may sound ambitious but doable if the existing collaboration between the industry association and online job seekers service providers can be enhanced.

CHAPTER 4:
COGNIZANT COMPUTING: THE NEXT ERA OF COMPUTING IS PERSONALIZED

The term cognizant computing is defined as the application of contextual information to computing in order to permit actions to be taken according to pre-defined rules - meaning the computer is aware of your context and your activities and can take actions on your behalf. Early iterations of cognizant computing include Apple Siri, Microsoft Cortana and Google Now. Cognizant computing also heralds the next evolution of the personal cloud as consumers switch their focus away from devices to services. IT research and advisory firm Gartner predicts that by next year (2015) the majority of the world's largest companies will be using Cognizant Computing to fundamentally change the way they interact with their customers.

By amalgamating and analysing data in the cloud from many sources (including apps, smartphones and wearable devices), cognizant computing provides contextual insights into how people behave — what they watch, do and buy, who they meet, and where these activities take place. Such analyses provide opportunities for companies to increase the lifetime value of their increasingly fickle customers, improve customer care, boost their sales channels, and change the customer relationship by making it more personal and relevant and more so embark innovation and create new business opportunities.

CHAPTER 5:
DIGITAL REINVENTION: PREPARING FOR A VERY DIFFERENT TOMORROW

This chapter by IBM draws attention to the fact that the individual-centred economy is already here. The newest digital technologies – among them social media, mobility, analytics and cloud – keep changing how people, businesses and governments interact. These digital forces enable unprecedented levels of connectedness and so the world is already investing in consumer-centricity. However, these new technologies are still in their infancy. The transformation that is already underway will soon intensify, resulting in a paradigm shift from customer-centricity toward an everyone-to-everyone (E2E) economy. The implication for value creation and allocation will be profound. New IBM research shows that many organizations are still not ready to navigate the E2E environment.

To prepare for the radical disruption ahead, companies need to act now to create experiences and business models that are orchestrated, symbiotic, contextual and cognitive. Today's uber-connected, empowered individuals seek 24/7 access and organizational transparency. They want to exert greater personal influence over organizations and participate in more digital activities as they conduct their daily lives. In the IBM Global C-suite Study, 55 percent of 4,183 C-suite executives report that consumers have the most influence on business strategy, second only to the C-suite itself.1 Looking ahead, 63 percent of the leaders we surveyed in this 2013 IBM Digital Reinvention Study expect consumers to gain even more power and influence over their businesses.

CHAPTER 6
MALAYSIA ICT 2014 TOP 10 PREDICTIONS: FLOODED WITH TECHNOLOGY BUT ANCHORED BY THE 3RD PLATFORM

In this chapter, IDC outlines the top 10 predictions for 2014 based on an understanding of local sentiments surrounding the market, business and technology trends, and with reference to the four pillars of transformation namely cloud, Big Data and analytics, social, and mobile. The highlights include: IT spending is forecasted to surpass the US$10 billion mark; data revenue is projected to take pole position in 2014; adoption of cloud solutions will move from conceptual to the practical stage; enterprise IT will remain unconvinced about achieving "returns on mobility"; Malaysia's Big Data market is anticipated to hit US$24.2 million but is likely to remain at a tactical level; creating a sandbox to explore the usage of social in an internal context for collaboration; channel transformation in the 3rd platform for IT growth and innovation, built on mobile devices, cloud services; social technologies and big data will be a key agenda; consumerization of IT or BYOD is real and happening now, and organizations need to make a stand on what it means; Government to connect to citizens via mobile devices and social media, accelerating a new type of citizen and Government relationship and innovation in the 3rd Platform will create unique mash-up opportunities but may also create a perfect storm for project failure.

CHAPTER 7
SYMANTEC 2014 INTERNET SECURITY THREAT REPORT

Essentially, Symantec reports that in 2013, much attention was focused on cyber-espionage, threats to privacy and the acts of malicious insiders. However, some areas deserve special attention, surmised as targeted attacks growing and evolving; 2013 was the year of the mega data breach; ransomware attacks grew by 500% in 2013 and turned vicious; and attackers are turning to the Internet of Things. Specifically, the report highlights that the number of targeted attack campaigns increased by 91 percent in 2013. Symantec also found that the length of these campaigns was three times longer than campaigns in 2012. In 2013, attacks were made against governments and the services industry, with the industries most at risk of attack being mining and manufacturing.

Second, the total number of data breaches in 2013 was 62 percent higher than in 2012 with 253 total breaches. However, 2013 was the year of the mega breach, with 8 of the data breaches exposing more than 10 million identities. Third, scammers continued to leverage profitable ransomware scams in which the attacker pretends to be law enforcement, demanding a fake fine of between $100 and $500. First seen in 2012, these threats escalated in 2013, growing by 500 percent and becoming vicious in encrypting victims' files, causing even more damage in businesses.

Fourth, a wide variety of Internet-connected devices such as baby monitors, security cameras and routers were hacked in 2013. While the benefit to attackers of compromising these devices may not be immediately clear and there is still a lot of hype, the risk is real especially with Internet of Thing (IoT) devices.

CHAPTER 8
CAPABILITY OF THE INFORMATION AND COMMUNICATIONS TECHNOLOGY SERVICES USER SECTOR IN MALAYSIA: AN INDUSTRY PERSPECTIVE

Contributed by the Malaysian Service Providers Confederation (MSPC), this chapter provides the capability of the ICT User Sector (demand perspective) in comparison to past study that focused on the capability of ICT services producers or the supply perspective. The demand side findings are based on probing 108 CIO Chapter members of PIKOM. The study netted a 90% response. Like in the case of the supply side, the demand study also probed eight broad factors namely strategic leadership, government relations, institutional support and security & risk, quality and process, knowledge management, innovation process, market globalization, human capital and working motivation. Each factor looked at three questions.

In essence, the study revealed that that ICTS User companies secured the lowest score of 1.05 for innovation process, followed by 2.95 for on Government Relations out of a maximum 5 in the Likert scale. Detailed examination by factor analysis revealed that Government Relations was the weakest link in the ICTS User sector, despite being large. This may be due to CIO members of ICT User segments not having direct business dealings with Government, as they focus on providing internal IT services to their organizations. Nonetheless, the ICT User segments also did poorly in business efficacy aspects that entail innovation, R&D, patenting and commercialization. Again, as internal IT service providers, these activities may not fit well into their routines. Despite these shortcomings, the companies surveyed revealed that the ICT User segments have a strong sense and presence for IT security (3.72), branding (3.64) and business intelligence (3.42). In short, it can be surmised that the big ICT User corporations have strong IT capability despite scoring low on innovation.

CHAPTER 9
SOCIAL NETWORKING TECHNOLOGY AND SOCIOECONOMIC BEHAVIOUR IN MALAYSIA

Social network technology (SNT) has advanced from traditional information communication technology (ICT) to become the hallmark of online social interaction. With better access to the network intelligence, SNT can act as a key enabler to motivate socially-connected users for greater reach and richness of connectivity, entertainment, knowledge resources, business avenues and opportunities, and digital lifestyle. This study shows that while Facebook has become an integral part of social communication among Malaysian users, they are also increasingly aware of the economic and utilitarian benefits of using Facebook. Results also show that users' utilitarian use is about half their hedonic use of Facebook. Further, the empirical results show that the uses of Facebook for businesses have yielded positive economic outcomes in terms of increased productivity, profit, customer attraction and retention.

This study argues that change of perception among users, that is having positive perceived socio-economic benefits of using Facebook, is vital to motivate users from hedonic use to more advanced use for economic and utilitarian purposes. Obstacles that hinder nonusers from benefiting from the use of Facebook are privacy and security concerns, lack of interest and inadequate time to use. Strategies to encourage more advanced use of SNT that will enable the diverse population in Malaysia to leapfrog to a high income economy are discussed in this paper.

CHAPTER 10
CROSS-CUTTING TECHNOLOGIES: KEY TO NEW INDUSTRY GROWTH

The paper by MIMOS Berhad is on the use of cross-cutting technologies to develop Open Innovation Platforms (OIPs) / Open Innovation Frameworks (OIFs) to help the domestic ICT industry to grow in scope and capability so that it could compete in the global market. It explains how these techniques are used in the market-driven (needs-to-novelty) approach to rapidly develop high-impact products and solutions. The paper also explains the need for talent specialization to optimally work the needs-to-novelty innovation process. MIMOS also discusses its experience in implementing the OIP/OIF emphasizing the efficacy and potential of the cross-cutting technology approach for effective implementation of large high-impact products and solutions involving multiple vendors. It also clarifies how this cross-cutting technology approach could pave the way for the local industry players to partake of new technologies and work together for mutual good and growth.

ACKNOWLEDGEMENTS

PIKOM is extremely grateful to all Executive Council members for their wise counsel, judicious guidance and unflagging support towards the publication of the ICT Strategic Review 2014/15 edition. PIKOM would also like to acknowledge the invaluable contribution of all the supporting organisations and authors of this series.

Specifically, we would like to thank the Ministry of Communication and Multimedia (MCMC), Gartner, IDC, IBM Malaysia Sdn Bhd, MIMOS Berhad, Symantec Corporation (Malaysia) Sdn Bhd, Malaysian Services Provider Confederation (MSPC) and Monash University (Malaysia Campus) as well as many others who have spared the time and resources for the publication. We hope these key players in government, industry and academia will continue to lend their support for the future.

Lastly, PIKOM would like to register its sincere appreciation to the entire team in the PIKOM Secretariat for their individual support in the course of preparing this publication.

CHAPTER I

MALAYSIAN ECONOMIC AND ICT INDUSTRY OUTLOOK

WOON TAI HAI

PIKOM Research Committee Chairman

thwoon@pikom.org.my

The National ICT Association of Malaysia

I. INTRODUCTION

The Malaysian economy is expected to remain strong in 2014, with a forecasted growth in Gross Domestic Product (GDP) of 5.2% compared with 4.7% registered in 2013; see Figure 1. The economic performance for 2014 continues the upward trajectory in GDP since the traumatic events of the Global Financial Crisis in 2009.

Indeed, a closer examination shows the economy has expanded in every quarter (up till Q2 2014) since Q1 2013; see Figure 2. This upward momentum is expected to continue for the rest of the year and also spill over to 2015 when GDP is projected to grow by 5.2%, as forecasted by the International Monetary Fund (IMF).

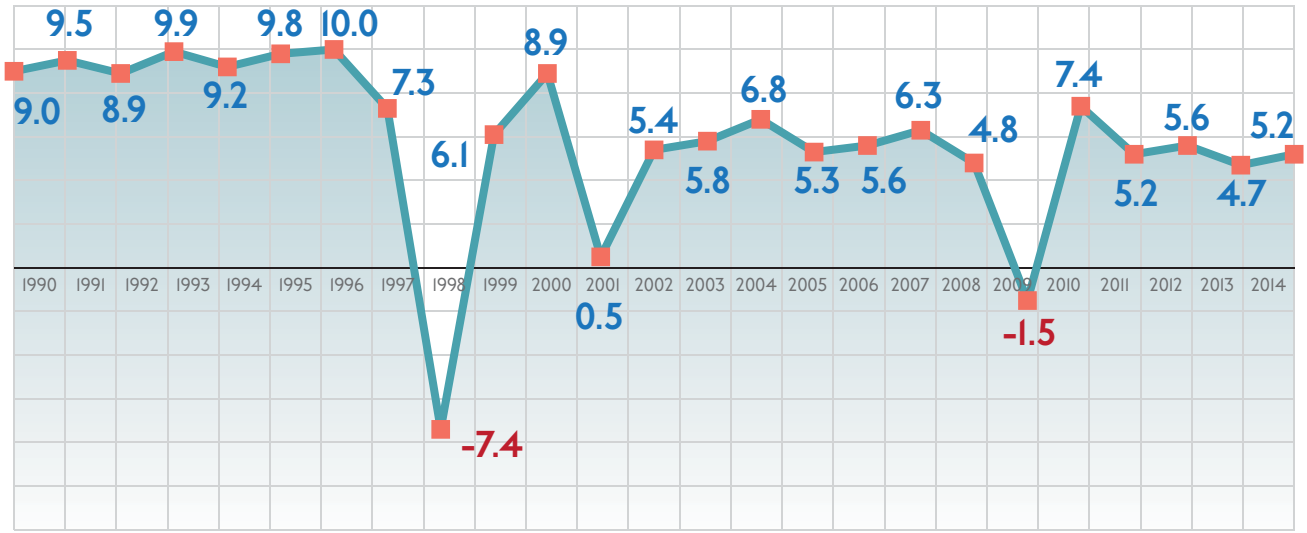


Figure 1: GDP Growth rate of Malaysia: 1990-2014
Source: Bank Negara Malaysia and Department of Statistics

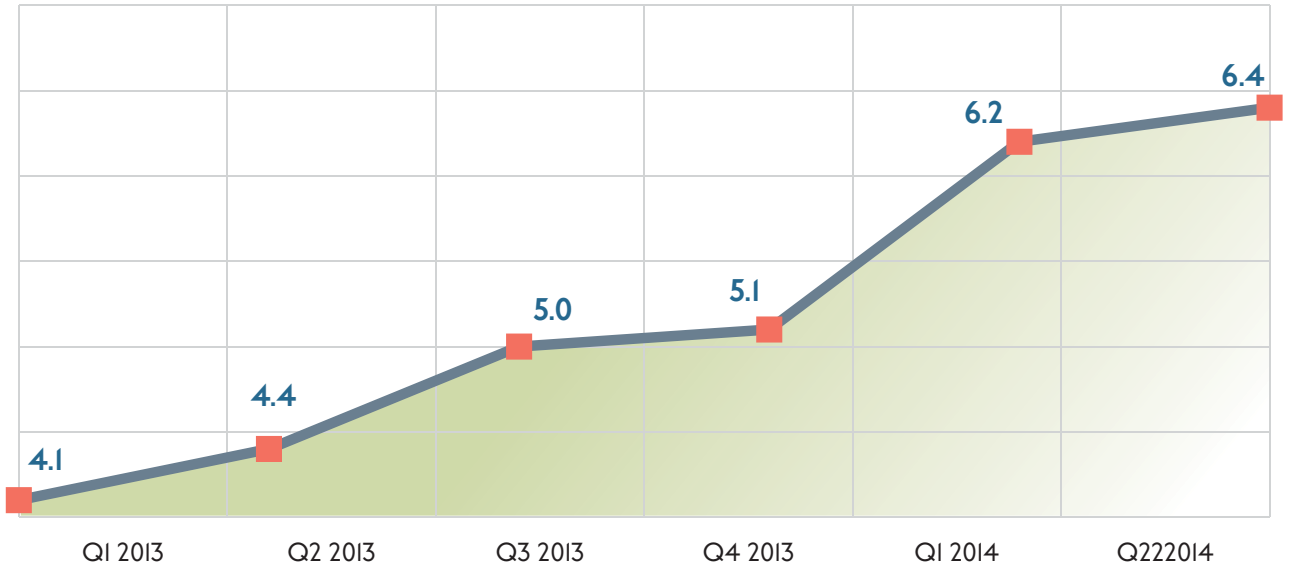


Figure 2: Quarterly Gross Domestic Product (GDP) Growth Rates: Q12013-Q22014
Source: Bank Negara Malaysia and Department of Statistics

Continuity in the positive economic growth can be attributed to healthy growth in domestic demand, private and public consumption, private and public investment, real imports and exports, as reflected in Table 1. Sound macro-economic conditions and prudent financial management as well political stability are the underpinning fundamentals that are stimulating economic growth.

2. MACRO-ECONOMIC FACTORS

2.1 PERFORMANCE OF ECONOMIC SUB-SECTORS

Table 1 shows the sectorial performance of Malaysia's economy from 2009 to 2013. Except for Mining & Quarrying and Manufacturing in 2009, all sectors have been registering positive performance over this period. Among the sectors, Construction and Services registered 10.9% and 5.9% in 2013 respectively. Indeed, in 2012 the growth rates for these two sectors were much higher, that is 18.6% and 6.4% respectively, as shown in Table 1. High growth rates in these two sectors are likely to have a positive impact on the Information Communications Technology (ICT) sector as these sectors are known for intensifying computer usage in improving efficiency and efficacy of their operations.

DOMESTIC DEMAND

As shown in Table 2, domestic demand driven mainly by private and public consumption expenditure as well as gross capital formation has been registering significant growth after the 2009 Global Financial Crisis, more so, driven by economic transformation and Corridor project activities. Specifically, private consumption expenditure grew by 7.2% in 2013, which was higher than the public consumption expenditure at 6.3%. However, the Central Bank of Malaysia has projected that consumption expenditure in the private and public sectors will register lower growth rates of 6.9% and 3.0% respectively in 2014 due to corrective measures in the financial

Economy Activity	2009	2010	2011	2012	2013
	Annual Percentage Change (%)				
Agriculture	0.1	2.4	5.8	1.3	2.1
Mining and quarrying	-6.5	-0.3	-5.4	1.0	0.7
Manufacturing	-9.0	11.9	4.7	4.8	3.5
Construction	6.2	11.4	4.7	18.6	10.9
Services (include Government services)	2.9	7.4	7.1	6.4	5.9

Table 1: Broad Sector GDP Growth Rate at 2005 Constant Prices (%), 2009-2013
Source: Department of Statistics

Domestic Demand by Type of Expenditure	2009	2010	2011	2012	2013	2014
	Annual Percentage Change (%)					
Private final consumption expenditure	0.6	6.9	6.9	8.2	7.2	6.9
Communication expenditure	5.9	10.6	10.4	12.5	10.5	13.4
Government final consumption expenditure	4.9	3.4	16.2	5.0	6.3	3.0
Gross fixed capital formation	-2.7	11.9	6.3	19.2	8.5	8.5

Table 2: Type of Expenditure of Malaysian Economy, 2005-2013
Source: Department of Statistics and PIKOM Estimates

system and subsidy rationalization measures theGovernment introduced recently. The lower growth in consumption expenditure is also likely to have a proportionate influence on the capital formation, which is poised to register the same growth rate in 2014 as that of the previous year. Pertinently, Table 2 also shows a significant growth rate in the expenditure incurred in the provision of communication services, which recorded double digit growth of 12.5% in 2012 and 10.5% in 2013. This translates into a positive impact on the provision of contemporary ICT services, which requires the requisite communication services in the form of wired or wired technology. PIKOM has forecasted a growth rate of 13.4% for Communication expenditure in 2014.

TRADE DEPENDENCY

While domestic demand is the key factor, external demand has an important supporting role. On the trade front, Malaysia's exports including goods and services expanded marginally by 0.6% to RM705.2 billion in 2013 from RM700.8 billion in 2012, and imports edged up 1.9% to RM649.4 billion from RM636.9 billion in 2012; see Table 3. During the first half of 2014 export trade expanded to RM380 billion on the back of 7.9% growth year-on-year;. Electrical and Electronic (E&E) products accounted for 33.3% of total exports, rising 5.5% or RM1.1 billion to RM20.4 billion. Imports declined by 5.5% to RM335.5 billion during this period; E&E products decreased by 3.8% or RM813.5 million from RM21.2 billion during the January-June, 2014 period. It is also interesting to note that exports of overall services such as professional, education, health and ICT services grew significantly by 7.7% from RM89.99 billion in 2009 to RM110.66 billion in 2013. In tandem, imports of services also grew by 5.5% from RM89.06 billion to RM120.92 billion over the same period. Table 3 also shows that share of export services increased from 14.6% in 2009 to 15.7% in 2013 and similarly, the share of import services expanded from 17.6% to 18.6% during this period.

Taking into consideration the significant growth in trade in services, attempts were made to analyse the exports and imports of ICT Services, which have increased its visibility in the trade sector as a result of the MSC Malaysia programme in the mid-nineties. As reflected in Figure 3, exports of ICTS grew from RM2,382 million in 2005 to RM9,122 million by 2013, registering an annual average growth of 18.3%. Similarly, ICT imports also grew from RM2,577 million to RM8,687, recording an annual growth rate of 16.4% over the same period. Notably, exports of ICTS services have been higher than imports of ICTS, indicating the country has become a net exporter of ICTS. In tandem, the share of ICTS exports to total Serivces exports

Trade	2009	2010	2011	2012	2013
	RM million				
Total Exports of Goods & services	**615,012**	**683,391**	**713,893**	**700,819**	**705,260**
Exports of Goods	525,021	591,165	615,970	598,081	594,604
Exports of Services	89,991	92,226	97,923	102,738	110,657
Share of services exports (%)	14.6	13.5	13.7	14.7	15.7
Total Imports of Goods & Services	**505,874**	**585,031**	**621,555**	**636,921**	**649,404**
Imports of Goods	416,811	490,351	518,431	522,232	528,481
Imports of Services	89,063	94,680	103,125	114,689	120,923
Share of services exports (%)	17.6	16.2	16.6	18.0	18.6

Table 3 : Exports and Imports of Goods and Services of Malaysia
Source: Department of Statistics

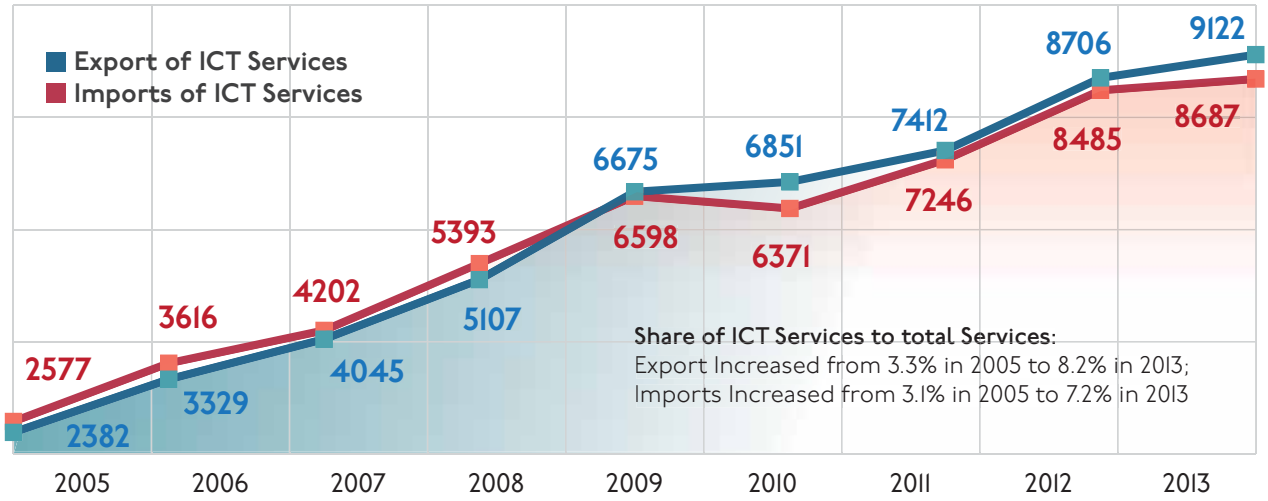


Figure 3: Exports and Imports of Telecommunication, Computer and Information Services
Source: Department of Statistics

Countries	Gross Exports	Countries	Gross Imports
Vietnam	13.30	Brunei Darussalam	40.11
People's Republic of China	13.00	Vietnam	27.16
Indonesia	12.32	India	15.07
New Zealand	11.02	People's Republic of China	11.69
India	9.41	Australia	10.34
Brunei Darussalam	8.83	New Zealand	8.74
Australia	7.04	Russia	8.54
Thailand	6.37	Singapore	6.83
Japan	5.68	Thailand	6.49
Korea	3.78	Indonesia	6.42
Singapore	3.78	Korea	4.94
Chinese Taipei	3.03	China Taipei	4.28
Russia	2.94	Hong Kong China	-0.22
Philippines	2.65	Japan	-1.47
Hong Kong China	0.94	Philippines	-8.65
Other countries	10.43	Others countries	11.86
ASEAN	6.82	ASEAN	6.77
Europe	0.85	Europe	4.40
North America	-4.78	North America	-1.4

Table 4: Trade Growth Rate Performance (%) of Malaysia Against Selected Country / Region : 2004-2013
Source Data: Bank Negara Malaysia; PIKOM

increased from 3.3% to 8.2% during the 2005-2013 period. Similarly, the share of imports of ICTS to total imports of Services also increased from 3.1% to 7.2% during this period.

Bank Negara Malaysia predicted only a 2.1% growth for real exports and 3.1% for real imports for the year 2014. This forecast is premised on continuity of trade with its strong partners especially China, ASEAN countries and Japan, with India joining the ranks of late, as shown in Table 4. Singapore alone accounted for 13.9% of total exports and 12.9% of total imports with Malaysia during

January – June 2014, with China accounting for 12.0% of exports and 16.0% of imports. Thus, the established trading volume is indeed an advantage to Malaysia especially when IMF has forecasted positive economic growth for these nations for the year 2014 and 2015.

It is conjectured that exports and imports of Services including ICT Services will rise when the ASEAN Common Effective Preferential Tariffs (CEPT), multilateral arrangements under the World Trade Organization (WTO) and bilateral Free Trade Arrangements (FTA) with Japan, Pakistan, New Zealand, India, Chile and Australia come into greater force resulting in a greater flow of goods, services and people.

FOREIGN DIRECT INVESTMENT

Despite promulgating endogenous growth through R&D and innovation strategies, the country is still highly dependent on foreign direct investment (FDI) to support the economy. Table 5 shows the flow of FDI by country of origin into Malaysia; the aggregated figures shown for the period 2010-2013 iron out the yearly fluctuations. It can be seen from Table 5 that Japan, Singapore and the Netherlands have been consistently ranked on the top, respectively registering 19.8%, 14.2% and 12.7%. Regionally, 25.6% of FDI came from North Asia, followed by 20.7% from Europe and 15.2% from ASEAN. Pertinently, it can be seen that there are hardly any FDI coming from countries currently

Countries	2010	2011	2012	2013	2010-2013	
	RM million	RM million	RM million	RM million	RM million	%
Other Countries	5,258	10,807	11,053	6,364	33,482	24.5
Japan	2,876	9,868	6,122	8,230	27,096	19.8
Singapore	1,405	6,347	5,962	5,653	19,367	14.2
Netherlands	6,125	3,552	1,981	5,630	17,288	12.7
USA	8,031	3,342	(1,707)	717	10,383	7.6
Central & South America	2,954	(3,381)	1,649	4,805	6,027	4.4
Switzerland	798	1,033	1,659	1,849	5,339	3.9
Korea	4,576	429	(203)	(512)	4,290	3.1
Hong Kong	(761)	(436)	854	4,077	3,734	2.7
Germany	(476)	3,077	1,097	(462)	3,236	2.4
Australia	15	675	1,679	494	2,863	2.1
Thailand	(398)	1,147	(192)	762	1,319	1.0
France	607	345	(127)	344	1,169	0.9
United Kingdom	(1,301)	1,030	908	481	1,118	0.8
China	(3)	25	(9)	444	457	0.3
Denmark	(104)	103	(59)	140	80	0.1
Luxembourg	132	(521)	695	(333)	(27)	0.0
China Taipei	(412)	(119)	(248)	90	(689)	-0.5
Total	29,322	37,323	31,114	38,773	136,532	100.0
Europe	5,781	8,619	6,154	7,649	28,203	20.7
North America	6,276	9,767	6,516	12,329	34,888	25.6
ASEAN	1,007	7,494	5,770	6,415	20,686	15.2

Table 5: Foreign Direct Investment in Malaysia 2010-2013
Source: Department of Statistics, 2014

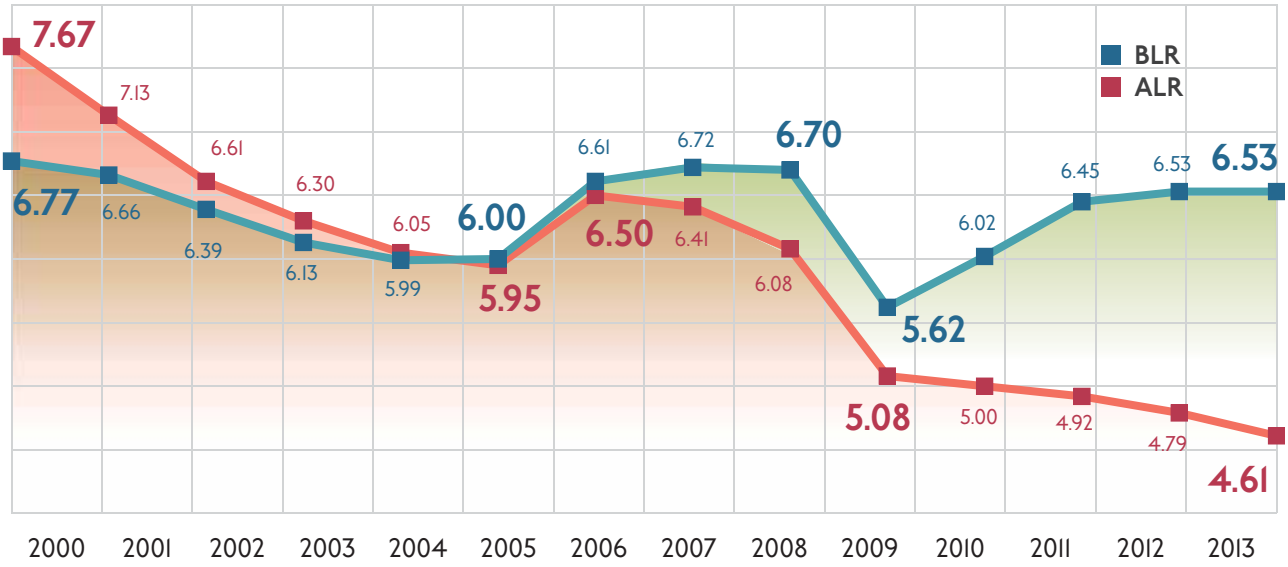


Figure 4: Average BLR and ALR Trend : 2000-2013
Data source: Bank Negara Malaysia

afflicted by political or economic crises. As such, it can be conjectured that this investment trendwill persist for Malaysia.

MACRO SELECTED INDICATORS

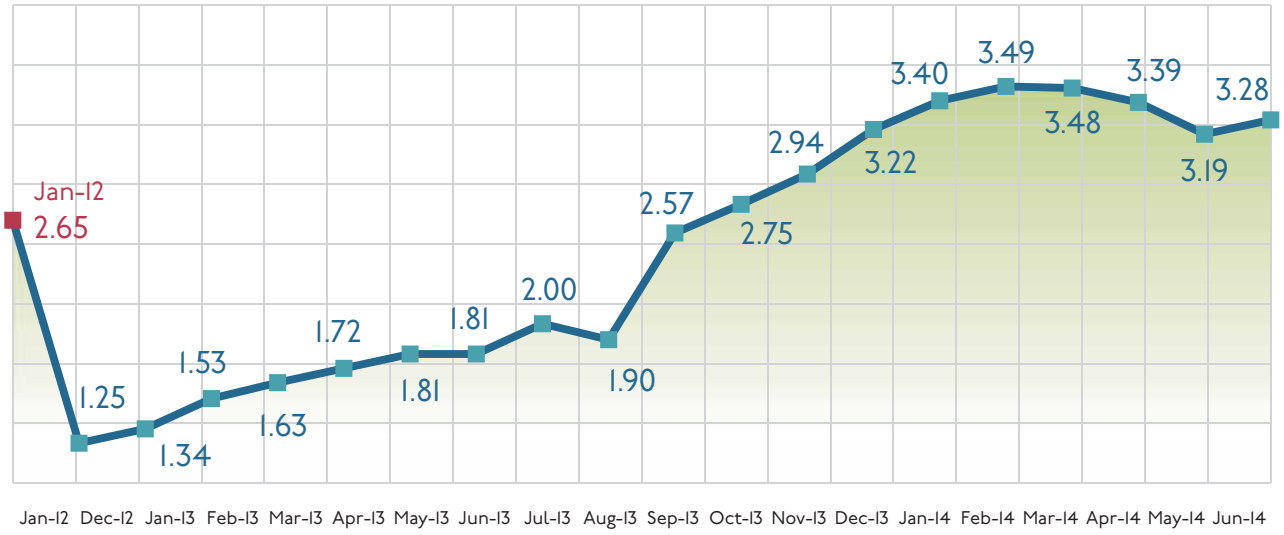
Despite some challenges, the macro-economic fundamentals remain largely unperturbed, and will still be supported in particular by a low inflation rate, low unemployment rate and low overnight lending rates.

LENDING RATES: OVERNIGHT POLICY RATE (OPR) AND BASE LENDING RATE (BLR)

As a response to the rising household indebtedness that reached 86.8% of GDP and a debt-service ratio (DSR), standing at 43% by the end of 2013, the Monetary Policy Committee of Bank Negara Malaysia increased the OPR to 3.25% on 10 July, 2014. With this increase, the base lending rates (BLR), inter-bank rates across all maturities and retail lending and deposit rates are expected to register upward movements. The BLR typically differs among financial institutions, which take into account the cost of operations besides statutory regulations and global monetary conditions. However, as shown in Figure 4, the BLR has yet to register any increase, and its average remains at 6.53% per annum like in the previous year. Such low BLR have been stimulating not only private consumption at the household level, but also small and medium business loans and domestic investments.

INFLATION RATE

Headline inflation, as measured by the annual percentage change in the Consumer Price Index (CPI), edged slightly higher to 3.28% in June 2014 (May: 3.2%). Pertinently, the inflation rate had declined from 2.65% in January 2012 to 1.25% in December 2012, before reversing this trend to head upwards. By taking into consideration the 6-month moving average as reflected in Figure 5, the inflation rate is projected to hit 3.68% mark by end 2014. Increasing inflationary pressures have been primarily attributed to the ongoing subsidy rationalisation efforts by the government starting from the fuel hike, higher electricity tariffs to the abolishment of sugar subsidies in 2013. Some research houses indicated that the impending introduction of GST in April 2015 is expected to exert additional pressure on inflation numbers partly as households bring forward their consumption or partly by the likelihood of profiteering activities prior to GST implementation.



Malaysian Inflation Rate Year on Year (YoY)%: December 2012 - June 2014
Data source: Bank Negara Malaysia

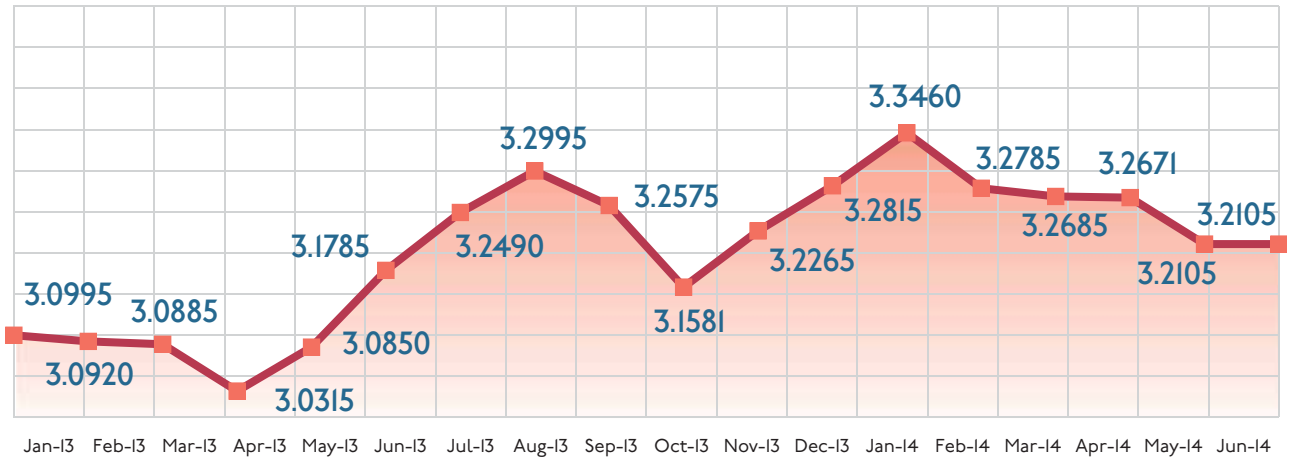


Figure 6: Exchange Rate per USD (Ringgit Malaysia) : January 2013-June 2014
Data source: Bank Negara Malaysia

FOREIGN EXCHANGE RATE

The performance of the Malaysian currency against the US dollar for the period January 2013 to June 2014 is shown in Figure 6. Purchasing power, especially on foreign goods and services, is augmented in tandem with the increasing strength of the Malaysian Ringgit against the USD. As reflected in Figure 6, the Ringgit was weaker against the US dollar from April 2013 to January 2014, fluctuating between RM3.0315 and RM3.3460 thus making imports costly. However, beginning January 2014, the Ringgit gained strength from RM3.346 to RM3.215 in June 2014, which partly explains the improved net trade performance during the first half of 2014.

UNEMPLOYMENT RATE

Figure 7 shows the overall unemployment rate in Malaysia from 1982 when the country began to pursue industrialization till May 2014, when it has largely remained low. Indeed, economically the nation has attained full-employment status. Due to the short supply of labour internally, selected businesses end importing foreign labourers especially in the production and operations sectors. However, a small number of ICT knowledge workers are also imported

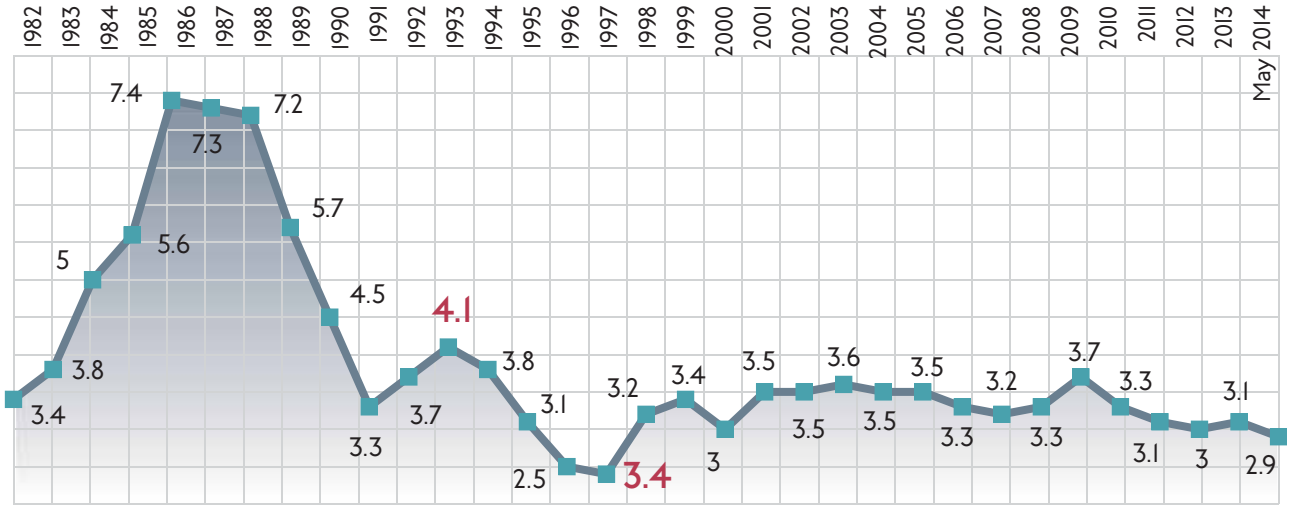


Figure 7: Unemployment Rate in Malaysia : 1982-May 2014
Source: Bank Negara Malaysia

from countries like India to meet the demand in high value adding sectors including R&D and innovation. Despite the low unemployment and tight labour environment, unemployment among graduates has always remained as a critical issue politically and socially, as it affects the aspirations and motivations as well as dignity among educated young job entrants into the market. Past studies have revealed that some graduates are choosy about their job placements, causing frictional employment; a significant number of degree and diploma holders worked in a field that did not match with their higher educational qualifications; and more importantly, attributed to the lack of employability owing to graduates not equipped with the requisite qualification, skills, experience and exposure that the industries demand. Some of the attributes in demand include competency in technical skills, problem-solving skills, confidence, maturity, leadership and communication skills, especially in English language.

ECONOMIC CHALLENGES

Despite political stability as well asprudent finance and favourable economic fundamentals, the Malaysian economy is not totally free from economic encumbrances especially investment-related risk factors.

Like in the previous years, the country is continuously plaguedby unpredictable commodity prices in the export market, erratic fluctuations in the macro indicators especially in foreign exchange and inflation rates, unemployment among graduates, presence of excessive foreign workers leading to unwarranted social problems, and short supply of graduates especially in meeting human capital needs in the ICT segments. Despite the emerging challenges, the Malaysian economy is compelled to deal with the following:-

- **Subsidy rationalization**
  Following the announcements on the hike in petrol prices, sugar and electricity tariffsthe Government, as expected, faced a backlash from various quarters. One of the challenges that the Government faces is rationalizing subsidies without placing too much of a burden on the lower and middle income families. The fear is the rising cost of living, which makes many, in particular those in the lower rung of society and those starting their careers, to tighten their belts. In coping with therising cost of living, some are even considering postponing marriage; forming even smaller families that is already below replacement level; and resorting to public transportation modes even though reliability

remains a challenge. On the contrary, the average monthly household income increased from RM2,283 in 2007 to RM3,080 in 2012, registering a 7.0% growth per annum. In other words, household income growth has not been translating into better consumption patterns for a typical family and as such, purchase of ICT products and services tend to be affected due to lack of affordability and priority of needs.

- **Reducing fiscal deficit**
  The Government is trying hard to achieve a balance budget before 2020, when the nation is expected to achieve developed status. In this endeavour, by pursuing aggressive government spending and reducing state subsidies, the Government successfully reduced the fiscal deficit to 3.9% of GDP in 2013, which in comparison was 4.5% of GDP in 2012. In this progression, theGovernment's immediate target is to realize a further reduction in the budget gap to 3.5% in 2014 and 3% in 2015. To reduce its fiscal deficit, the Government may do sequencing or re-scheduling of megaprojects that are likely to have adverse effects on ICT spending.

- **Goods and Services Tax (GST) implementation**
  The consumption-based GST system is due for implementation by April 2015. This broad-based system is poised to replace the current narrow-based sales tax, which only an estimated 1.7 million of the 12 million working population currently pay. The biggest problem is that the Sales and Services Tax can easily be evaded by the people because there is no connection with the production so it is harder to audit. With a credit-system in place, the evasion of tax can be mitigated. Thus, by migrating from the direct system regime into a value-added consumption tax scheme, the national coffers can increase. Increase in Government revenue can help since it could lead to new development programmes that may fuel growth in ICT Sector. Under the current input-output tax system, purchases of computers and their accessories are exempted from sales tax. However, under GST, no tax exemption is granted for such purchases and thus retail prices of computers and accessories are projected to go up in the initial stages of implementation until the GST tax filing system stabilizes.

ICT INDUSTRY OUTLOOK

Like in the previous years, the ICT industry especially its services components continue to show a positive outlook. The ICT Services components include telecommunication entailing fixed and mobile telephony services, Internet access, satellite and data communication services; computer services comprise hardware and software wholesaling, retailing and consulting, programming as well as repair and maintenance activities; publishing activities entail both traditional and online printing; motion picture, video and television programmes and information services activities such as data processing, hosting data, web portals that are considered as content activities. With this contemporary definition, as shown in Figure 8, the ICT Services sector is expected to register 13.6% growth in 2014 by shoring up its value added services to RM68.0 billion from RM59.8 billion in 2013. Conservatively, the overall ICT Services sector is poised to grow at 12.7% in 2015 and is expected to record RM77.7 billion in terms of value added services. The projected growth rate takes into consideration the inherent dynamism the ICT Services during the period 2010-2014 when the value added services increased from RM42.1 billion to RM68.0 billion. Pertinently it is also worthy to note that the share of ICT Services to overall GDP is projected to increased from 3.3% in 2000 to 6.7% in 2015.

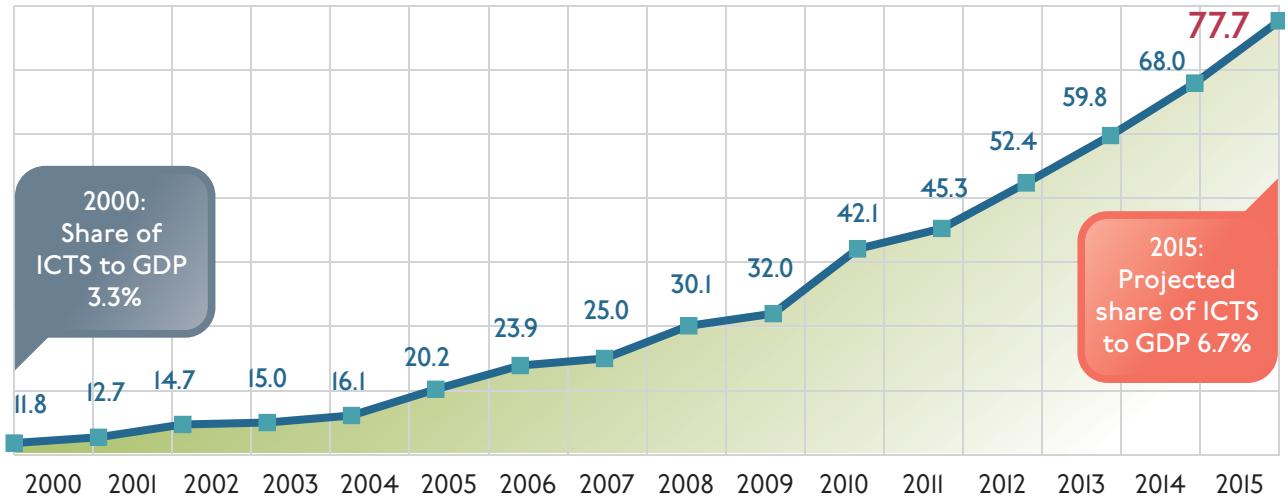


Figure 8: Distribution and Growth Rates of ICT Services by Sub-sectors: 2000-2015
Source : Department of Statistics and PIKOM Estimates

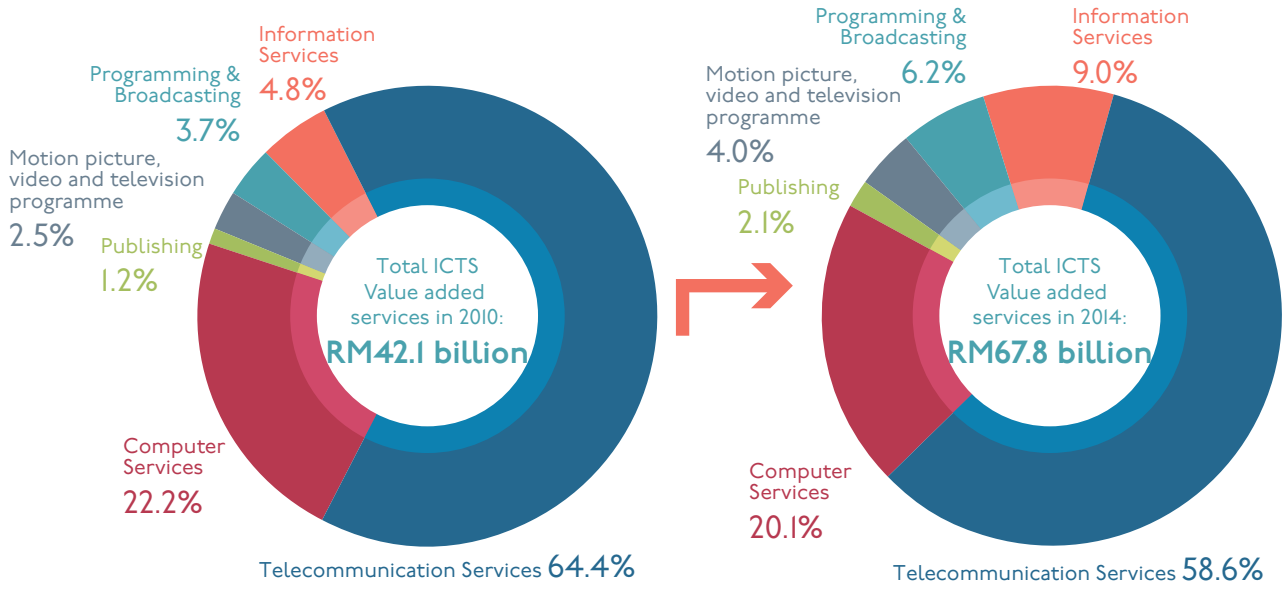


Figure 9: Share of ICT Services Components, 2010 and 2014
Source : Department of Statistics and PIKOM Estimates

The other interesting thing that warrants attention is structural changes within the ICT Services segments. As shown in Figure 9, the share of telecommunication services declined significantly from 64.4% in 2010 to 58.6% by 2014. Similarly, computer services declined marginally from 22.2% to 20.0% during this period; this decline may be attributed to changes in the devices landscape where miniaturization of computing devices in the form of cellular, tablets, Internet of things and wearable technology is gaining ground and surpassing traditional computers in the industry. In tandem, the share of information services activities markedly increased from 4.8% to 9.0%; share of provision of content related activities also rose significantly. It is generally conjectured that the fast emerging structural changes are attributed to the significant increase in the deployment of cloud computing, Internet of things, wearable technology, big data analytics, social media and mobile applications in a reinforced and convergent manner.

KEY CHALLENGES IN THE ICT SECTOR

Despite its dynamism, the nation's ICT sector will continue to face several persistent challenges. Like in the previous years, the issues pertaining to short supply of ICT graduates from Institutes of Higher Learning (IHL), quality of graduates not able to meet the industry demands, negative perception and disillusionment of low employment opportunities in the ICT segments by the wider public and the students and lack of professional recognition and accreditation, continue to plague the sector. At the industry level, the uptake of globally recognized certifications such as Capability Maturity Model Integration (CMMI), People Capability Maturity Model (PCMM) certification, research and development, innovation, patenting and commercialisation culture et cetera are still at a very low ebb. However, the more pressing challenges that warrant industry attention are: one is talent migration across borders; and the other is preparedness of businesses to embrace convergence and reinforcement of technology, people, process and institutions.

TALENT MIGRATION

Talent migration across borders is likely to pick up once the ASEAN 2015 takes effect, enabling a greater flow of goods, services and people across borders. It is expected that ICT graduates and experienced professionals will be prone to migrate in search of better remuneration opportunities, career advancements and in search of experience, skills, and exposure. Table 6 below shows a comparative analysis of the remuneration earned by ICT professionals in selected Asian and English speaking countries. Without any purchasing power parity (PPP) adjustment, the results show that more advanced Asian economies, in particular skilled employment in Hong Kong and Singapore, recorded average remuneration that were 2.47 to 2.26 times more than the average remuneration earned by Malaysian ICT professionals in 2013. Besides these two countries, China, Thailand and Vietnam also offer higher remuneration for ICT professionals at 1.93, 1.50 and 1.66 times more than Malaysia respectively, perhaps for expatriate employment. Indeed, technically speaking, ambitious job seekers should use PPP adjusted figures when searching for overseas jobs as the compilation takes into account inflation and foreign exchange rates as well as the standard of living. Malaysians are typically known to search for better opportunities beyond the shores of Asia especially in English speaking countries, in particular the United States, United Kingdom, Canada, Australia and New Zealand.

CONVERGENCE AND REINFORCEMENT OF TECHNOLOGY, PEOPLE AND PROCESSES

One of the fast technological advancements, especially in the world of digitization of processes, is convergence and reinforcement of technology, people and processes. Such phenomena are on the rise with increasing deployment of cloud computing, big data analytics, application of social media in businesses, miniaturization of devices taking the shape of wearable technology and Internet of things, Y and Z generations demanding buy your own device (BYOD) and flexi working hours and arrangements as integrals of tele-working practices and mobility enhancing business agility. Now the question is how well businesses, and industries as well as the employers and employees, are prepared in harnessing these emerging phenomena including challenges and threats. Indeed, not only preparedness, but also strategic planning and systematic implementation of new technology nuances and best practices warrant due attention for business continuity and relevance as well as for innovation and creating new business opportunities.

Country	ATLAS CRITERION			PURCHASING POWER PARITY ADJUSTED		
	Skill & Speciality	Years of Experience	Employment Size	Skill & Speciality	Years of Experience	Employment Size
Malaysia	1.00	1.00	1.00	1.00	1.00	1.00
Australia	3.74	3.20	3.45	1.65	1.41	1.52
United States	3.25	2.98	3.17	1.97	1.81	1.92
New Zealand	2.99	2.55	2.77	1.77	1.51	1.64
Canada	3.01	2.69	2.90	1.52	1.35	1.33
United Kingdom	2.51	2.29	2.40	1.46	1.33	1.40
Indonesia	0.71	0.81	0.82	0.60	0.68	0.69
Hong Kong	2.47	2.34	2.57	2.13	2.01	2.21
Vietnam	1.66	1.40	1.44	2.42	2.04	2.10
Philippines	0.43	0.49	0.40	0.46	0.52	0.42
1.98	1.93	1.97	2.18	1.84	1.88	2.08
India	0.48	0.54	0.42	0.72	0.81	0.63
Singapore	2.26	2.30	2.28	1.74	1.76	1.75
Thailand	1.50	1.25	1.54	1.61	1.34	1.66

Table 6: Benchmarking Average Salaries Earned by ICT Professionals of Selected Countries against Malaysia, 2013
Source : PIKOM

CONCLUSION

As reflected in the macro economic scenario, the country is poised to register positive growth in 2014 and 2015. The ICTS sector is poised to contribute significantly to the share of the economy and the Services sector with the increasing presence of new age technologies such as cloud computing, big data analytics, social technology media, broadband et cetera. The growth can be further enhanced provided small and medium-sized enterprises (SME) are mainstreamed through new age technological advancements. Effective economic growth can only be sustained provided the country pursues effective measures in resolving some of the issues and challenges plaguing the industry.

CHAPTER 2

INTERNET OF THINGS (IoT) DRIVE INFORMATION OF THINGS (IOT): MOBILITY, SECURITY, ANALYTICS AND TALENT PERSPECTIVES

WOON TAI HAI
PIKOM Research Committee Chairman
thwoon@pikom.org.my

RAMACHANDRAN RAMASAMY
Head of Policy, Capability and Research
ramachan@pikom.org.my

The National ICT Association of Malaysia

PIKOM

I. INTRODUCTION

Today, Internet-Enabled digital devices not only give one access to global information but also a channel to navigate the physical world. The early nineties saw the emergence of webpages that typically provided text-filled boxes and hyper-links to more content. By the dawn of the century, social web phenomena such as Friendster, Facebook, Twitter et cetera came to the fore. Social web platforms provide a medium for the world to be more open and stay connected with greater interactivity that transcends geography, time, traditions and cultures. Apart from individual or group profiles, social webs support content presentation in multimedia formats. As such, it is hard to find a Facebook account without photographs, graphics, animation and videos. Initially, social webs started off by facilitating individuals to build peer relationships as well as share social activities and routines. However, in the process, some began leveraging social webs for business so much so that its original intent and outlook for social interconnectivity became muddled with business information. These include products and service advertisements, vacancy announcements, job recruitment, conference invitations, fund raising campaigns, political deliberations, interest groups formation, crowd sourcing et cetera. All these things have become a reality in the social realm, more so proliferating at an unprecedented rate even as technology increasingly pursues its path of miniaturization, ubiquity, pervasiveness, mobility and agility (Carlton, 2012; Gartner, 2014). Hand-held devices like cellular phones, tablets and phablets - when connected to wireless broadband and supported with ease of operations and user friendly features - are now providing a true sense of anywhere, anytime and anyone usage opportunities in businesses and social life.

Technology conveniences in online and real-time communications for relationship building have certainly increased the number of social technology users exponentially in recent years (Carlton, 2012; IBM, 2013). More so, the economy of scale is driving down the subscription costs of social technologies. Consequently more people from every walk of life have begun to subscribe to the new virtual reality that was once populated by the elite, educated and professional groups. Recognising the demographic diversity and the inherent value, many social web service providers have embedded big data analytics (BDA) as an integral component of their business operations; essentially aimed at culling out actionable business intelligence from their huge member databases. More and more, BDA best practices have now become part of the strategy in business entities especially those that have adopted Internet practices in their business operations. Nonetheless, the adoption of new technology or best practices is not that easy and straightforward as it comes with a price. Most critically, the implementation of BDA practices requires an inter-disciplinary approach, demanding not only the traditional statistical science knowledge, but also computing and operations research skills and more importantly, business development knowledge.

The discipline also fuels the demand for data scientists who are presumably equipped with the requisite inter-disciplinary knowledge (IBM, 2013; Bersin, 2013). Indeed, BDA is still very much in its infancy. Many organizations in both the private and public sectors, big and small & medium-sized enterprises, have just started to explore analytics and their potential. However, the challenge is always in engaging the right candidate for the BDA job. Contemporary data science discipline is new toacademic institutions. Thus, the current supply of data scientists is also limited. Nonetheless, the emerging industry demands that academia start churning out data scientists. Organizations that have traditional BDA practices are retooling and reskilling their

analysts with requisite BDA capabilities. An IBM study has revealed that in the US, BDA penetration in businesses is poised to grow significantly in the years ahead. Enthusiasm and motivation in pursuit of new knowledge or innovations or best practices are critical in spearheading businesses to competitive levels. At this juncture, countries are at different levels of readiness in implementing BDA initiatives. In Malaysia, the level of enthusiasm and readiness for BDA is at best still in its infancy. Before BDA becomes a widespread practice, businesses are again at another point of inflexion in harnessing opportunities offered by the Internet of things (IoT). IoT, on its own,drives new opportunities in the Information of Things (IOT) (Gartner, 2014).

Gartner defines the "Internet of Things" as the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. It is also referred to by some vendors as the "industrial Internet," the "Internet of Everything" or "cloud of things" or even the "connected world". However, the connections are essentially through the existing Internet infrastructure. Premising upon this technological advancement, the IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications (Holler et al, 2014). The interconnection of these embedded devices, including smart objects that can describe their own possible interactions, are expected to usher in automation in nearly all fields such as heart monitoring implants, biochip transponders on farm animals, automobiles with built-in sensors, or field operation devices that assist fire-fighters in search and rescue. Advanced applications like smart thermostats in many smart home devices - for example in washer/dryers - are already utilizing WiFi for remote monitoring. This trend is poised to leverage and revolutionize the smart grid utilization that employs analog or digital ICT to gather and act on information - such as the behavior of suppliers and consumers - in an automated fashion to improve the efficiency, reliability, economics, and sustainability of applications. Due to the ubiquitous and pervasive nature of connected objects in the IoT, an unprecedented number of devices are expected to be connected to the Internet. According to Gartner, there will be nearly 26 billion devices on the Internet of Things by 2020 (Gartner, 2014). ABI Research estimates that more than 30 billion devices will be wirelessly connected to the Internet of Things by 2020 (ABI, 2014). The current challenge is Ipv4, whichhas limited space for integration and can accommodate only 4.3 billion unique IP addresses. However, Ipv4 is poised to expand many fold upon the full realization of Ipv6. In tandem, research and development on low energy consumption devices that can operate independently of WiFior cellular network technology, as well as higher order computing devices needed to perform heavier duty tasks like (routing, switching, data processing and etc.), are aggressively being pursued by research scientists.

The development of protocols, systems, architectures and frameworks aimed at enabling the IoT through prominent standardization bodies such as the IETF, IPSO Alliance and ETSI, are also taking centrestage in the research endeavour. In other words, the plethora of new application areas poised to arise from the IoT phenomena are projected to generate large amounts of data from diverse locations in integrated, networked, aggregated and more so, in a very high-velocity form, thereby increasing the need to better index, store and process such data. Thus, it is becoming apparent that the Information of Things (IOT) is emerging as the next inflexion point for business intelligence, more so in the form of ambient intelligence. The notion of ambient intelligence was mooted in the early nineties as an integral part of

consumer electronics, telecommunications and computing and nowadays, it is emerging as reality in the form of the Information of Things.

AMBIENT INTELLIGENCE

In computing, ambient intelligence (A&I) refers to electronic environments that are sensitive and responsive to the presence of people. Specifically, in an ambient intelligent world, devices work in concert to support people in carrying out their everyday life activities, tasks and rituals in an easy, natural way using information and intelligence that are hidden in the network connecting these devices. As these devices grow smaller, more connected and more integrated into our environment, the technology disappears into our surroundings until only the user interface can be perceived by users. The ambient intelligence paradigm builds upon pervasive computing, ubiquitous computing, profiling, context awareness, and human-centric computer interaction design and is characterized by systems and technologies that are (Aarts, Harwig & Schuurmans 2001):

- embedded: many networked devices are integrated into the environment
- context aware: these devices can recognize you and your situational context
- personalized: they can be tailored to your needs
- adaptive: they can change in response to you
- anticipatory: they can anticipate your desires without conscious mediation

As such in the context of today's technological advancements, ambient intelligence is shaped by IoT, which increasingly drives IOT since technologies are able to automate a platform by embedding the required devices for powering context aware, personalized, adaptive and anticipatory services. As highlighted in Figure 1, IoT is the key driver of semantic web, termed as Web 3.0, which has been projected to grow exponentially in the near future and subsequently forecasted to evolve into intelligence web or web 4.0, mainly characterized by elements of reasoning.

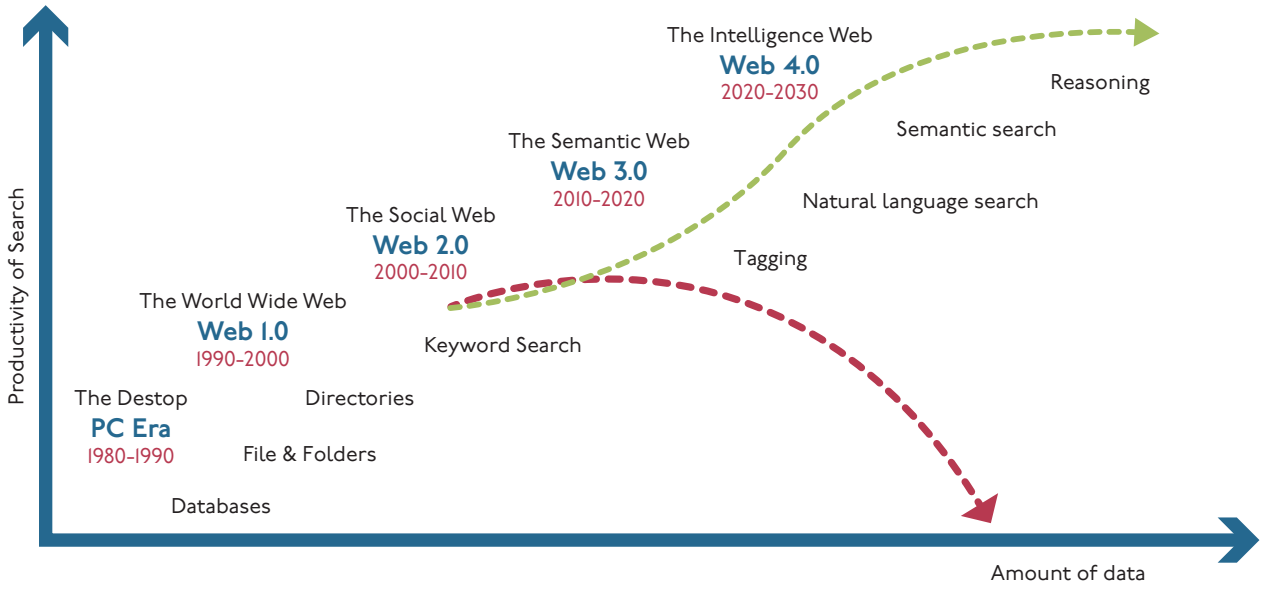


Figure 1: Web Evolutionary Framework: 1990-2030

MOBILITY SECURITY ANALYTICS AND TALENT (MSAT) FRAMEWORK

Acknowledging the rapidly-emerging diversity and complexity, among many others, businesses are called to pay due attention to four fundamental elements that are poised to influence the dynamics of Information of Things of future businesses.These are mobility, security and analytics as shown in the Mobility Security Analytics and Talent (MSAT) Framework (Figure 2). With f high speed broadband technology, mobile or wearable devices for businesses and lifestyle are becoming more agile, ubiquitous and pervasive. As depicted in the framework, the future business and policy intelligence collation is not only confined to the three dimensional factors of MSAT, but also the interactive components among them, namely agility, ubiquity and pervasive as well as talents, which is the overarching component that drives all the other three elements. The notion of the framework is that businesses are becoming more agile under secured mobile transactions; ubiquity increases when mobile transactions are constantly monitored, gauged and evaluated and supported with prescribed solutions in addressing the issues, challenges, problems, threats and opportunities and similarly, pervasiveness comes with security analytics in place as an integral component of business strategy and operations.

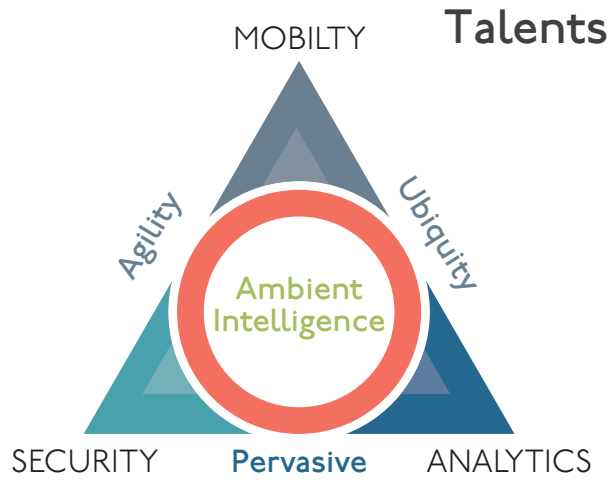


Figure 2: Mobility Security Analytics and Talent (MSAT) Framework

MOBILITY

Businesses have become more mobile and agile. Convergence and reinforcement of content, process and the people through contemporary ICT changes the roles, rights, rules and regulations of governance processes. The exertions are unprecedented, compelling organizations to change in the way they work, learn, play, communicate, network, entertain, perform transactions and build relationships. It has been more than two decades since the advent of Internet technology, which distinctly marked the beginning of contemporary ICT or information age. Since then, ICT has gone through a number of inflexion points, pertinently:

- witnessing the emergence of knowledge-based or ICT-led innovation economy;
- rise of knowledge workers equipped with computing and ICT skills and competencies;
- enhancing elements of good governance through tripatriate partnerships connecting public, private and tertiary sectors including civil societies, non-governmental organizations and media virtually, besides physically;
- public institutions and business organizations intertwined with online connectivity and real-time interactivity;
- work cultures, practices and processes are evolving to meet the aspirations of technology savvy Y and Z generations whose expectations for teleworking and buy your own device (BYOD) are posing challenges to traditional HR practices;
- transcending borderless transactions and building relationships irrespective of time, geography and traditions;
- changing devices landscape where hand-held mobile devices are fast replacing traditional desktops and laptops;
- the world wide web (WWW) of yesteryear has evolved into structured social webs and is poised to evolve into semantics or intelligence webs in the future;
- and advent of blogs and social technology

tools revolutionizes governance processes, demanding greater openness, transparency, accountability, integrity and responsibility

These phenomenal growths are poised to proliferate ubiquitously and pervasively in tandem with cost reduction and improved service level quality in the provision of high speed broadband technology. As per Malaysian official statistics, cellular phone subscriptions had overtaken fixed line DEL connections in 2000 when residential subscriptions began to register a decline. A decade later, that is since 2010, fixed line business subscriptions have also stagnated. The Internet dial-up subscriptions that commenced in r 1998 also came to a standstill in 2008 and thereafter due to the increase in broadband technology that marked its beginning in 2002. In the broadband technology segment, the market is heading for another point of inflexion where mobile broadband technology is poised to overtake fixed line broadband technology. In tandem, businesses are projected to embrace mobile broadband technology that provides much bigger scope and coverage for "anywhere", "anytime" and "anyone" modes of services in comparison to what fixed line broadband technology can offer.

Within national borders, public sectors are increasingly experiencing greater citizenry participation especially in the delivery of public goods and services and decision making processes at all levels of administration. Direct engagement of customers and employees in business strategies and operations are increasingly becoming a reality through technology flattening traditional hierarchies, blurring of divisions of responsibility and embracing new work cultures demanded by the technology savvy new workforce. With global connectivity, future businesses are increasingly becoming independent of geography and time constraints, as well as traditions and cultures. Thus, the trade and market liberalization policies that the World Trade Organization (WTO) promulgates, and bilateral and multilateral agreements that Malaysia have duly signed, have begun to shape local businesses either by providing new opportunities or threats. In these evolutionary, sometimes revolutionary governance processes, a number of items warrant due attention for future business continuity and relevance. Among many others, the key critical items are mobility and agility which are poised to have the following profound impact, as follows:

- technology adoption and adaption;
- institutional or organizational realignment and responsiveness towards change;
- citizenry empowerment in public policy and programme formulation and implementation;
- service level quality and customer satisfaction in businesses;
- user and employee engagements in change management, organizational process and quality improvements including waste mitigation;
- product and process innovation;
- intellectual property rights and commercialization strategy;
- analytics and business intelligence institutionalization; and
- market, business and trade development intricacy and efficacy.

The risk is that businesses may become obsolete or irrelevant if there is complacency and a lack of responsiveness to emerging demands. As witnessed, some traditional businesses, tools and services like the postal system, landlines, typewriters and travel agencies went bust after failing to respond effectively to the onslaught of new age technologies that evidently revolutionized all spheres of life. Once again, businesses are at a crossroads in embracing and harnessing elements of mobility in their businesses - which need to be monitored, measured and evaluated, and more so, prescribed with way-forward strategies. Among many other models,

as shown in Box 1, the IDC Mobility Framework provides a methodology for gauging business agility that has become imperative for future survival and growth.

SECURITY

The Internet of Things (IoT) is the term that refers to internet-connected devices from fitness wristbands to connected cars. But once fully connected, the pertinent question emerges as to who is responsible for the data governance, especially the flow of data between linked-up devices, service providers and more importantly, the ultimate user. Application Programming Interfaces or API is an essential component of the IoT system architecture, providing the requisite connections and allowing devices to speak to each other. With the fast emergence of IoT, the APIs are everywhere such as when a fitness wristband sends jogging-related signals like time, date, calorie consumed, body temperature, heart beat et cetera to a website; or when one remotely unlocks a car with a mobile application or monitor all the physical happenings in a smart home from office or change the temperature in office using thermostat. The IoT revolution on a much larger scale is bound to hit with greater benefits through increased connectivity and wireless remote controls. Indeed, API is not a new terminology to the technology sector but what is new is its ubiquity and pervasiveness in devices and wearable items. With the increasing levels of personal data flying around the internet, and now between devices, security is a greater cause for concern. Thus, these APIs must be managed and secured so that they are not prone to attack.

Aside from issues of ownership, there are problems in determining who is responsible for ensuring that it arrives safely where it's needed, without interruption. Recognizing the significance of Information of Things, some countries like the UK has set up an Information Commissioner's Office (ICO). Every organization processing personal data is required to register with the ICO and take responsibility for ensuring that the data remains private. CIOs admit that the Data Protection Act (DPA) 1998 is out of touch with the technological times. So enterprises buying into the IoT need to implement stringent API management systems from the offset to ensure that the flow of data is not interrupted on its journey between devices. As everyday objects become data transmitters, their developers become responsible for governing this flow of data. There are three key elements to be taken into account, the cornerstone being visibility. First, businesses need to know where their data is at all times which demand business intelligence and security analytics capability; the second, aspect is security, ensuring the data is protected by the right authentication protocols and data protection acts; and the third is community management.

ANALYTICS

Companies trying to understand their business using analytics is not a new practice. What is new then? Its form and shades have evolved into a multi-disciplinary subject entailing not only traditional statistical analysis but also computing, operations research and business elements. Analytics has its beginnings in the sixties with the emergence of data support system (DSS) by IBM, which by the late 80's had evolved into online analytic processing (OLAP) applications. Indeed, OLAP marked the beginning of Business Intelligence Analytics (BIA) models providing fact-based decision making and planning processes. The legacy BIA models are essentially confined to data processing activities pertaining to organizational operations and processes that are driven by Enterprise Resource Planning (ERP), Customer Relationship Manager (CRM) and Supply Chain Management (SCM) types of systems. Today, the essence and philosophical notion of analytics still very much remains the

same, that is, discovering and communicating meaningful patterns in data. But the roles and the rules, the processes and the procedures as well as data governance have changed. Unlike the legacy models where business intelligence is culled from structured databases, today's technological sophistication and advancements in programming skills allow analysis on semi-structured data like web streams and unstructured databases using various analytics techniques and capabilities such as text analytics, context analytics, speech analytics, predictive analytics, prescriptive analytics, text and web analytics (CIPD, 2013; Gudipathi et al, 2013). Not only is data within organizations integrated and explored, but it is also linked to meaningful and relevant external sources such as web-based postings, blog spots, You Tube videos, Facebook posts, sensors of various types, call centres et cetera that are truly revolutionary in expanding data scope and coverage. Contemporary analytics often favours data visualization to communicate business insights. New technology adoption like Apache Hadoop, NoSQL, R and Google Analytics support the open source culture, which admittedly drives down the operational cost and provides ease of data governance that are typically the opposite in the case of proprietary software business arrangements. With tremendous cost reduction, it is anticipated that even small and medium-sized enterprises can leverage the emerging BIA opportunities. More importantly, from the people perspective, contemporary analytics reorientate work cultures and practices by directly engaging customers and employees by reducing and flattening organizational hierarchies and eliminating unwarranted divisions of responsibilities. In traditional BIA practices, business intelligence reports, typically statistical in nature, are produced only for top-management purview, but today with the ease of data visualization and infographics techniques, even employees and customers are given access. Consequently, employee motivation and responsiveness in business performance and customer satisfaction tend to increase. Indeed, greater engagement of employees and customers in the production and delivery of goods and services are critical for realizing improvements in processes and quality and also for discovering new products and services through innovation, research and development practices.

Today, there is much more data around. Its volume is ever expanding. It's getting faster and spreading everywhere. It is available through more channels and devices. As highlighted earlier, it integrates the structured or semi-structured or unstructured database across organizations (intra-linkages) and between organizations (inter-linkages). The integration process is increasingly becoming a nightmare technologically for IT departments. For strategic planners and decision makers, contemporary analytics pose a formidable challenge for culling values that can support business, market, trade and investment growth, andis poised to be the next frontier for innovation, competition and productivity. Such phenomenal growth is simply attributed to the advent of Internet technology followed by intense virtual digitization processes that lead to the proliferation of data. Additionally, the pressing need to stay ahead of the competition has sharpened organizations' focus, and indeed, has raised the need to use analytics within organizations. As such, organizations that have BIA already are repositioning business intelligence activity as big data analytics (BDATaking into consideration the continuous reduction in cost and increasing ease in deployment, many organizations including SMEs are jumping on the BDA bandwagon. Succinctly put, BDA comes with volume, velocity, variety and value. Internet of Things (IoT) driving Information of Things (IOT) is poised to continuously flood the business environment with much more bigger and real-time data.

Volume simply depicts the amount of data, which at the moment has no distinct criterion

or cut-off value for defining big data. However, they are measured in terms of petabytes, zetabytes, exabytes, yottabytes. The variety of data entails the complexity of data types and data sources (CIPD, 2013; Gudipathi et al, 2013). Velocity depicts the data in motion, in particularly the rate at which data is created, processed, analyzed and disseminated. With technological advancements, the latency speed - that is, the lag between the creation of data and the conversion to meaningful information or knowledge - is becoming shorter and it matters for business growth and competition. Veracity dimensions deal with data quality, integrity validity and reliability which are central to any data compilation activity. Value deals with analytics that is supposed to close the gap between data and business needs.

TALENTS

The overarching component in the MSAT framework is talent. Without the right talent, developing the other three components namely mobility, security and analytics will not go far in future business development. Thus, sound talent management is considered key for companies and organizations to reach their business goals and strategic values. Specifically, whom to hire, how to manage people, what motivates performance, rewards that can make people work, retention of staff and customer loyalty, forms an integral part of current talent management science and strategic workforce planning. Given the pace and speed of technological advancements in ICT domains, it has become equally important for human resource practitioners to monitor and evaluate the relevance of current jobs in the industry. What was relevant in the past like Cobol programmers is no longer of any pertinence today and similarly what is relevant today may not be in the future job market. Some of the job functions need to be modified or redefined to meet future demands. Figure 3 highlights the current hot ICT jobs by area of applications (PIKOM, 2014).

For instance in the past, smaller businesses used Microsoft's Excel spreadsheets to manage everything from finances to payroll. But as these businesses grew into large companies, they purchased custom on-premise software from Oracle and SAP to help scale up operations. But the rise of cloud computing - storing data in remote servers over the Internet - has challenged those industry giants because companies increasingly demand software that offers flexibility and lower IT costs. Cloud-based data does not require companies to purchase and house big servers and employ in-house technicians to maintain the machines. Gartner has predicted that by 2018, at least 30 percent of service-centric companies will

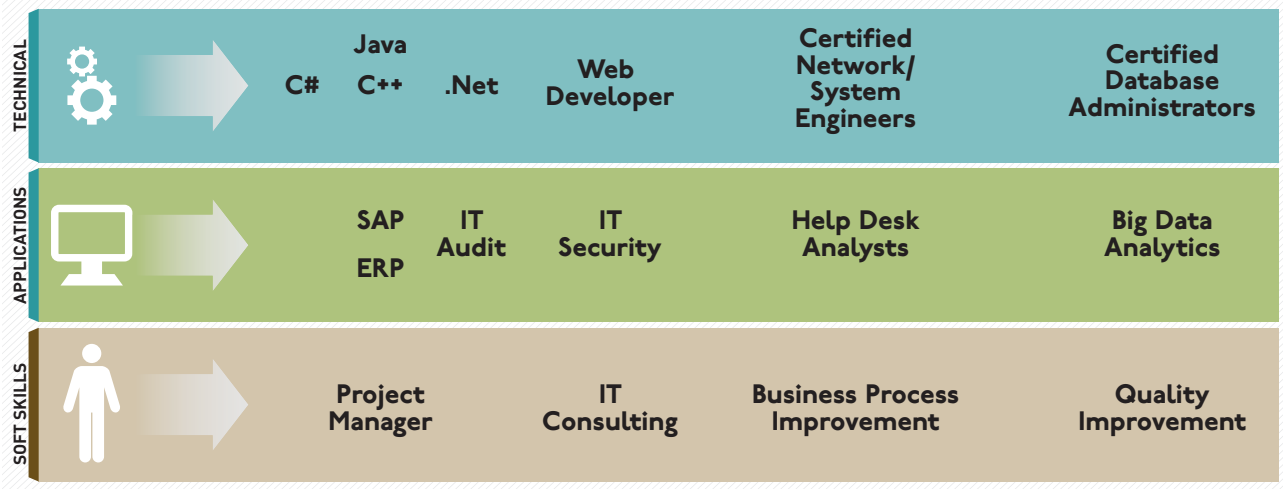


Figure 3: Hot ICT Jobs by Area of Applications

move the majority of their needs to the cloud, thus posing challenges to the relevance of proprietary based SAP or ERP jobs.

The soft skills jobs such as project management, process and quality improvement are likely to undergo limited variations with technological evolution. However, in the technical and application sides, more changes in the job functions are anticipated. As it is now, three areas of disciplines namely wireless engineering, security analytics and big data analytics are sought after for effective implementation of the MSAT framework. Wireless engineering that duly addresses the design and application may not be a new discipline, but over the years with the invention of the FM Radio in 1935, wireless engineering has evolved to provide a wide spectrum of applications, most notably cellular networks. Specifically, mobile data traffic has led to a plethora of new devices (e.g. iPhone, smart phones and tablets) and new applications (e.g. YouTube, Facebook, social networking, machine to machine communication, video conferencing and immersive communication). With emergence of IoT and IOT in particular, mobile video is forecasted to be one of the main drivers behind the current and predicted traffic growth by a factor of thirty over the next ten years. In tandem, the demand for security analysts is also expected to rise significantly with increasing hacking and data breaching activities. As such, information security analysts have to stay one step ahead of cyber attackers in order to protect the computer networks of a company or government agency. Security analysts focus on three main areas: risk assessment (identifying problems an organization might face), vulnerability assessment (determining an organization's weaknesses) and defense planning (installing protections such as firewalls and data encryption programs). With IoT driving IOT, the role of data science that entails extraction of knowledge and business intelligence from raw data, is gaining ground in the BDA environment. In comparison to traditional statisticians and analysts, data scientists are generally expected to be equipped with inter-disciplinary knowledge entailing mathematics, statistics and business knowledge, besides computing science. So that they have the ability to find and interpret rich data sources, manage large amounts of data despite hardware, software and bandwidth constraints, merge data sources together, ensure consistency of data-sets, create visualizations to aid in understanding data, build mathematical models using the data, present and communicate the data insights/findings to specialists and scientists in their team and if required, to a non-expert audience.

CONCLUSION

To implement the MSAT Framework, the potential starting point is to first define the big business objective and insights before proceeding to identifying those pieces of data needed for answers. In defining the business objectives and direction, a number of factors warrant due attention: organization-wide policy implementation; aspirations of customer focus; readiness of employees; adequate resources; employing skilled and competent workforce; human resource practitioners equipped with talent analytics; multi-disciplinary team; monitor, measure and evaluation model practices; continuous process and quality improvement strategies; and instituting change management programme.

REFERENCES

1. Aarts, Emile; Harwig, Rick; Schuurmans, Martin (2001), chapter "Ambient Intelligence" in The Invisible Future: The Seamless Integration Of Technology Into Everyday Life, McGraw-Hill Companies.
2. ABI Research, 2013 . More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020, ABI Research
3. Bersin, J, 2013. Big Data in Human Resources: Talent Analytics Comes of Age. (http://www.forbes.com/)
4. Beyer, Mark (2011) "Gartner Says Solving 'Big Data' Challenge Involves More Than Just Managing Volumes of Data". Gartner
5. Carlton, Darryl (2012). The Nexus of Forces: Social, Mobile, Cloud and Information. Gartner Research.
6. CIPD, (2013). Talent analytics and big data – the challenge for HR. Chartered Institute of Personal and Development (CIPD)/ Oracle Research Report. Gudipati M., Rao, Shanthi, Mohan, N. D. and Gajja, N. K. (2013). Big Data: Testing Approach to Overcome Quality challenges. Infosys Labs Briefings Vol.11 No1
7. Gartner, 2014 "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020". Gartner. 2013-12-12. Retrieved 2014-01-02.
8. Greer, Chris (2014). The Internet's Next Big Idea : Connecting People, Information and Things. National Institute of Standards and Technology. Commerce. Gov. United States of Commerce.
9. IBM, (2013) "IBM What is big data? — Bringing big data to the enterprise". www.ibm.com. Retrieved 2013-08-26.
10. PIKOM, 2014. ICT Job Market Outlook . Annual series published by PIKOM.

CHAPTER 3

LEVERAGING UPON PRIVATE SECTOR BIG DATA: INFORMATION COMMUNICATIONS TECHNOLOGY (ICT) PROFESSIONALS SALARY PERSPECTIVE

ONG KIAN YEW
Executive Director
oky@pikom.org.my

RAMACHANDRAN RAMASAMY
Head of Policy, Capability and Research
ramachan@pikom.org.my

The National ICT Association of Malaysia

PIKOM

I. INTRODUCTION

This paper attempts to depict a practical scenario where big data generated by the private sector can be sourced or tapped upon for the interest and use by both the business community as well as government officials. In the business world, the growing notion is that as the future unfolds, more business decisions will be supported by the facts that only analytics can provide; as such fewer business decisions will be made on the basis of instinct and guesswork in the near future (Martin Hilbert, 2013; Davenport and Harris, 2007).

Recognising the relevance, business organisations are increasingly leveraging upon big data from various sources at an astounding rate. Big data analytics (BDA) helps organisations by not only collecting, organising and analysing patterns and trends residing in large data sets, but also directs in discovering the data that are most important to the business and future business decisions (Evelson, 2010).

Indeed, BDA processes are pervading into business organisations of all sizes and types at an unprecedented rate in the history of analytics (CDW, 2013), though participation of bigger organizations are more pronounced at the moment. Government organisations and non- profit organisations have also geared up to take advantage of whatever opportunities BDA may offer.

This exercise aims to explore and explain the evolutionary process involved in gleaning the public policies relevant in preparing the salary profile of information communications technology (ICT) professionals in Malaysia. by the National ICT Association of Malaysia, popularly known as PIKOM. PIKOM does not own any salary profile database of ICT professionals but it has successfully instituted an arrangement with online job service providers to provide the requisite data annually (PIKOM, 2014). This paper elucidates the governance process, scope, coverage and analytical mechanisms as well as information dissemination and interpretation that are typically found in official statistics environment but viewing it in the context of big data phenomena.

2. DATA COMPILATION GOVERNANCE, SCOPE AND COVERAGE

Even before the term “big data” became a working language in the Malaysian ICT industry, in 2006 PIKOM collaborated with JobStreet.com to generate annual series on salary profile of ICT professionals in Malaysia. Jobstreet.com is a leading online recruitment company, presently covering the employment markets in Malaysia, Singapore, Philippines, Indonesia, India, Japan, Thailand and Vietnam.

The Group currently services over 230,000 corporate customers and over 13 million jobseekers in its database providing online recruitment services for all categories of jobseekers, from fresh jobseekers after graduation to senior level positions. In Malaysia, alone 2.3 million jobseekers have registered in Jobstreet.com. Of the overall total in 2013, IT or the computer segment constituted 8% of its database; with 84% having post-secondary qualifications ie diploma, degree, professional certifications and post graduate qualifications ; and 82% being non-executive job seekers entailing fresh graduates, junior, senior, managerial and senior managerial category.

Initially the collaboration with Jobstreet.com aimed at compiling and publishing only basic data pertaining to the average salary of ICT professionals, by job category and industry. The job category entailed junior ICT executive with fewer than 4 years of experience, senior ICT executive with 5 years and above of working

experience, middle ICT manager and senior ICT manager.

Subsequently, the scope and coverage expanded to incorporate salary data of fresh graduates provided by industry break down, top ICT paying industries, ICT industry segments namely ICT hardware, ICT software and call centre including ICT Enabled Service, ICT user and ICT producer segments. Since 2012, the coverage further expanded to provide median salary by type of ICT job functions, employment size, years of working experience, geographical location and gender but using PayScale.com web published records.

Wherever possible, benchmark scaling numbers are also compiled and published. The scaling numbers are obtained by comparing the median salary in the lowest paid category against other categories by assuming one for the lowest level. Such benchmarks are compiled for years of working experience, employment size and geographical location categories as well as regional benchmarking.

Since 2012, PayScale.com web records have been used for compiling regional benchmark statistics. In this compilation, Malaysia assumes a scaling factor of one. All measures are tallied in US dollars. The average salary value for each country is obtained by averaging across three variables namely IT skills, company size and years of working experience. The benchmarks are published by Atlas criterion and purchasing power parity (PPP) adjusted criterion. PPP is considered a more refined measure as it provides a more meaningful comparison by taking into account of inflation rates and foreign exchange rates. Indeed, technically speaking ambitious job seekers should use PPP adjusted scaling numbers when searching for overseas jobs.

Selected Asian and English speaking countries, where the Malaysian ICT professionals have higher tendency to head for in search of better employment opportunities and career advancements are considered. The Asian countries include Singapore, Indonesia, Thailand, Philippines, Vietnam, Hong Kong, India and China and English speaking destinations include USA, Australia, United Kingdom, Canada and New Zealand.

Moreover, these countries have strong and long established diplomatic, trade and cultural ties with Malaysia. Being English is a popular lingua franca among Malaysian businesses especially among the private sector and thus, there has been always a natural attraction for Malaysians to do more businesses with such English speaking countries, despite distance in some cases. Indeed, these destinations are no exception to ICT professionals as well, especially software developers and networking engineers who are in demand at all times globally.

3. BIG DATA ANALYTICS (BDA) MIGRATORY FRAMEWORK

As data history cites, big data is not a new phenomenon. It started seventy years ago when first attempts were made to quantify the growth rate in the volume of data (Luhn, 1958) or what has popularly been known as the “information explosion” (a term first used in 1941, according to the Oxford English Dictionary), before current buzz around big data emerged. Sixties saw emergence of data support system (DSS) by IBM, which by late 80’s evolved into online analytic processing (OLAP) applications. Indeed, OLAP marked the beginning of BIA models ingrained with fact-based decision making and planning processes (Pieter M, 2008; Power, D.J., 2010).

The legacy BIA models essentially confine data processing activities pertaining to organizational operations and processes that are driven by Enterprise Resource Planning (ERP), Customer Relationship Manager (CRM)

and Supply Chain Management (SCM) types of systems (Aberdeen Group, 2013). With the advent of Internet technology followed by intense virtual digitization processes new types of big and real-time data have begun to flood business environment (Rainie & Wellman, 2012; Snijders et al, 2012).

Consequently, unprecedented advancements in data recording and storage technology the traditional BIA systems are compelled to adopt BDA systems. The anticipated changes in the process dimensions and framework include integration of various departmental data within organization; expansion of new data sources through linking to external databases; new technology adoption especially open source culture; changing roles, systems, structures, functionality, cultures and practices in work environment and orientating to customer aspirations, expectations and experiences and responsive to businesses and employee motivations (Miele and Shockley, 2013; CDW, 2013).

BIA and BDA systems have common objectives of culling out actionable insights and business intelligence from the data (Martin Hilbert 2013; CDW, 2013 Evelson, 2010)). However, as highlighted in Figure 1, there are some distinct characteristics differences if one were to look at how data supported systems of yester years have evolved into BDA of today especially in comparison against BIA. First, BIA confined to structured back-office systems data, in comparison BDA explores, semi-structured and unstructured data sourced from within and outside organizations, besides binary database. Specifically, newer sources include unstructured text from comments and social media streams and semi-structured data from log files and click streams, besides the rectangular array structured traditional databases (Miele and Shockley, 2013; CIPD, 2013; Gudipathi et al, 2013.

Web based postings, blog spots, You Tube videos, Facebook posts, sensors of various types, call centres, credit card and online payment transactions and store inventories have emerged as key sources on big data. Second, the legacy BIA is technology centric, demands heavy IT involvement like usage of Structured Query Language (SQL) for querying (CDW, 2013), whereas BDA deploys user-friendly interfaces. Third, BDA processes have gone beyond the realms of typical numerical based statistical analysis by encompassing text analytics, context analytics, speech analytics, predictive analytics, prescriptive analytics and embedded analytics (BDA) (TATA, 2012; Gudipathi et al, 2013). Fourth, BIA generates reports and dashboard visualizations for top management review to facilitate top-down driven actions only, while BDA targets customers and employees at all levels and promulgates flow of constructive criticisms and feedback that can improve process, quality and innovation (Evelson, 2010).

Fifth, BDA deploys open source solutions like Apache Hadoop, NoSQL, R and Google Analytics that drives down cost significantly in comparison to costly proprietary software used in BIA models (Bertolucci, Jeff . 2013). Sixth, being business BDA budgeting requirements are moving away from IT to business team. As such, organizations are reinventing themselves by defining BDA as an integral part of seamless workflows across organizations. Ease of use features and characteristics enables effective data usage and institutionalization of actionable insights at all levels of operations and planning processes. Surmising the whole phenomena, IBM has succinctly differentiated and qualified the upheavals that physical size of the organization or the data set is irrelevant in defining a “big data”; rather as “any data set that cannot be managed by traditional processes or tools” (Miele and Shockley, 2013).

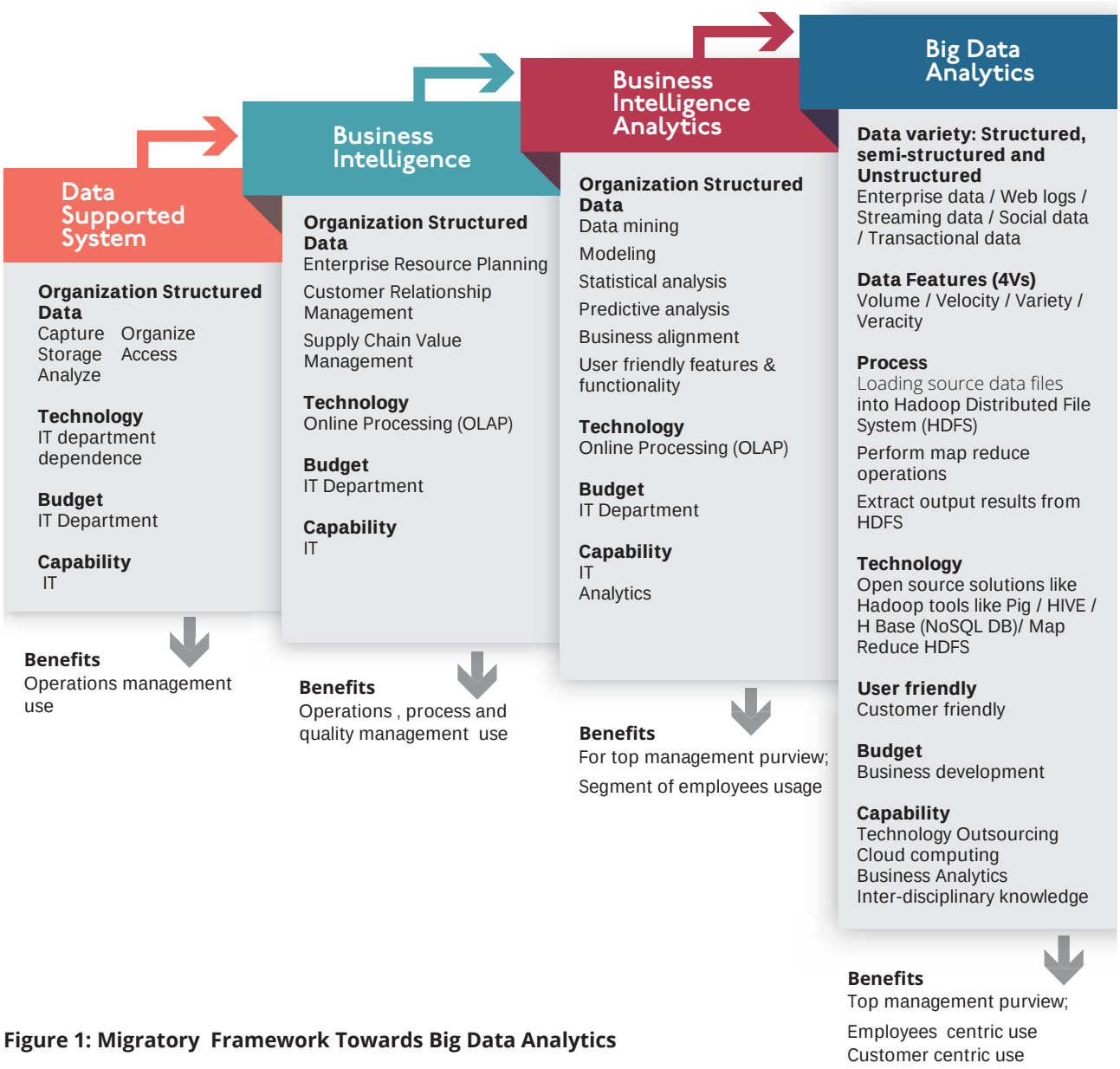


Figure 1: Migratory Framework Towards Big Data Analytics

BIG DATA EVALUATION FRAMEWORK

Business organizations are at various stages of development (Nandyal, 2011). Some organizations plan and carry out business operations by intuition and guesswork as they fear over analysis can paralyse their business performance. Some organizations use only basic data supported system that can generate essential business numbers and help to improve day to day business operations efficiently. Some matured organizations are not only pursuing performance efficiency but also business effectiveness by exploring new frontiers in research and development, creativity and innovation strategies. Such matured organizations are deemed to embrace and adopt BDA culture and practices. As highlighted in Figure 1, having evolved into a distinct work practice and culture, the necessity for an evaluation framework on BDA has become an imperative, in particular for assessing and asserting presence of big data elements.

A decade ago, Gartner described the challenge of big data in terms of 3 'V's – volume, velocity and variety (Laney, 2001; McAfee and

Brynjolffson, 2012), while IBM viewed it under four "V"s (4V) namely volume, velocity, variety, and veracity (Miele and Shockley, R, 2012); see Figure 2. In depicting big data talent analytics phenomena the Chartered Institute of personal and Development (CIPD) also mooted 4 Vs but differently entailing volume, velocity, variety and value dimensions (CIPD, 2013). Reckoning the significance and relevance of all the 'V's, this paper provides a consolidated Five V Big Data Model Framework, as shown in Figure 2. This framework is used for assessing the features and characteristics of big data phenomenon embedded in the ICT salary profile compilation initiative. The framework is also used for identifying the gaps that need to be rectified in realizing a full-fledged BDA in the near future.

Volume simply depicts the amount of data, which is continuously growing at an unprecedented rate (Miele and Shockley, 2013; CIPD, 2013; Gudipathi et al, 2013). There is no distinct criterion or cut-off value in terms of petabytes and zetabytes for determining volume of a big data set (IBM, 2013). High volume today will be higher volume tomorrow (Miele and Shockley, 2013). In the case study considered above the Jobstreet.com currently servicing over 50,000 corporate customers and over 6 million jobseekers regionally and another 3000 paying business customers under PayScale.com globally, more so the institutional arrangements and processes deployed indicate the features and characteristics of big data. The volume is poised to increase many folds when external data and unstructured online data are sourced.

Variety of data entails the complexity of data types and data sources (Miele and Shockley, 2013; CIPD, 2013; Gudipathi et al, 2013). In typical BDA activity the data comes not only in the structured form in the form of rectangular array or matrix format but also in the form of non-traditional particularly, semi-structured data from log files and click streams or unstructured text from comments and social media streams (CDW, 2013; CIPD, 2013). Such non-traditional data are residing in sensors, smart devises and social technology tools and infrastructure, both within and outside organizations. When organization extract untapped value from such data sources enormous knowledge convertible into intelligence and benefits can be realized (IBM,2014). Like in any online system, Jobstreet.com and PayScale.com too are endowed with data in the form of text, web, tweets, audio, video, click streams and log files that yet to be explored.

Velocity is indeed depicts the data in motion, in particularly the rate at which data is created, processed, analyzed and disseminated ((Miele and Shockley, 2013; CIPD, 2013; Gudipathi et al, 2013)). With technological advancements the latency speed, that is, the lag between data is created and being converted into meaningful information or knowledge is becoming shorter (Miele and Shockley, 2013). Jobstreet.com and PayScale.com have institutionalized online schemes for updating job registrants and job provision profiles, which yet to be explored to increase latency speed and report frequency; current arrangement is to produce annual report.

Veracity dimensions deals with validity and reliability aspects in data compilation (Miele and Shockley, 2013; Oracle, 2012). Data quality and statistical integrity have been an age old concern in any measurement procedure and quantitative analysis (Gudipati et al, 2013) and BDA is not an exception. Issues are of concerns in BDA authentication are include exactitude, genuineness, originality, legitimacy, legality, rightfulness, dependability, authoritativeness, credibility, factualness, trustworthiness, historicity and bona fides. Lack of data veracity bound to have far reaching negative implications on data analyses including predictive exercises. In the current ICT salary

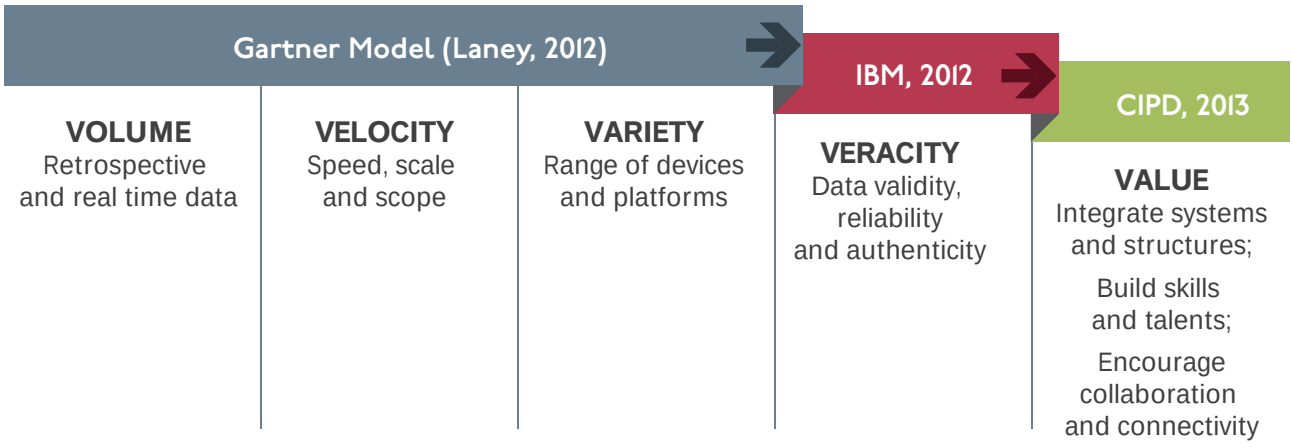


Figure 2: Integrated Five V Big Data Dimensions

compilation arrangement Jobstreet.com provides first level validity and reliability before supplying the data to the industry association. As a data user the industry association on its part also undertakes basic equivalence, stability and consistency checks that any typical statistical procedure demands (Gudipati, 2013). However, data veracity tasks will be more challenging when internal and external databases are linked and integrated as typically envisaged in BDA (Gudipathi, et al, 2013).

The challenges include validating structured and unstructured data, data storage and executing map reduce process using Hadoop technology and complex Pig and Hive programmes (Bertolucci, Jeff. 2013). Besides functional testing, non-functional validation such as harmonizing differences in technological standards and settings, interoperability mechanisms, process scalability elements, work culture and processes, and institutional rules and regulations as well as conformance to service level agreement (SLA) warrant due attention.

Value deals with analytics that purposed to close the gap between data and business needs (CIPD, 2013; Snijders et al, 2012; Bayer, 2011; Lavlle, 2011). This requires understanding and mitigating obstacles in systems and structures in support of data and evidence driven approach (Boja, C; Pocovnicu, A; Bătăgan, L., 2012); developing the skills, smarts and talent pools; and encouraging internal collaboration and connectedness among departments with the idea of data and information as a key part of transformational tool kit (CIPD, 2013; Oracle, 2012). In the current on-going ICT salary compilation exercise it may not entail the element of on-the-fly-decisions (CDW, 2013) but fostered and nurtured cooperation, collaboration, trust and confidence between the online service providers and the industry association. Currently, the report serves as a source document for remuneration adjustments, career structuring and policy advocacy. Indeed, such alliance is critical for any future endeavour in enhancing business relevance, improving operations, performance and innovation.

BUSINESS AND POLICY PERSPECTIVES OF KEY DATA HIGHLIGHTS

For illustration purposes this paper publishes only key data highlights on average salary of ICT professionals, by job category, ICT job functions, employment size and geographical location as well as regional benchmarking data in comparative form. Initially, these data were published for the benefit of ICT

producer and user industries especially for those human resource practitioners who are involved in recruitment exercises and salary adjustment decision making processes. But, over the years the ICT salary records attracted the attention of public policy makers in the mainstream who are, in particular involved in formulating, planning and implementing ICT programmes that envisaged in driving innovation driven economy through ICT led strategy that the Government of Malaysia has been promulgating since the initiation of New Economy Model (NEM) in 2010.

SALARY GROWTH RATE

The Table 1 shows the average monthly salary of ICT professionals in Malaysia. From business perspective the salary trend for ICT professionals, registering an annual average growth rate of 8.5% during the period 2006-2013, has been very encouraging at least for two reasons. Firstly, the average annual growth rate (AAGR) is well above the national inflation rate that fluctuated between the lowest rate of 0.6% in 2006 and the highest rate of 5.8% in 2008 during the period. The highest inflation rate occurred in 2008 when the oil prices in the global market skyrocketed and brought about adverse effects on the prices of consumer goods and services. Another reason is the fact that the average salary of ICT professionals is well above average household income at national level, though not strictly comparable in terms of scope and coverage, as shown in Table 1. The Figure 1 also has highlighted that the rate of average salary growth of ICT professionals is at 8.5% per annum level, which is much higher than rate of average growth of household income that is growing at 6.3%, thus indicating the gap is getting wider.

SALARY GAP

Despite overall growth in average salary, as shown in Table 2 the gap among ICT job category has been widening as observed during the period (2011-2013). This particular piece of information has signalled the industry players that appropriate measures are needed to reduce the gap. Otherwise, the industry will continue to face rampant job hopping problem among lower category ICT professionals in search of better opportunities and career advancement. In the job tight environment in Malaysia where the unemployment rate has been low over the past two decades, lingering around at 3%, job hopping pose instability to the industry growth. For the employee job hopping may provide wide exposure and experience across many industries and different size companies as well as provide

Year	Average salary of ICT Professionals (Ringgit Malaysia)	ICT Salary Growth rate (%)	Average Household Income (Ringgit Malaysia	Household Income Growth Rate (%)	Average Inflation Rate (%)
2006	4,184	-	-	-	3.8
2007	4,443	6.2	3,686	-	2.0
2008	4,807	8.2	3,854	4.6	5.4
2009	5,200	8.2	4,025	4.4	3.5
2010	5,714	9.9	4,352	8.1	1.7
2011	6,165	7.9	4,657	7.0	3.2
2012	6,673	8.3	5,000	7.4	2.1
2013	7,152	7.2	-	-	3.2
AAGR (%)	8.5%		6.3%		

Table 1: Salary Profile of ICT Professionals, National Household Income and Average Inflation Rate, 2006-2013
Source: ICT Job Market Outlook 2014, PIKOM

Year	Fresh Graduates (Entry Level)	Junior Executive: (1-4 Years Working Experience)	Senior Executive: (≥ 5 Years Working Experience)	Middle Management: (Manager)	Senior Management: (Senior Manager)
			Ringgit Malaysia (RM)		
2010	-	2,936	4,514	7,005	10,795
2011	2,238	3,151	5,039	7,837	12,166
2012	2,343	3,205	5,344	8,381	13,446
2013	2,451	3,439	5,744	8,986	14,738
Percentage Change (%): 2012 - 2013	4.6	7.3	7.5	7.2	9.6
			Benchmarking Against Average Monthly Salary of Fresh Graduates		
2011	1.11	1.57	2.51	3.90	6.05
2012	1.16	1.59	2.66	4.17	6.68
2013	1.22	1.71	2.85	4.46	7.32

Table 2: Average Monthly Salary of ICT Professionals by Job Category : 2010-2013
Source: ICT Job Market Outlook 2014, PIKOM

greater access to information and resourceful networks.

But from the employers' and investors' perspectives, workforce disruptions can cost businesses millions in lost productivity. It is always a costly and time consuming process for employers recruiting, courting, hiring and ramping up new employee in an attempt to provide stable employment, instil staff loyalty and long term retention. From policy perspective widening salary gap widens the societal disparity that public policy always attempts to redress to avert unduly dissatisfaction citizens.

JOB FUNCTIONS

The average monthly salary earned by key ICT professionals is shown in Table 3. It can be seen from this table that ICT professionals in the management category, whether they are Java, HTML, SQL or MCP certified, netted the highest earnings compared to other ICT job functions. IT Project Managers could net a median monthly salary as high as RM8,947 in 2013, which is 24.9% higher compared to RM7,165 in 2012.

Being a highly specialized job, the average monthly salary earned by SAP Consultants in 2013 was RM7,817, which marginally increased by 2% from RM7,647 in 2012; however, experienced ones can net double this amount. Those in the technical line especially the software engineers, Senior Software Engineers and Programmer and System Analysts too registered significant growth in median salary by 31.8%, 19.4% and 16.5% respectively. From both business and public policy perspective the salary records by job functions seem to indicate that non-technical type of functions are paid better their counterparts in technical fields.

Indeed, the finding contravenes the Government aspiration of increasing the knowledge workers pool. Knowledge workers especially those specialize in technology driven creativity and innovation are considered critical for ushering the nation into innovation based economy. The Government also has made a clarion call to accord due employment status and recognition by offering better remunerations, perks and accreditations as well as motivations.

Job Function	2013	2012	% Change
Information Technology, Project Manager (Java, HTML, SQL, Microsoft Certified Professionals)	8,947	7,165	24.9
SAP Consultants	7,817	7,647	2.2
Senior Database / System Administrators (Microsoft and Cisco Certified)	7,580	6,867	10.4
Information Technology Consultants (Java, HTML, MCP...)	6,967	6,920	0.7
Senior Software Engineer (Java, HTML, SQL, Microsoft Certified Professionals)	6,956	5,973	16.5
Database / System Administrators ? SQL (Microsoft and Cisco Certified)	5,044	4,327	16.6
Programmer / System Analyst (Java, HTML, SQL)	4,099	3,432	19.4
Software Developer / Programmer (Java, HTML, SQL)	4,034	3,778	6.8
Software Engineer (Java, HTML, SQL, Microsoft Certified Professionals)	3,459	2,997	31.8
AutoCAD: Civil Engineering	3,459	3,419	1.2
Web designer, HTML	3,173	2,773	14.4

Table 3: Average Monthly Salary of ICT Professionals by Job Function
Source: ICT Job Market Outlook 2014, PIKOM

JOB MOBILITY WITHIN THE COUNTRY

According to PIKOM's past findings, only 10% of the new entrants to the workforce is directly employable, while others need to be trained before placing in proper routines. Companies especially the smaller ones are not willing to mobilize their scarce resources in training or coaching or mentoring activities in fear of rampant job hopping behaviours among new recruits. According to the ICT salary report, the big companies having employment size more than 2000 on an average pay 1.78 times higher than small companies having less than 10 employees. When the data was investigated in terms of geographical location the average salary of ICT employees in highly urbanized areas like in Kuala Lumpur or Putra Jaya tend to earn 1.75 times higher than in Kuching or Ipoh where investments and business activities are considered lower. As such, there is always a strong tendency among new entrants in job market to move to better paying companies or locations once they have acquired adequate experiences and exposures. As shown in Table, 1 the average salary of fresh graduates grew only at 4.6% per annum compared to 9.6% at senior management level, reflecting poorly on the ICT job market outlook, thus warrants the attention of industry players.

Again from public policy perspective low enumeration, in particular lower rate of growth in average salary for ICT fresh graduates is also can bring about negative implications on the supply of right ICT talents in adequate number. In the Malaysian experience, the ICT enrolment in higher learning institutions including both public and private have almost halved from 96,090 in 2002 to 49,731 in 2012. During the 1990's up to the year 2001, there have been a high number of graduates in ICT field attributed to government's policy emphasizing on ICT as driver and enabler of knowledge economy and society especially through the launch of MSC Malaysia flagship applications. More so, the supply was supported with the liberalization of the higher education sector vide Education Act 1995 that fuelled growth of private sector education (ICT Human Capital Development Framework 2012). Subsequently, the decline in ICT enrolment, among many other reasons, is partly due to disillusionment arising from "dotcom bubble burst" in 2000, and partly due to lack of professional recognition and prestige for ICT professionals in comparison

to perceived glamour accorded to medicine, engineering, architecture, legal and accountancy fields.

Gartner study also noted globally declining interest in ICT profession among younger generations due to high technological demands and long and tiring working hours. All these factors in one way or other have gravitated prospective students to pursue other emerging courses especially in health related studies, which in the recent years that the Malaysian Government strongly advocated. In other words, slow growth in average salary for the ICT fresh graduates adds woes to the existing problems and challenges that the industry currently face.

JOB MIGRATION ACROSS BORDERS

The other useful data gleaned from the exercise was benchmarking salary data, which compared the average ICT salary of Malaysian ICT professionals were compared with their counter parts regionally and globally. This piece of information is increasingly becoming important for both industry players who are concerned about employee retention strategy and policy planners who are concerned about talent pool depletion arising from job migration across borders. Specifically, the low remuneration always constituted as push factor for professionals in search of better career opportunities and advancements not only in the region also across distant lands especially those friendly nations that have long diplomatic and trade ties. As reflected in Figure 3 (Atlas criterion) and Figure 4 (Purchasing Power Parity Adjusted) the benchmarking data has revealed that of all countries studied except Indonesia, India and Philippines have emerged as an attractive destination for competent Malaysian ICT workforce and fresh graduates.

The distant lands that become attractive destinations for Malaysians are mostly English speaking countries, in particular United States of America, United Kingdom, Canada, Australia and New Zealand. Since English has been a popular lingua franca among Malaysian businesses especially among the private sector and there has been always a natural attraction for Malaysians to do more businesses with such English-speaking countries. These destinations are no exceptions for ICT Professionals as well, especially software developers and networking engineers who are in demand at all times globally including Malaysia. Indeed, for countries like Malaysia has been a mind boggling task to formulate appropriate talent retention strategy both at industry and country level.

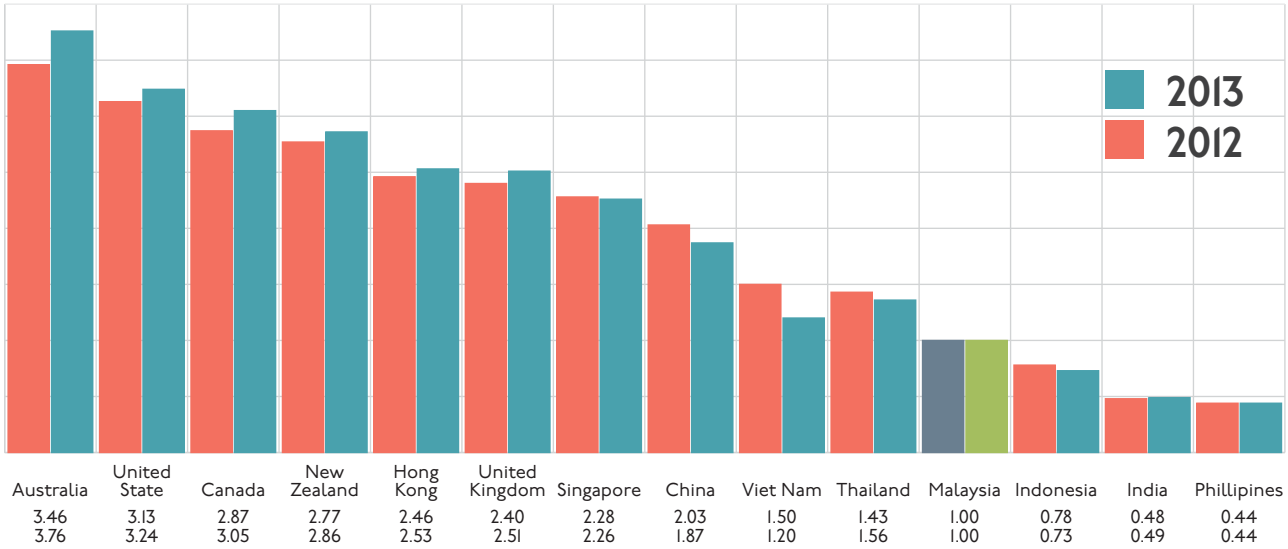


Figure 3: Overall ICT Salary Benchmarking Against Malaysia using Atlas Criterion

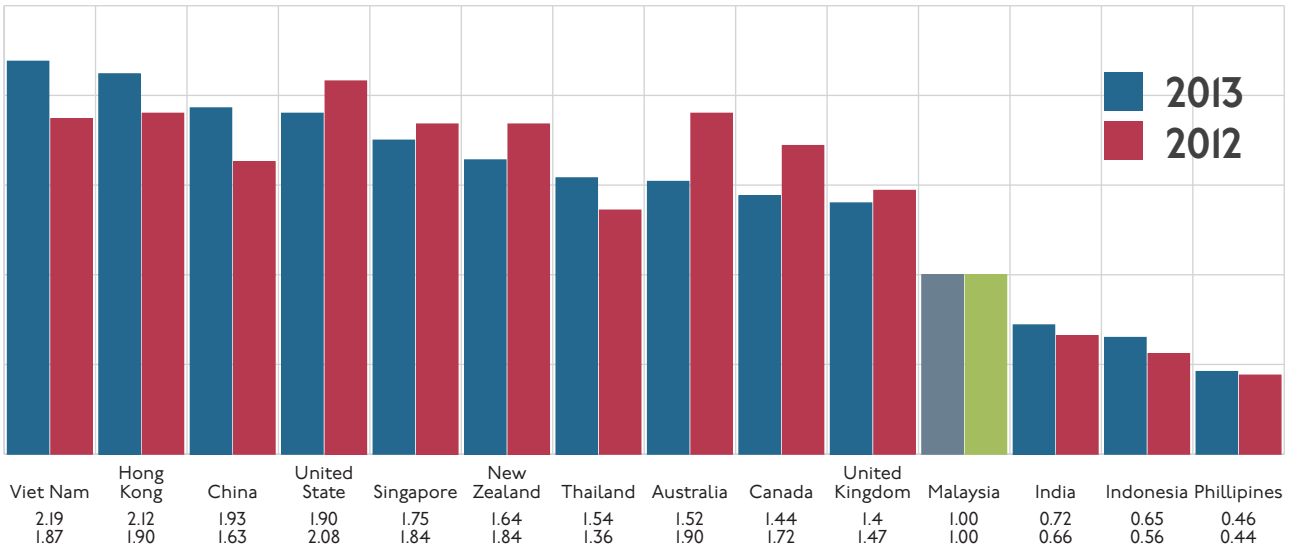


Figure 4: Overall ICT Salary Benchmarking Against Malaysia using Purchasing Power Parity (PPP) Adjusted Criterion

Recognizing the challenge, the Malaysian Government help to address some of the talent gaps in the ICT sector through the TalentCorp institution, which was established in January 2011 (PIKOM, 2013). Since its inception, this institution has implemented three major public policy thrusts. First, is to optimize Malaysian talents through initiatives such as providing career awareness and to work transition and building career guidance, enhancing school platforms on optimise talents. Second, is to attract and facilitate the global trend through programmes such as outreaching to Malaysians abroad, facilitating returning talents and enhancing expatriate facilitation. Third, is building networks of top talent via building networks of future leaders, developing diaspora networking platforms and engaging the expatriate community.

BIG DATA IN OFFICIAL STATISTICS

The big data analytics collaboration between the industry association and online job service providers has brought out a number of distinct features and merits. Firstly, the collaboration fostered a good working relationship, mutual trust and confidence between the online job service providers and industry association.

This relationship model has demonstrated that through appropriate working arrangement, process and mechanism private sector data can be leveraged on generating not only business relevance numbers but also public policy relevant statistics. Secondly, the research collaboration has expanded the role of PIKOM beyond its traditional routines, which entail looking after industry growth and welfare of the members (Kian Yew & Ramachandran, 2012).

PIKOM uses the salary data for policy advocacy and intervention exercise whenever the mainstream Government agencies approach industry associations to provide issues and challenges plaguing the ICT industry. Thirdly, as a consequence of constant policy advocacy and intervention role the mainstream agencies have accorded recognition to various statistics by the industry association, without doubting its methodological integrity, validity and reliability (Kian Yew & Ramachandran, 2012).

Fourth, the ICT salary profile data published by PIKOM annually has gained equivalently "official statistics" status that typically remained the forte of national official statistical agencies. Indeed, PIKOM is the only private sector association admitted as a permanent member in the Digital Economy Satellite Account

(DESA) working group. DESA was established in 2010 as the official statistics database that consolidates and integrates all ICT statistics compiled by various government agencies. In this endeavour the ICT salary profile compiled by PIKOM annually accorded 'near' official statistics status, thus paving the way for other industry associations also to follow suit. Fifth, the inclusion of ICT data as an integral data for the DESA system enhances the national scope and coverage of official statistics, particularly under ICT data domain.

Sixth, and most importantly, the ICT salary profile data complemented the gaps in the national household income data that periodically published by the national statistical agency. Specifically, being a sample survey, the National Household Income Survey is able to provide valid and reliable as well as meaningfully consistent data at one digit level as per depiction in the Malaysian Standard Occupation Classifications 1998 (MASCO 1998). In other words, due to sampling limitations and fluctuations it will not be tenable and meaningful for compiling any data at three digit occupation level.

But, at the one digit occupation level the income data under managerial and professional groups lumps up all kinds of professional jobs such as doctors, lawyers, engineers, legislators, accountants et cetera, including all ICT professionals especially those who have attained tertiary qualifications (Ramachandran and Vigneswarer, 2011). As highlighted in Table 3, the job market outlook study that PIKOM undertakes with online job service providers able to provide average income data earned by ICT professionals by type of job functions.

STATISTICAL INTEGRITY CHALLENGE

As far as business relevance and usage is concerned, the compilation of salary profile of ICT professional has not posed any problem thus far. Contrary to that, it is the market and business driven initiative where cost effective statistical production that is of paramount concern. Moreover, private sectors are in dire need of not only timely statistics but also numbers that can help to project future businesses. On the other hand in the case of official statistics production statistical integrity gauged in terms of quality, validity and reliability warrant due attention and always accorded top priority in any official statistics compilation activity (Wyckoff, 2001; Biggeri, Luigi, 2004; Ramachandran, 2008). As such, the national statistical offices or Government ministries that are routinely involved in the production and dissemination of various statistics implicitly assumes the role of quality function as per aspirations stipulated in the Principle 2 of Fundamental Principles of Official Statistics of UNSD (ISI, 1986; UNSD, 2006).

Specifically, "to retain trust in official statistics, the statistical agencies need to decide according to strictly professional considerations, including scientific principles and professional ethics, on the methods and procedures for the collection, processing, storage and presentation of statistical data". Thus, premising upon these tenets the statistical endeavour undertaken jointly by the industry association and the online job service providers will not be accorded any exception to the statistical demands depicted in the Principle 2 of Fundamental Principles of Official Statistics of UNSD.

If that is so, then the question is how and who can ascertain the quality, validity, reliability and statistical integrity that are critical to safeguard the professionalism and standards of the practice> This is imperative in order to ensure accuracy and consistency across geography and over time; to guarantee statistics that are free from political interference, biasness and skewed interpretation; and towards quality management inclusive of the sound application

of methodology to achieve the desired quality (Biggeri, Luigi 2004; Straf, Miron L., 2003; ISI, 1986; UNSD, 2006).).

Response to these questions and challenges seems to suggest that the role of national statistical office needs to be broadened (Ramachandran, 2003). Their role is not only to confine to the official statistics production and dissemination but also need their proactive involvement is assessing and endorsing the conformity and admission of private sector statistics as official statistics, wherever applicable. This process will help in expanding the scope and coverage of official statistics, particularly when many enterprises are turning big data into valuable information of uncovering inherent business, market, trade, investment and policy trends.

CONCLUSION

Converting private sector data into official statistics may not be that easy. Despite institutional challenges in creating official statistics, the big data exercise is also facing at least two other major challenges at its current infancy stage. First, advanced and predictive analytical skills demand inter-disciplinary technical competencies and knowledge such as programming, cloud computing, mobility and social computing for getting the most value from BDA activities especially projecting anticipated changes using historical and current data (Miele and Shockley, 2013).

Secondly, technologically designing an integrated business intelligence and big data platform can be a logistical and administrative nightmare especially involving external databases and more so ensuring data security, safety and interoperability elements (Jamack, 2012). Nonetheless, BDA is achievable through pragmatic and incremental implementation through establishing supportive working relationships between the service providers and industry associations. Essentially, this process requires identifying business and public policy requirements, tailoring the infrastructure, identifying the data sources and instituting analytics capability (IBM, 2013; CIPD, 2013; Oracle, 2012). In addition, for generating private sector driven official statistics support of official statistical community is imperative.

REFERENCES

1. Elena Kvochko, (2012) Four Ways To talk About Big Data (Information Communication Technologies for Development Series)". worldbank.org. Retrieved 2012-05-30.
2. Aberdeen Group, 2013 . Ever Harder and Faster: Managing the New Demands of Data Integration. Analyst insight by Aberdeen Group.
3. Bersin, J, 2013. Big Data in Human Resources: *Talent Analytics Comes of Age.* (http://www.forbes.com/)
4. Bersin, J, 2013. *Big Data in Human Resources: Talent Analytics Comes of Age* (http://www.forbes.com/sites/joshbersin/2013/02/17/bigdata-in-human-resources-talent-analytics-comes-of-age/)
5. Bersin, J, Karen O'Leonard, and Wendy Wang-Audia, 2013. *High-impact talent analytics: Building a world-class HR measurement and analytics function,* Bersin by Deloitte, October 2013,
6. Bersin, Josh. (2012). *Big Data in HR: building a competitive talent analytics function – four stages of maturity* [online]. Oakland, CA: Bersin by Deloitte: Available at http://www. Bersin.com/Practice/Detail.aspx? docid=15430 & mode=search&p=Human-Resources
7. Bertolucci, Jeff. (2013). "Hadoop: From Experiment To Leading Big Data Platform", "Information Week", 2013. Retrieved on 14 November 2013.
8. Beyer, Mark (2011) "Gartner Says Solving 'Big Data' Challenge Involves More Than Just Managing Volumes of Data". Gartner
9. Biggeri, Luigi (2004). Integrity – A Pre-requisite of Independence and Credibility of Official Statistics. Published in the Statistical Journal of the United Nations Economic Commission for Europe. Volume 21, Number 3-4/2004. P-199-205. IOS Pres.
10. 10. Boja, C; Pocovnicu, A; Bătăgan, L. (2012). "Distributed Parallel Architecture for Big Data". *Informatica Economica* **16** (2): 116–127.
11. CDW, (2013). Business Intelligence Shows its Smarts. *White paper published at CDW.com/businessintelligence.*
12. CIPD, (20130.. Talent analytics and big data – the challenge for HR. *Chartered Institute of Personal and Development (CIPD)/ Oracle Research Report.* Gudipati M., Rao, Shanthi, Mohan, N. D. and Gajja, N. K. (2013). Big Data: Testing Approach to Overcome Quality challenges. *Infosys Labs Briefings Vol.11 No1*
13. Davenport and Harris, 2007.
14. David Leinweber (April 26, 2013). "Big Data Gets Bigger: Now Google Trends Can Predict The Market". Forbes. Retrieved August 9, 2013.
15. Evelson, Boris, 2010). "Want to know what Forrester's lead data analysts are thinking about BI and the data domain?"
16. IBM, (2013) "IBM What is big data? — *Bringing big data to the enterprise".* www.ibm.com. Retrieved 2013-08-26.
17. ISI (1986). Declaration of Professional Ethics for Statisticians. International Statistical Review 227-247. International Statistical Institute.
18. Jamack, Peter J. (2012). Big data business intelligence analytics. *www.ibm.com/developerworks/ibm/trademarks/*
19. Kian Yew, Ong & Ramachandran (2012). PIKOM moving up in the value chain: Advocacy to value creation. Published in "ICT Strategic Review 2012/13: The Digital Opportunity". PIKOM
20. Laney, Douglas (2012). "The Importance of 'Big Data': *A Definition".* Gartner. Retrieved 21 June 2012.
21. Lavlle, Steve, et al (2011). Analytics: The new path to value: How the smartest organizations are embedding analytics to transform insights into action. *IBM Global Business Services.*
22. Luhn, H.P. (1958). "A Business Intelligence System". *IBM Journal* **2** (4): 314. doi:10.1147/rd.24.0314).
23. Manyika, James et al Hung (May 2011). Big Data: The next frontier for innovation, competition, and productivity. *McKinsey Global Institute.*
24. Martin Hilbert (2013), Big Data for Development: From Information- to Knowledge Societies", SSRN Scholarly Paper No. ID 2205145). Rochester, NY: Social Science Research Network; http://papers.ssrn.com/abstract=2205145
25. McAfee, A. and Brynjolfsson,E. (2012). Big Data. The management revolution. *Harvard Business Review, Vol 90, No 10, October, pp60-68.*
26. Nandyal, Raghav S. (2011). "CMMI. Framework of Constellations for Building World Class IT Organizations". Nandyal, R.S. Tata McGraw-Hill publication.
27. Oracle and FSN (2012). "Mastering Big Data: CFO Strategies to Transform Insight into Opportunity", December 2012
28. Pieter M, 2008; Power, D.J., 2010)
29. PIKOM, 2013. "Addressing talent needs of the Economic Transformation Programme" by TalentCorp Malaysia. Published in "ICT Strategic Review 2013/14: The Digital Opportunity". PIKOM
30. PIKOM, 2014. ICT Job Market Outlook . Annual series published by PIKOM.
31. Power, D.J. (10 March 2007). A Brief History of Decision Support Systems, version 4.0. DSS Resources.COM.
32. Raine, L. & wellman, B. (2012). *Networked. The New Social Operating System.* Cambridge: MIT Press.

33. Ramachandran and Vigneswarer (2011). Statistical Compilation of ICT Sector in Malaysia publication. Published by *Orbicom, the International Network of UNESCO Chairs in Communication 2011.*
34. Ramachandran R (2003). Measuring Knowledge Development and Developing Official Statistics for the Information Age, International Statistical Review, 71, 1, 83-107, Printed in The Netherlands.
35. Ramachandran, R. (2008). Measuring Information Development in the New Millennium. *Thesis submitted in fulfilment of the requirement for the Degree of Master of Philosophy,* Multi-media University, Cyberjaya. Malaysia.
36. Snijders, C., Matzat, U., & Reips, U.-D. (2012). 'Big Data': Big gaps of knowledge in the field of Internet. *International Journal of Internet Science, 7,* 1-5. http://www.ijis.net/ijis7_1/ijis7_1_editorial.html
37. Straf, Miron L. (2003). *Statistics in next Generation.* Journal of the American Statistical Association. Pages 1-6, Volume 98, Issue 461.
38. UNSD (2006). *Fundamental Principles of Official Statistics* ST/ESA/STAT/OFFICIALSTATISTICS/WWW
39. Webster, John (2013). "MapReduce: Simplified Data Processing on Large Clusters", "Search Storage", 2004. Retrieved on 25 March 2013.
40. Wyckoff, A.W. (2001). OECD Efforts to Address the Measurement and Policy Challenges posed by the Information Society. Paper presented at IAOS Satellite Meeting on Statistics for the Information Society, 30-31 August 2001, Tokyo Japan.

CHAPTER 4

COGNIZANT COMPUTING: THE NEXT ERA OF COMPUTING IS PERSONALIZED

NICK INGELBRECHT
Research Director
Gartner

Gartner

Cognizant computing is a conceptual framework that describes the next era of "personal cloud" computing. It will become one of the main focuses of consumer technology investments during the next decade and provide a quantum increase in the utility and usability of computing in people's everyday lives. The term cognizant computing is defined as the application of contextual information to computing in order to permit actions to be taken according to pre-defined rules.

The future of personal computing is "cognizant"; that means the computer is aware of your context and your activities and can take actions on your behalf. Those actions could range from waking you up 10 minutes early in the morning because of an unexpected traffic delay on your regular route to work, to re-arranging your schedule on the fly, or even driving the car itself. Cognizant computing is impacting every aspect of the technology business, because it is fundamentally changing the value chain of digital services.

Early iterations of cognizant computing include Apple Siri, Microsoft Cortana and Google Now. By 2020, the capabilities of these virtual assistants will have converged with the smart advisor technologies of systems like IBM Watson that combine big data analytics with natural language processing This convergence will transform the operating environment for technology and service providers. Any company in the business of providing a service, using apps or selling devices will be directly affected.

Global technology vendors are making large investments in the enabling technologies of Cognizant Computing and positioning their businesses to exploit the emerging revenue opportunities. IBM, for example has internally projected $10 billion in revenue from Watson within 10 years , equivalent to 10 per cent of current annual sales.

Cognizant computing also heralds the next evolution of the personal cloud, as consumers switch their focus away from devices to services. IT research and advisory firm Gartner predicts that by next year (2015) the majority of the world's largest companies will be using Cognizant Computing to fundamentally change the way they interact with their customers.

By amalgamating and analyzing data in the cloud from many sources (including apps, smartphones and wearable devices), cognizant computing provides contextual insights into how people behave — what they watch, do and buy, who they meet, and where these activities take place. For companies of all kinds, this provides an opportunity to increase the lifetime value of their increasingly fickle customers, improve customer care, boost their sales channels, and change the customer relationship by making it more personal and relevant. In essence, this new development will help companies innovate and create new business opportunities.

As a conceptual framework, Cognizant Computing provides an innovation roadmap for the technology sector and provides industry context for policy makers in developing Malaysia's ICT industry under the 11th Malaysia Plan (2015-2020).

DEMAND DRIVERS AND CURRENT STATUS OF COGNIZANT COMPUTING

There are two demand side drivers for Cognizant Computing: Consumers find they get far greater value and enjoyment out of their digital devices and services if the technology addresses their needs at a particular place and

time. Similarly, businesses can make far more efficient and effective use of their technology investments if they meet the specific needs of employees and customers when and where they are needed. In either case, the more customized those interactions are, the greater their value and impact.

Consider how Cognizant Computing could address these issues using technology available today using a car crash as an example:

Imagine the driver of a car has a smartphone equipped with the typical range of sensors such as accelerometers, GPS/location, temperature sensors and perhaps body sensors connected to a Fitbit or other health monitoring device. The driver in this example is hit by another vehicle running a red light.

In this case, the driver's smartphone detects the sudden deceleration of the car and the concussion of the impact. This automatically triggers a pre-loaded "auto accident app" on the smartphone, which is pre-programmed with a number of automatic actions, including (for example):

- Checking your heart rate to assess whether you are alive
- Calling an ambulance if the vital signs are outside normal limits

The app also has an "Insurance" module that sets to work by -

- Checking the vehicle status by plugging into the car's telematic diagnostic system
- Alerting the insurance company and triggers a claims process and instructions for the driver on what to do at the scene of the accident
- Uploading video of the crash from onboard cameras to cloud storage (in the event the car catches fire)
- Fulfilling legal obligation to notify accident to police
- Alerting roadside assistance to get a tow truck
- Interrogating local traffic cameras, devices, cars individuals collecting names and addresses of potential witnesses
- Calling husband, wife, parent, or work administrator to alert them to probable delays

While all these technologies exist in isolation today, the overall app design and enabling middleware is not yet in place. Insurance companies, roadside assistance, traffic authorities, device vendors, communications companies, healthcare and automotive providers all have an interest in pulling the disparate pieces of the "car crash app" together. However the winner is likely to be the technology provider that can integrate these capabilities into a "Cognizant" app.

Consumers today are increasingly demanding ease of use from their digital devices and technologies, as well as real benefits from smarter apps and services. In order to meet this demand, technology and service providers are pursuing Cognizant Computing strategies in various ways.

However, most technology offerings have yet to move beyond simple data synchronization and storage. This can be illustrated by deconstructing Cognizant Computing into four distinct phases, as shown in Figure 1:

Each phase assists in increasing personal and commercial information about a consumer, offering advanced features and benefits to both the business and its customers. The four stages are described as follows:

SYNC ME

The Sync Me phase of Cognizant Computing is the activity where apps and content get synced with the cloud. Over the coming years, we expect an increasing amount of consumer apps to sync information with the cloud rather than

Figure 1. Four Phases of Cognizant Computing
Source: Gartner (July 2014)

simply storing information solely in the app. This will create an increasing amount of traffic to the cloud while making it easier for apps developers and brands to gather information about consumers, their apps and content usage. Evernote is a good example of an app that syncs consumer notes with the cloud and enables those notes to be downloaded from anywhere on other devices. Evernote aspires to become the user's digital brain at some stage in the future.

SEE ME

The See Me stage of Cognizant Computing is where data is gathered about a consumer's digital and physical footprint. It is closely aligned with information about a consumer's physical location, social graph and brand preferences. Data can be collected from a variety of sources such as: apps, maps, photo-tagging on social networks, mobile payment history, IP address and Internet cookies, loyalty cards, billing information and face recognition.

Key Cognizant Computing assets for the See Me phase include:

- Location: Where am I?
- Device: How is information gathered?
- Connectivity: How important is connectivity?
- Regulations: How to set boundaries?
- Commerce: How to monetize data?

KNOW ME

Where See Me is a simple data-gathering exercise, Know Me is the stage where analytics are applied to the data and inferences made. This is where consumers begin to actively interact with data that they are "supplying" and where analytical tools and network intelligence is piecing data fragments together, interpreting and making deductions about where consumers normally go, at what cadence and who they are more likely to interact with and also which brands they typically prefer. Most importantly, this is where consumers can set their preferences and rules about who will be able to see and access their data. They may give some apps and service providers more access than others — for example, they will probably give their bank more insight into their daily lives than an estate agent they interact with.

Key cognizant computing assets for the Know Me phase include:

- Personal Information: Who am I?
- Behaviour Analytics: Activities I do/like, people I meet, when?
- Consumption Pattern: What I purchase, what my purchase preferences are?
- Personal Preferences: Who I will allow to have access, to "See Me"?

BE ME

The Be Me stage is the real objective of Cognizant Computing. By this stage, systems have gained a 'good enough' knowledge of the individual to take limited actions on their behalf. This will typically involve a smartphone or other device and its related apps and cloud services, to make "smart" decisions for the consumer based on predefined rules. Consumers will have established a level of confidence in their device and apps that they allow them to make the right type of decisions for them.

It is assumed that the app is acquiring knowledge over time and gets better with

improved predictions of what users need and want, with data collection and response happening in real-time. The first service that will be performed "automatically" will generally help with menial tasks — and significantly time consuming or time wasting tasks — such as time-bound events (calendaring) like booking a car in for its yearly service, creating a weekly to-do list or sending birthday greetings. Gradually, as confidence in the outsourcing of more menial tasks to the smartphone increases, consumers are expected to become accustomed to allowing a greater array of apps and services to take control of other aspects of their lives.

From a commercial perspective, the Be Me phase presents a critical opportunity for sales and marketing managers. They will have a rounded picture of the customer and their present needs.

The Know Me phase of cognizant computing cannot exist if there are none of the earlier phases. Attempting to move from the See Me stage to the Be Me stage may lead to critical errors, mistakes and compromise private data. Similarly, some consumers may decide that they do not want to approach the Be Me stage due to regulatory concerns or personal preferences. Technology providers need to tread carefully in creating services and apps that consumers can both trust and have confidence in without violating their personal data.

Key Cognizant Computing assets for the Be Me phase include:

- Quality of Experience: My expectations
- Rules and Permissions: Setting the rules and giving appropriate permissions
- Confidence and Trust: Regular, reliable and responsible service delivery in the interests of the customer
- Commerce: Now you Know Me — make decisions and purchases for me

Through data gathered and processed in the first three phases a Cognizant system has the ability to predict a consumer's next move or their next purchase decision. In the Be Me stage, the system interprets those actions based on those previous stages and acts upon them according to pre-set rules. In a B2C context, that might involve automatically delivering a product to a customer. In the consumer context, the four stages of cognizant computing comprise a virtual assistant that can perform routine tasks automatically with very little effort from the user.

Today, smartphones typically carry around ten different sensors, measuring things such as geographical location (GPS), orientation and movement (gyroscope, accelerometer, compass), temperature, humidity etc. The personal virtual assistants of the future will add to this the ability to sense users' moods, trigger emergency alerts, automatically help with language issues, process bills and order things. Additionally, they will follow the consumer's instructions regarding their various pre-set personas. For example, the system could be set to function in business mode as a work persona between (say) Mondays and Fridays during the hours of 8 a.m. and 6 p.m., and in personal mode at other times and in parental persona mode at any time, day or night.

By 2018, Gartner predicts that virtual assistants will evolve as cloud-based apps that integrate with multiple apps in the personal cloud, as well as integrated apps closely tied to a device or app.

TECHNOLOGY UNDERPINNINGS AND EARLY ITERATIONS OF COGNIZANT COMPUTING

The flurry of activity around Siri, Cortana and Google underpins the probability that virtual assistants that achieve early success and mindshare will have a better chance of

dominating the market in future because of their lead in the knowledge base, semantics and integration with apps.

Consumers tend to use a cluster of apps for performing certain tasks. For instance, a consumer might take a photo using the camera on their smartphone, then enhance the photo using a photo editing app, store the image in a cloud dropbox and share it on Facebook. Consumers need to move from one app to another to do this, mainly because they prefer different apps for different functions. Similarly, consumers get their information from multiple apps (for example, appointments, news, emails, weather forecasts and traffic situations).

Virtual assistants simplify app usage and save the user the trouble of moving in and out of multiple apps by combining the information to offer a more informed and intelligent suggestion.

Through appropriate APIs and user instructions, a virtual assistant can do the following:

- Draw commonly used information and updates from multiple apps (such as messages, news alerts and weather forecasts) and cache the data for fast delivery to the user in a natural language question answer (NLQA) format. As a start, Google Now recognizes repeated actions that a user performs (for example, common locations, repeated calendar appointments, search queries and, emails) to display more relevant information to the user in the form of "cards."

- Offer relevant advice through a more holistic understanding of users' preferences, online activities and information in the apps they use. The notion of quantified or measurable information is growing as consumers use wearable devices to track their performance. Apps in the personal cloud will progressively have a lot more disparate personal data about consumers (captured by wearable devices) that can be pieced together by the virtual assistant to provide an intelligent suggestion. For example, a virtual assistant may know your dietary preferences, health and daily calorie needs to be able to suggest a restaurant that serves food suited to your requirements.

- Launch the relevant app for user access if no information is available.

App ecosystem providers developing and customizing virtual assistants should try to focus on specific tasks. They should take a realistic approach to developing virtual assistants to perform a specific set of tasks. Prioritize those tasks that are closely tied to users' frequent online activities (like reading emails, news and updates from social networks, recommending shopping deals, finding the nearest store, booking a taxi, flight or restaurant, or simply taking a photo). For example, this could involve helping a user find a particular movie showing locally and purchasing tickets for them.

Users can ask Google Now about their appointments, flights, certain purchases and photos. Artificial intelligence (an umbrella technology for virtual assistants) started to have more success when research began to focus on specific issues within industry verticals such as logistics and healthcare.

Figure 2 shows the role of virtual assistants, which involves a better understanding of users ("Know Me") and the ability to act on behalf of users by becoming digital extensions of users ("Be Me").

Virtual assistants are developing on the back of some foundational technologies, capabilities and market factors that include:

- **Big data**. Most notably, a virtual assistant will improve once it has access to the

Figure 2: Virtual Assistants evolve Cognizant Capabilities

volume of big data in the personal cloud scattered across multiple apps. The rise of sensor-based, wearable and other devices as part of cognizant computing will create large volumes of data about customers that virtual assistants can process into suggestions and actions for users.

- **Natural language processing.** NLP has advanced by allowing a computer or service to answer non-conversational, information-centered queries. This is helping to advance the NLQA system used for evolving from search options to zeroing in on the exact answer, as exemplified by IBM Watson.

- **Proliferating apps environment.** Aside from smartphones and tablets, TVs and other devices (such as watches) that are not best suited to touch user interfaces are increasingly incorporating an apps environment. Manufacturers will need alternative human to machine interaction for such devices.

- **Semantic Web .** This is the evolving standard for enabling machines to process Web pages by attaching Web page metadata and their relationship between the pages.

Virtual assistants will also improve as computing power advances, along with the use of context and machine learning techniques.

Historically, virtual assistant providers have sold their softwares to businesses for self-service in customer care and education. In these markets, the virtual assistant has evolved over time from the early version (generation 1) with little visual appeal and mostly text-to-text based interactions, to a sophisticated "human-like" version (generation 6), with moving images and speech-to-speech based interactions, supported on mobile and Web-based platforms. Nuance communications' virtual assistant, Nina (which validates a user's identity from their unique voiceprint), is targeted at customizing third-party apps for customer self-service.

IBM Watson is being commercialised for a variety of different industries with the low-hanging fruit in customer care, banking and healthcare.

The introduction of Apple Siri has popularised the idea of virtual assistants on smartphones and tablets, adding in personality traits that attempt to make for a more appealing user experience. Apple has also focused on improved hardware and multiple microphones to cancel background noise. In iOS7, Apple improved Siri with better quality voice and answers to new sets of queries, integration with Wikipedia, Twitter and Bing and a new interface.

Google has strong fundamentals in search, which it used to build Google Now. Its wearable device, Google Glass will respond to voice commands and perform actions such as "take a picture" or deliver information, but it remains to be seen at what stage Google Glass will support a distinct virtual assistant application. Samsung, on the other hand, offers S Voice on its Samsung Galaxy devices.

In addition, those companies with a core competence in voice recognition technologies or artificial intelligence will try to build a virtual assistant application. Tempo AI has transformed the calendar into a virtual assistant and plans to use an anticipatory model for user content from various apps in the personal cloud to provide advice and perform actions.

COGNIZANT COMPUTING ASSETS

Cognizant Computing is an evolution of the "personal cloud", the personal computing paradigm comprised of the apps and services that allow users to store, stream, sync and share data on contextual basis between devices. For the personal cloud to become smarter and evolve into cognizant computing a number of assets need to be put in place.

There is a direct relationship between assets and how they contribute to each of the phases. Sync Me and See Me — the earlier phases in the evolution of the personal cloud — will be filled with assets that help consumers manage and access their data, or provide useful but discrete services that often do not (or cannot) mesh together. In the later phases — Know Me and Be Me — asset creation will be in its most intense period and asset functionality will transition to fully understanding individual consumer behaviour, then becoming able to accurately predict and make decisions for its users. Not all assets are necessary and the chart below shows their contribution if they are being used.

Figure 3 below represent the Cognizant Computing asset life cycle and is colour coded as follows:

- During the early (green) phases the asset will take shape and its value as a contribution to the overall strategy will be established.
- During the asset's middle phases (blue) it will be monetized.
- During its final phase (red) it will fully mature and become commodity or commonplace.

Each type of asset may transition through these phases differently and some assets, such as connectivity, are already well established. For most assets the scale presented will indicate that there will be critical times at which investment will be needed, or that asset may take too long to mature.

From a commercial perspective, companies will be able to monetise their Cognizant Computing assets through their increased knowledge of the consumer and the fine-tuning of offers that can now be achieved and are increasingly perceived as personal and highly relevant. This improves the performance of the brand and provide cross-sell / up-sell opportunities.

The mobile commerce opportunities are will increase through the Be Me stage as the smartphone is enabled to make certain authorized purchases automatically via a customer's mobile wallet or credit card linked

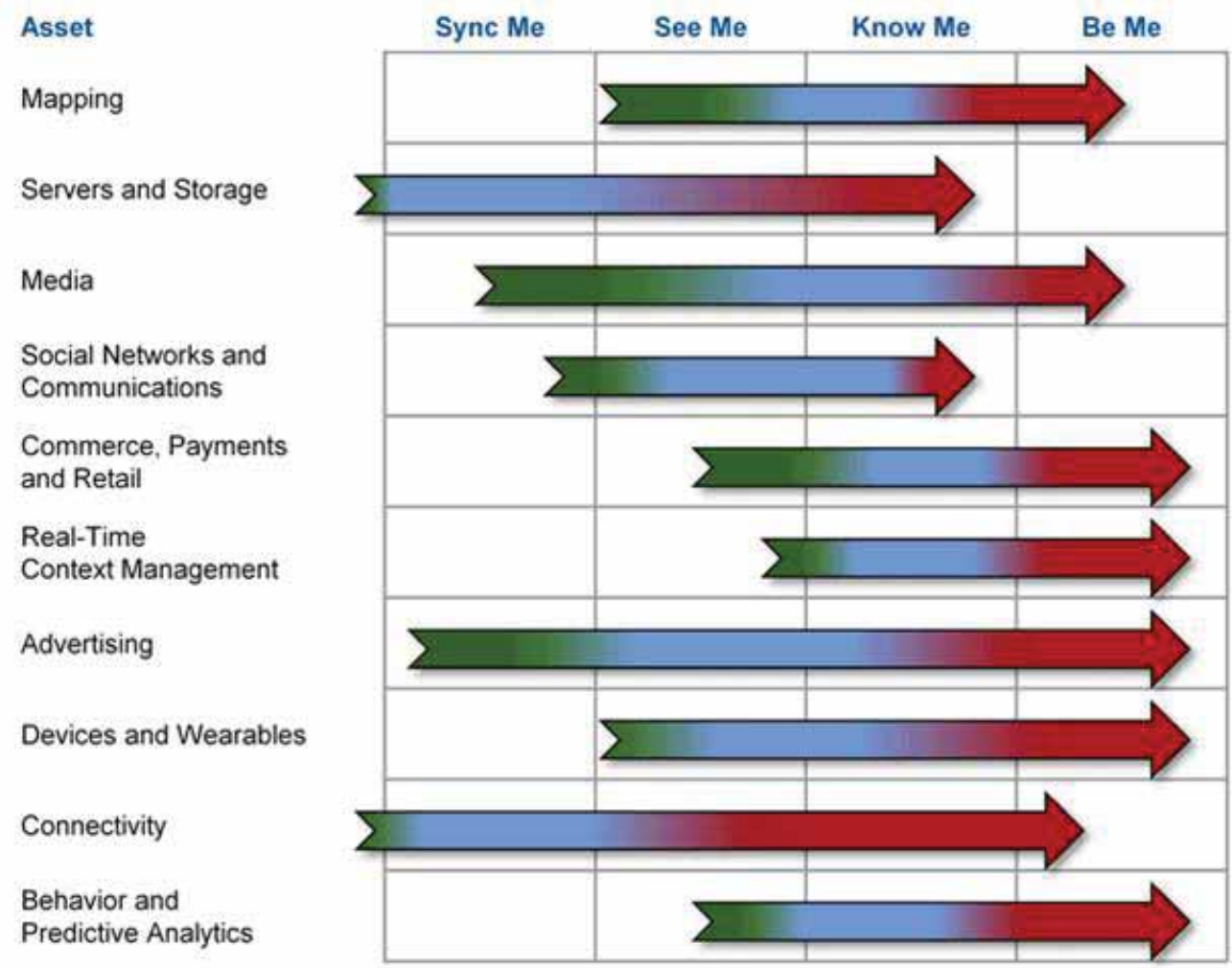


Figure 3: Cognizant Computing Asset Life Cycles

Green = early phase, the asset will take shape and its value as a contribution to the overall strategy will be established; Blue = middle phase, the asset will be monetized; Red = final phase, the asset will fully mature and become commodity or commonplace.

to the mobile device. Correctly executed, Be Me services will flow from the permissions set by the user, hence non-agreed purchases would not occur. The key issues is ensuring that the right rules and permissions are set in place by the user so that only actions that are pre-approved will happen — rather than the smartphone making "rogue" purchasing decisions. This will occur through a progressive series of authorizations that create a pattern of trusted interactions which the user is comfortable with.

Consumer technology businesses and their products have reached only the first plateau of cognizant computing, since many apps have demonstrated usefulness but still lack the ability to fully "understand" user behaviours and intentions. Technology providers are responding by creating more compelling products and services that go beyond a base level of service, because they want to extend their usefulness by building in advanced features that are derived from user-generated data and rules about how to act on the user's behalf.

Businesses can use cognizant computing assets as their building blocks to increase the "smartness" or perceived usefulness of their apps and services. Today, consumers are accustomed to using these assets without

even actually recognizing they exist. For example, it is common practice to take for granted basic functionality such as being able to watch a movie using an online movie service on one device, then pause the movie and start playback on another different device at a later time. That basic functionality requires the integration of media, devices, connectivity, servers and storage among other assets.

As companies leverage Cognizant Computing, they will refine the use of these assets and begin to rely on them as a foundation on which they can build and develop smarter apps. The 10 assets shown above are not exhaustive, but they do represent a confluence of technologies and products that are uniquely positioned to enable a wide variety of "hyper-personalised" apps and services.

Assets for Cognizant Computing can be categorized based on their inherent attributes and their impact on users:

- **Intrinsic Assets:** These assets are defined as those that are internal to a business and are considered to be building blocks for other assets. In a few cases they are exposed to end users as some type of service or technology that is, at its core, the Cognizant Computing experience.

- **Extrinsic Assets:** These assets are more focused on the user experience aspect of Cognizant Computing. They represent the technologies that directly impact how users interact with cognizant-enabled apps, what type of services the apps offer, and what types of revenue they can expect.

Their relationship is illustrated below in Figure 4.

The various assets bring different capabilities and will not be applied to a business or product strategy in the same way. Each asset has its own unique properties and contributes differently to the final customer experience. In practice, some assets will be used in combination with others, some on their own, while others can be deconstructed into smaller constituent parts. In all circumstances, when a business wants to implement the continuum of phases, at least one will be necessary to deliver products and services to customers and users.

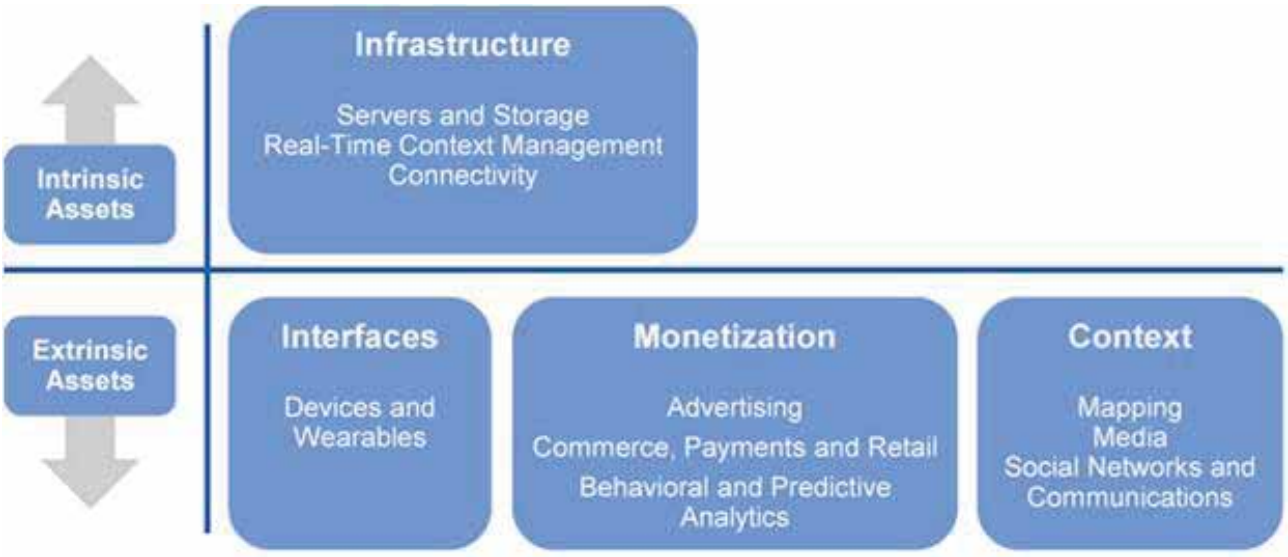


Figure 4. Cognizant Computing Asset Map
Source: Gartner (July 2014)

COGNIZANT COMPUTING BRAND ANALYSIS

All the major technology brands are developing their Cognitive Computing capabilities. Figure 5, below, provides an evaluation of how advanced the various brands in using or supplying Cognizant Computing Assets.

The ratings range from Emerging, which signifies that the company is just starting to use or deploy those assets, to Mature, which means those companies have consolidated and are fielding an advanced set of assets.

Most companies have reached a base level of Cognizant Computing asset functionality, which can be characterized as having basic data synchronization and storage capabilities. This is evident in many consumer mobile apps that manage personal data where it is expected that the data is readily available anytime on any device. Beyond this basic data synchronization functionality, most technology and service providers — except Google — have only recently begun to transform their apps and services from basic to smart. Google's acquisition of Nest, for example, opens up significant inroads into the connected home. It positions Google as the potential provider of the "command centre" in the connected home, integrating hundreds of IoT devices (Gartner estimates that some homes will each have upwards of 500 connected devices by 2020). This command centre capability will be essential for consumers to manage their homes more efficiently and in so doing, potentially provide insight into consumer behaviour for marketing purposes. Although the assets are in place, Google's intentions are not clear at this stage.

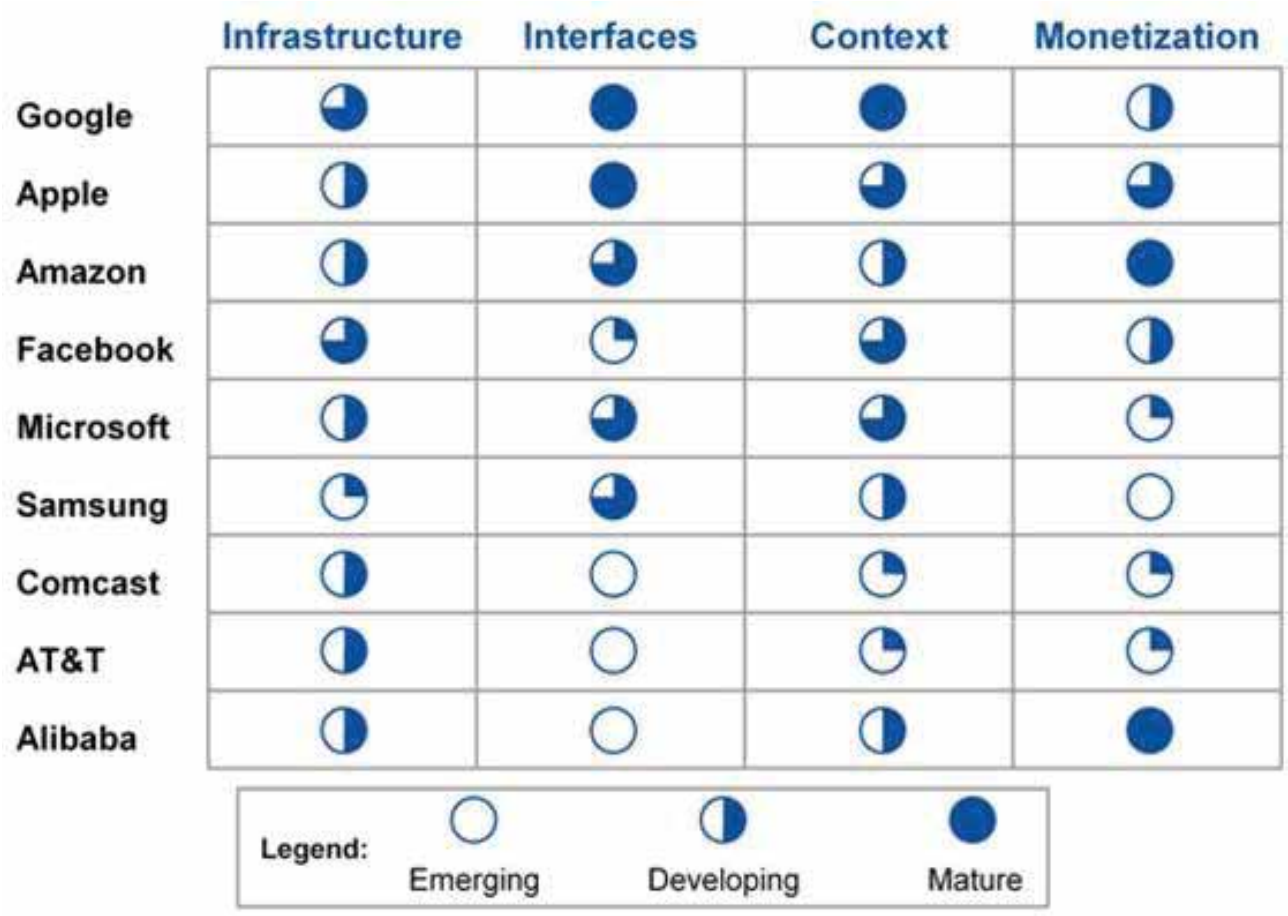


Figure 5. Evaluation of Cognizant Computing Assets
Source: Gartner (July 2014)

As of mid-2014, most cognizant computing activity is around the first two stages. As big data aggregation and the Internet of Things become more pervasive and the analytics required to process the vast amounts of information evolve, cognizant computing will come of age.

Technology firms will need to evaluate their current stock of assets to determine those that are already able to implement the early phases of the transformation. For the rest of the assets, an implementation plan should be developed, taking into account which consumer apps and services would most benefit from the addition of those assets.

CHAPTER 5

DIGITAL REINVENTION PREPARING FOR A VERY DIFFERENT TOMORROW

SAUL BERMAN
saul.berman@us.ibm.com

ANTHONY MARSHALL
anthony2@us.ibm.com

NADIA LEONELLI
nleonelli@us.ibm.com

IBM Institute for Business Value

IBM INSTITUTE FOR BUSINESS VALUE

IBM Global Business Services, through the IBM Institute for Business Value, develops fact-based strategic insights for senior executives around critical public and private sector issues. This executive report is based on an in-depth study by the Institute's research team. It is part of an ongoing commitment by IBM Global Business Services to provide analysis and viewpoints that help companies realize business value. You may contact the authors or send an e-mail to iibv@us.ibm.com for more information. Additional studies from the IBM Institute for Business Value can be found at ibm.com/iibv

The individual-centered economy is already here. The newest digital technologies – among them social media, mobility, analytics and cloud – keep changing how people, businesses and governments interact. These digital forces enable unprecedented levels of connectedness and so the world is already investing in consumer-centricity. However, these new technologies are truly still in their infancies. The transformation that is already underway will soon intensify, resulting in a paradigm shift from customer-centricity toward an everyone-to-everyone (E2E) economy. The implication for value creation and allocation will be profound. New IBM research shows that many organizations are still not ready to navigate the E2E environment. To prepare for the radical disruption ahead, companies need to act now to create experiences and business models that are orchestrated, symbiotic, contextual and cognitive.

Today's uber-connected, empowered individuals seek 24/7 access and organizational transparency. They want to exert greater personal influence over organizations and participate in more digital activities as they conduct their daily lives. In the IBM Global C-suite Study, [5]5 percent of 4,183 C-suite executives report that consumers have the most influence on business strategy, second only to the C-suite itself.[1] Looking ahead, 63 percent of the leaders we surveyed in this 2013 IBM Digital Reinvention Study expect consumers to gain even more power and influence over their businesses. The culmination of accelerating digital and other technological forces is spawning disruption on an unprecedented scale. And yet, most organizations have not fathomed the full implications of a radically different, digitally-charged future. When asked what kind of digital strategy their enterprise has, more than sixty percent of CEOs told IBM they still lack an integrated physical and digital strategy.[2]

Digital technologies will ultimately drive drastic changes in the economy: value chains will fragment, industries will converge and new ecosystems will emerge. As a result, the mechanics of value creation and value allocation will also change. Looking five years out, 58 percent of 1,100 executives we surveyed in the Digital Reinvention Study expect new technologies to reduce barriers to entry and 69 percent expect more cross-industry competition.

So, what will this future of continual digital disruption entail? How will new convergent technologies impact organizations and industries? What can organizations start doing today to begin preparing for a vastly different business environment? In particular, which investments, priorities and actions can set the stage for success during turbulent and ongoing change?

This 2013 IBM Digital Reinvention Study considers the answers to such questions. To better understand the deepening impact of digital technologies on today's organizations, the IBM Institute for Business Value surveyed approximately 1,100 business and government executives and 5,000 consumers across 15 countries. We also conducted in-depth interviews with 30 leading futurists (see Methodology section in appendix for more details).

Our analysis of study findings shows that as technological change persists, the interactions between organizations and individuals also keep changing – and this change is accelerating fast. In fact, the global economy was characterized as highly organization-centered for most of the 20th century. Its current state – individual-centricity – emerged around 1990, but this will further evolve into an everyone-to-everyone (E2E) model of engagement.

Prospering in an E2E setting demands disruptive innovation that challenges established norms and blurs organizational boundaries. It will be critical to open up to external influences, expand partnering and accelerate digital investments – the sooner, the better. This executive report offers practical ways to prepare for that fast-approaching and very different tomorrow.

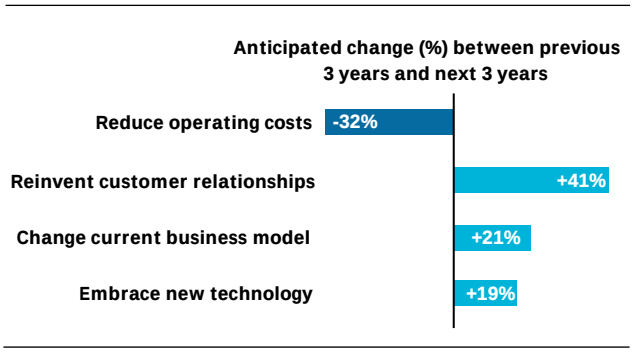


Figure 1: Organizations are transitioning from intense focus on operating costs toward growth and transformation.
Source: IBM Global Csuite Study, CEO question: "What are the top priorities in your business strategy?"

NOW AT WARP SPEED: DIGITIZATION

Digitization is rapidly changing the nature of how individuals and organizations interact: the result is an individual-centered economy. Individuals are more connected and empowered, leading to rising expectations about information access, ubiquitous connectivity and transparency. The ability to stay connected through a variety of devices has increased consumer influence over organizations and drives a consumer-centric business strategy. Competition is coming from new and different areas, opening up opportunities for previously unforeseen entrants – and simultaneously creating new threats. Organizations are adapting innovative business models and using newly found digital capabilities to enable original consumer experiences. The IBM Global C-suite Study shows that the intense focus of the past three years on business strategy that reduces operating costs is shifting to a renewed focus on growth and transformation (see Figure 1).[3]

In the early part of the 20th century, the economy was organization-centered and dominated by producer-driven consumption. Ford and its Model T are an example of this model. Industries were characterized by high barriers to entry and capital-intense production, with larger enterprises controlling production.

Later, as technological capabilities changed consumer expectations, the organization-centered economy evolved into today's individual-centered economy (see Figure 2). The individual-centered economy is characterized by product differentiation and individualized market segmentation targeted at deriving value for the consumer. There is a strong emphasis on design and marketing, and organizations listen to create relevant, customized experiences that realize value for the consumer.

As discussed in our 2011 study, "Digital transformation: Creating new business models where digital meets physical," organizations have been embracing digital transformation to create compelling consumer experiences.4 In the individual-centered economy, four elements of digital transformation are critical: being flexible, integrated, tailored and responsive (see Figure 3).

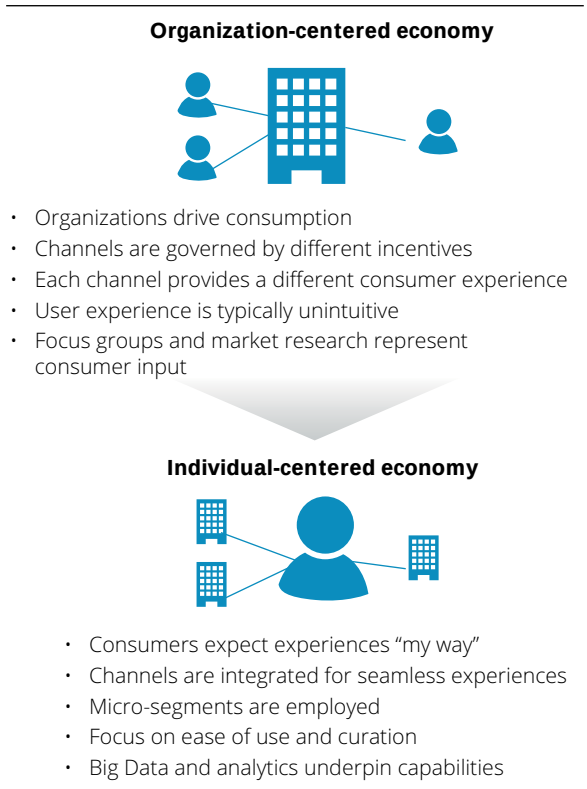


Figure 2: The attributes of an individual-centered economy: keeping the focus on creating customer experiences that are rewarding.

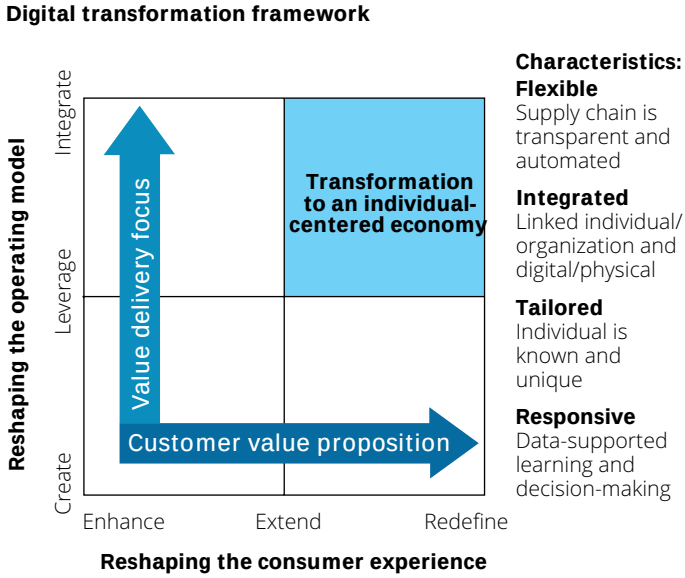


Figure 3: Digital transformation produces customer experiences that support what individuals need or want. support what individuals need or want.
Source: IBM Institute for Business Value analysis; "Digital transformation: Creating new business models where digital meets physical." IBM Institute for Business Value.

TECHNOLOGICAL DISRUPTION: THEN AND NOW

Looking back to 1978, personal computers, mobile phones and the Internet were in their infancy. Those powerful disruptive innovations have shaped the society we live in today and it took decades for their impacts to be fully realized. Today, technological change is happening in a time span that is highly compressed compared to what has come before. We are at the beginning of another shift, as these newer technologies develop and mature – but much faster and even more profoundly.

Social media explosion. Even as they heighten control and privacy issues, collaboration and information sharing are spurring new models of value creation. "Social" has become revenue-generating, evolving from a dot-com trend to a sharing platform and business model. Groupon (a crowd-based deals company) and peer-to-peer lending (lending to individuals without a financial intermediary) are examples of collaborative buying and revenue sharing models that are driving the sharing economy movement.

Mobile revolution. Mobility and miniaturization are transforming consumer experiences via new capabilities, such as the increased use of location-based services to enable both global positioning systems (GPS) and targeted retail promotions. New payment ecosystems using the mobile wallet turn dollars digital. And the miniaturization of mobile devices moves from palm-sized to wearable devices, including fitbit (enabling wireless fitness tracking) and Samsung Galaxy Gear (enabling receipt of texts and emails).

Analytics. Advanced analytics enable deeper business intelligence and consumer insight to be drawn from big data, producing information that ranges from descriptive to predictive. Internal and external data sources can now be integrated and services can be highly personalized based on consumer data, for example, the recent partnership of American Express with Twitter.

Cloud enablement. Cloud enablement allows for new models of interaction between individuals and organizations, and will help facilitate cross-platform data analytics. Examples of these new ways to interact include subscription access to enterprise applications such as Adobe Cloud, cross-platform on-demand content such as Netflix and computing without boundaries such as virtual collaboration spaces.

A VIEW OF THE VASTLY DIFFERENT FUTURE

The promise of compelling customer experiences can now be realized because of these technological and social changes. As industries converge, new ecosystems that cut across multiple organizations, functions and industries will emerge to enable new and compelling experiences.

VALUE CHAINS WILL FRAGMENT

New technologies will make value chains more transparent and easier to decompose (see Figure 4). In the past, value chain disruptions often involved replacing whole value chains or big chunks of value chains, such as replacing traditional banking processes with Internet-based, virtual banking. Next generation value chain disruption will involve contesting more specific elements or functions within value chains.

A value chain is a sequence of activities that organizations perform to create and deliver some type of product or service to market.

Organizations will increasingly recognize their own unique competitive strengths related to specific functions and expand capability in these areas. These new specialists will begin to contest their chosen functions more aggressively in their own and other markets, for example, outbound logistics providers such as Maersk and Li & Fung. Specialization will generate ever greater pressures to improve. Faced with new functional offerings comprising better capability at lower cost, organizations will as a consequence begin to cede more and more non-core functions to specialists.

Ritz-Carlton, for example, recognized that their true competitive strength is their customer experience. The Ritz-Carlton Leadership Center now trains organizations in other (nontravel) industries on how to create outstanding consumer experiences. Leading hospitals are

Figure 4: How the fragmentation of a value chain may look as specialists enter to provide key capabilities.
Source: IBM Institute for Business Value analysis. Margin

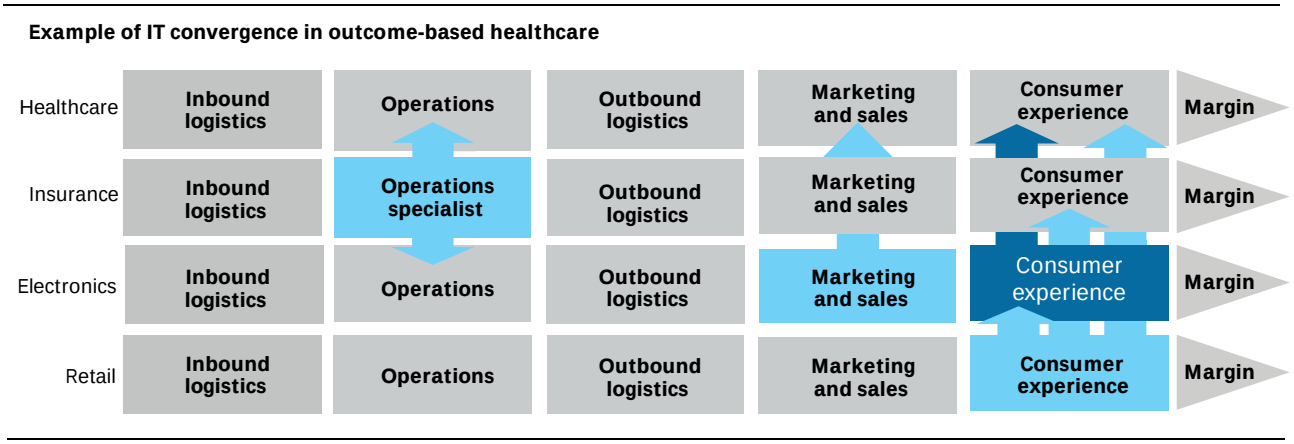


Figure 5: Illustrative example of how industry convergence can occur based on functional specializations.
Source: IBM Institute for Business Value analysis.

applying Ritz-Carlton's quality principles to improve their patients' medical experiences.[5] Chipmaker ARM designs chips for use in smart phones and tablets. Through licensing and royalty agreements, ARM passes the benefits of scale economies and design innovations on to consumers.[6]

INDUSTRIES WILL CONVERGE

As specific functions in value chains are contested, new competitors will emerge. Functional specialists from one industry will begin competing in specific value chain functions of other industries. This cannibalization across industries will begin to drive industry convergence (see Figure 5).

Organizations will begin pursuing dual strategies: to continue the focus on core business in their primary industries; and to seek growth opportunities in their chosen specialized functions across other industries. Specialization will drive industry convergence as competition expands around specific, common value chain functions.

An ecosystem refers to a complex web of interdependent enterprises and relationships directed towards the creation and allocation of business value.

A projected future example is advanced telemedicine, which allows delivery of quality healthcare, regardless of physical location. Access to medical expertise without regard to geographic boundaries can be possible via haptic (tactile) sensor technology from the electronics industry and infrastructure for real-time communications from the telecommunications industry. Related innovations from other industries may also emerge as the telemedicine market evolves.

NEW ECOSYSTEMS WILL EMERGE

Functional specialization, value chain fragmentation and industry convergence will begin to support formation of ecosystems or value nets (see Figure 6). Ecosystems will typically cut across multiple organizations, functions and industries, providing a foundation for new, seamless consumer experiences and camouflaging functional complexity.

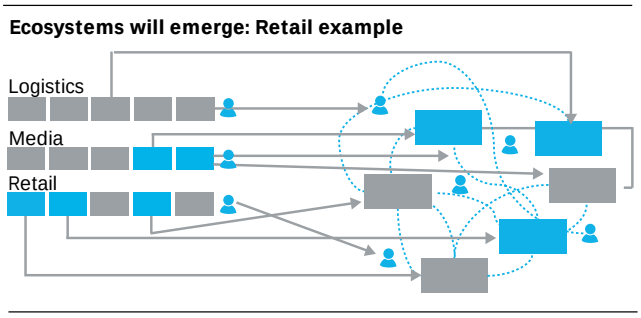


Figure 6: Illustrative retail industry example of forming new ecosystems.
Source: IBM Institute for Business Value analysis.

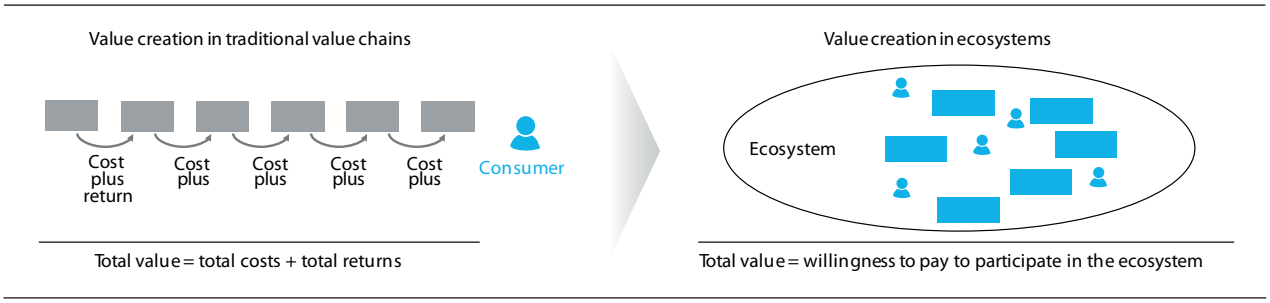


Figure 7: The way that value is created and allocated within ecosystems will differ from traditional value chain environments (as described in Figure 4).

Looking to the future, the projected future of retail is an example of emerging ecosystems. An omni-channel retail experience adapts real-time to a particular consumer's context. A combination of elements creates this experience: a concierge service acts as a single contact point for all needs; in-store assistance is augmented with intelligent, mobile self-help options; inventory and product delivery are fully integrated; and mobile payment is available and seamless across physical and virtual channels. Ecosystems will be very dynamic and able to deliver more complex experiences or activities than single – or even convergent – value chains. The manner in which value is created and allocated changes as organizations evolve from participating in traditional value chains to participating in ecosystems.

In traditional value chains, organizations optimize value with a "cost plus return" model, where organizations at each stage in the chain optimize value creation (see Figure 7). Total value reflects the aggregation of value created at each step in the chain. Organizations typically interact with the prior function and the next function in the chain, but have little sense of the overall market context.

But in ecosystems, organizations realize value through the engagement with the system as a whole, where "value" is defined by participants' willingness to pay for access to the ecosystem. Once access occurs, specific transactions may occur within the ecosystem. Total value created reflects the value of access to and engagement within the system as a whole.

This creates a substantial opportunity for organizations to insert themselves within emerging ecosystems. Mechanisms are required and can be established to share the value created for access among ecosystem members, whether through central allocation, looser orchestration or some other arrangement.

ENVISIONING THE NEW TRAVEL ECOSYSTEM

In the traditional travel value chain, value is tied to sales of specific travel services, including seat and room reservations, baggage and other service fees, itinerary coordination and post-trip services. Intermediaries benefit from the value that the entire system generates – by providing specific services in the value chain, such as online travel agents and global distribution systems that extract fees for reservations (see Figure 8).

In a future travel ecosystem, value is tied to the value perceived through access to a comprehensive travel experience, including physical goods, services, information and coordination. As each member of the current value chain expands its aperture, it will realize that consumers value the net benefit of the entire experience, not just isolated travel components. In this ecosystem view, value

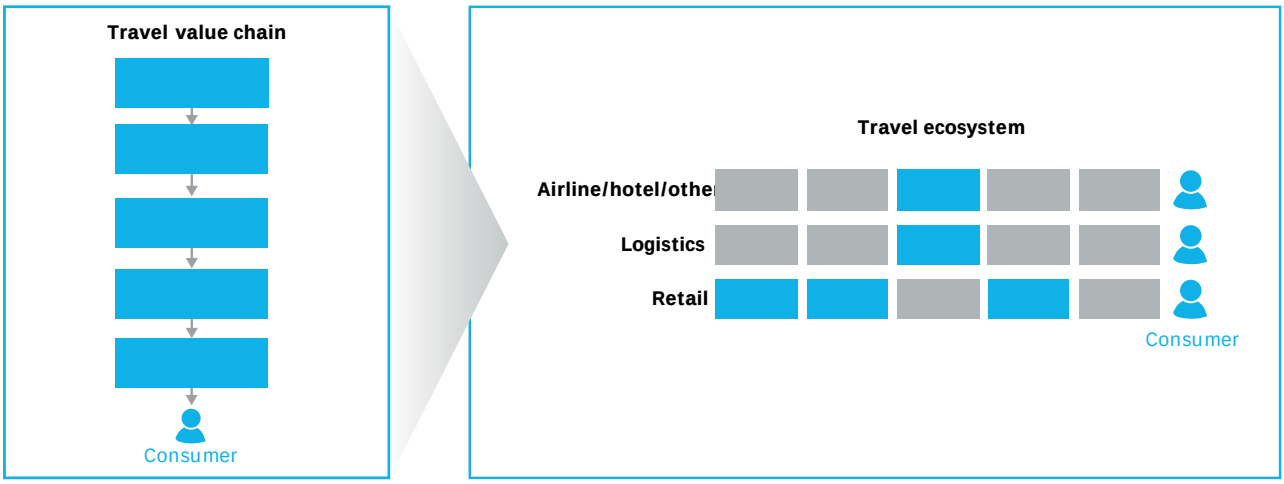


Figure 8: Value creation in a Travel ecosystem is based on delivery of the end-to-end travel experience.
Source: Travel 2020: The distribution dilemma" and "New routes to profitability." IBM Institute for Business Value.

is extracted by a party that orchestrates the delivery of service, not just the travel provider or asset owners. Key travel ecosystem players include airlines and hotels that provide the primary perishable "good," the retail industry that provides travel-relevant goods, and the logistics industry that provides baggage pick-up and delivery.

Price is determined by consumers' willingness to pay for the travel experience – consisting of a personalized package of goods and services rendered. Airlines and hotels are already experts at pricing perishable assets like rooms and seats based on specific willingness to pay criteria of individual consumer segments. But as the ecosystem emerges and expands, the number of variables they must optimize against will also increase. Soon, prices will need to be set on the basis of what each individual is willing to pay for the specific set of goods and perishable services that meets personal preferences. Such pricing algorithms will need to be robust enough to include variables collected not just across the travel domain, but also across retail, social media and other sources of information that can inform an estimate of an individual's willingness to pay.

A RADICALLY DIFFERENT AUTOMOTIVE/MOBILITY ECOSYSTEM

In a traditional automotive value chain, value is tied primarily to the vehicle and controlled by the original equipment manufacturer (OEM). Additional value is contained in ancillary products and services including suppliers, dealership networks, tire and automotive maintenance providers, gas stations, auto parts stores, insurance providers and the like (see Figure 9). Value creation is focused on product differentiation and supporting services, including upgrade options like leather interiors and sun roof, as well as safety ratings and brand exclusivity.

In a future Automotive/mobility ecosystem, value will be tied to the utility gained from the entire mobility experience and associated services, instead of the value inherent in the car itself which acts as means of transportation. Value creation reflects the quality of the overall consumer experience with better consumer experience, creating more value. Supporting services like satellite radio (SiriusXM) and remote services such as OnStar or high speed connectivity improve the enjoyment of the ride and afford greater convenience to

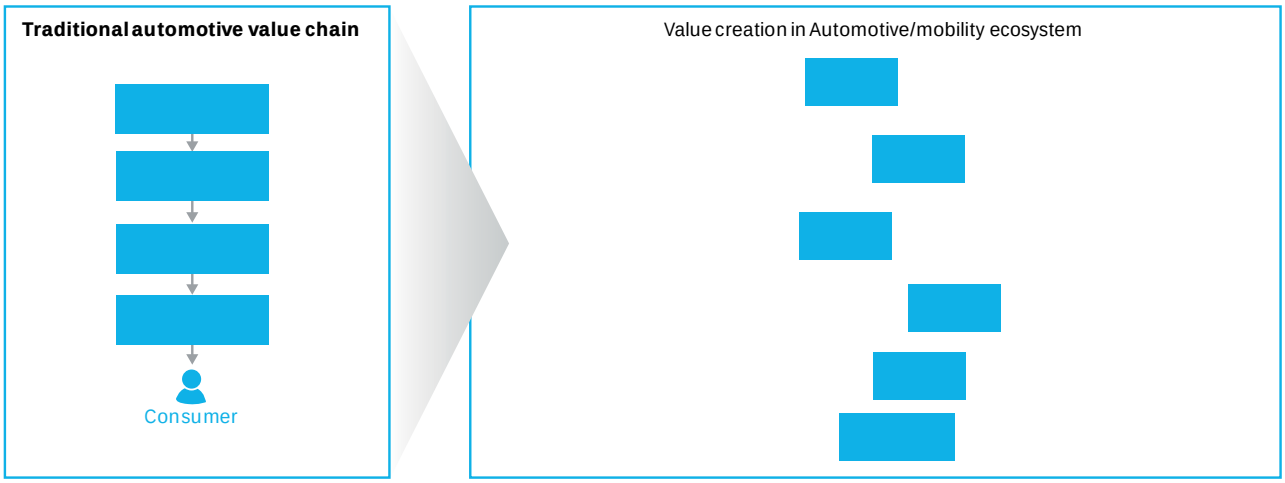


Figure 9: Value creation in an automotive/mobility ecosystem is tied to utility gained from the entire mobility experience.

the consumer. Since the experience creates more value, the consumer is likely to have a greater willingness to pay. Value will also likely shift from the automotive manufacturer and distributor to the mobility ecosystem orchestrator.

KEY DIMENSIONS OF AN E2E ECONOMY

Just as the organization-centered economy gave way to the individual-centered economy, a new sea change is brewing. The maturation of social media, mobility, analytics and cloud are motivating a transition from an individual-centered to an *everyone-to-everyone (E2E) economy.*

E2E is characterized by hyper-connectedness and collaboration of consumers and organizations across the gamut of value chain activities: co-design, co-creation, co-production, co-marketing, co-distribution and co-funding. In this integrated system, consumers and organizations work together to create value, with transparency driving trust and effectiveness. The differences among the three types of economic models can be illustrated by considering four key dimensions: connectivity, interactivity, awareness and intelligence (see Figure 10).

CONNECTIVITY: HOW IS THE ECOSYSTEM COORDINATED AND WHAT ARE THE DRIVING FORCES?

In an organization-driven economy, connectivity is best described as asymmetric. Information flows in one direction – from the organization to the consumer. Traditional insurance is one example, both because insurance costs are driven up by unknown risks that drive complexity and because there is limited visibility into operations of insurance providers such as how premiums are determined and approval/claims processing.

In the individual-centered economy, flexible connectivity prevails, thanks to a supply chain that is transparent and automated. Traffic management systems are an example of connectivity that is more digitally mature than in an organization-driven setting. For example, real-time traffic management information systems such as Bitcarrier get data from wireless network activity and the information enables active traffic management and identifies pedestrian movements.7 Knot Standard, a clothing retailer, allows individuals to order custom-fitted suits, shirts and other men's clothing by transmitting their measurements digitally via webcam or other methods, including use of a local tailor or an old suit. The company

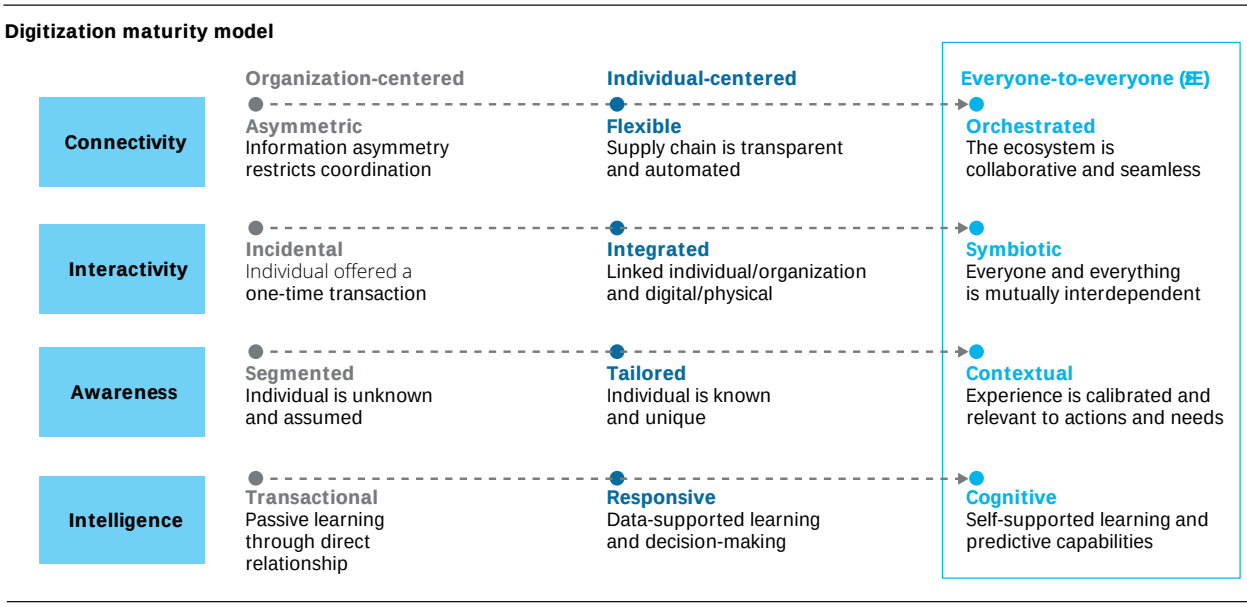


Figure 10: A comparison of "digitization maturity" for three economic models: organization-centered, individual-centered and E2E. An E2E environment is orchestrated, symbiotic, contextual and cognitive.

guarantees a "100% perfect" product to be shipped in 20 days.[8]

In the future, connectivity will become orchestrated, within an ecosystem that is collaborative and integrated. An example of this is Kiva.org, a microfinance non-profit provides small, interest-free loans around the world. Through its online community of over 600,000 lenders, Kiva has issued over US$250 million in loans to hundreds of thousands of people in 60 countries since 2005. With U.S. loans comprising less than 1 percent of borrowers, it partnered in 2010 with Visa on a program to help small Gulf Coast businesses get microloans. Expanding further, Kiva formed Kiva City with the Clinton Global Initiative to serve small businesses in American cities by collaborating with civic leaders, community organizations, financial institutions and lenders. Within three hours of launching in Detroit, Kiva raised over US$25,000 to help fund five local start-ups and 14 loans totaling more than US$125,000 were fully funded within 24 hours of launching in New Orleans.[9]

INTERACTIVITY: WHAT IS THE DEPTH OF RELATIONSHIP BETWEEN THE INDIVIDUAL AND THE ORGANIZATION?

In an organization-centered economy, interactivity is best described as incidental, where an individual is offered a one-time transaction. Interaction between organization and consumer only occurs because it is necessary for a transaction to be executed. Product-focused retailers are one example, operating with high turnover, low margin and low-value transactions. Here, the goal is to maximize volume as a priority over developing long-term, personal consumer relationships.[10]

By comparison, the interactivity in an individual-centered economy is integrated, linking individuals with the organization, as well as linking the digital with the physical. Digitized eyewear purchasing is an example of integrated activity that is more digitally mature than in an organization-driven setting. Retailers such as Warby Parker offer online, direct-toconsumer sales for eyewear bypass physical outlets. Online retailers focus on low prices and

convenience as they digitize physical products: consumers can receive glasses to try on at home or try on glasses virtually.[11]

The future of interactivity will be symbiotic, in which virtually everyone and everything are mutually interdependent. An epidermal electronic system is such an example. Electronic circuits that are like a "second skin" and are aware of a user's cognitive state can stimulate tissues for rehabilitation. Future applications are expected to blur the physical and digital further and extend to include external limb control, sub-vocal communication and military uses.[12]

AWARENESS: WHAT IS THE DEPTH OF MARKET INSIGHT AND IS IT REFLECTED IN THE CONSUMER EXPERIENCE?

In an organization-driven economy, awareness is segmented, with individuals being both unknown and assumed. Traditional beverage marketing illustrates this approach. Beverages maintain classic flavors with some regional diversity. Manufacturers use traditional demographic and psychographic consumer segmentation to promote products.[13]

But in an individual-centered economy, awareness is tailored and each individual is known and unique. Mass customization in retail is an example of awareness that is more digitally mature than in an organization-driven setting. For example, Jockey, a clothing manufacturer, developed a new volumetric bra featuring a new sizing system offering 55 size combinations based on surveys of women. These size combinations create a mass-customized alternative to existing bras, which are often described as ill-fitting.[14]

The future of awareness will be contextual, with an experience that is calibrated and relevant to each individual consumer's preferences, location and moment in time. An example of this is a projected future retail experience: retailers integrate data across multiple sources, combining location, behavior, servicing, social, virtualization, fulfillment and access to create a "for-me-only" experience. The provider of the retail experience may, in fact, know the consumer better than the consumer knows his- or herself. The future contextual experience may even be capable of turning on when needed and off when not wanted.15

INTELLIGENCE: HOW IS DECISION-MAKING INFORMED?

In an organization-driven economy, intelligence is primarily transactional, which results in passive learning through direct relationship. Traditional telephony illustrates transactional intelligence since providers offer combinations of subscriptions and service packages that can be flexibly combined, but do not vary based on usage history or length of consumer relationship.[16]

By comparison, an individual-centered economy has responsive intelligence, featuring data-supported learning and decision making. Energy optimization systems are an example of intelligence that is more digitally mature than in an organization-driven setting. Optimization systems like the Nest learn user preferences and behavior for smart energy management.[16] These systems leverage data to support convenient product usability and future development of energy efficiency services.[17]

In the future, intelligence will become cognitive, using probabilistic techniques that enable computer-based decision making. One example of this is applying the artificial intelligence of IBM Watson in the field of medicine. Watson will soon help diagnose medical conditions by leveraging its cognitive ability and ingested medical documentation, and continuously learning from mistakes. In a recent test, Watson successfully diagnosed lung cancer 90 percent of the time compared to 50 percent for human doctors.[18]

GUIDING PRINCIPLES FOR AN E2E ECONOMY

Heightened consumer expectations for seamless, connected experiences and increased collaboration among organizations characterize the E2E. To find direction within complexity, consider these guiding principles:

- ***Organizations will only be as relevant as their ability to deliver the best experience through the right partner ships.*** Consumer experiences will require services from different providers, and will demand that companies work together to adapt. Value delivered to customers will not be concentrated in one company, but distributed across multiple organizations. The ability to attract, assemble, manage and retain the right organizational partners will be a differentiator for success in the E2E marketplace. Ecosystems require trust and mutuality – open lines of communication and shared agility are vital.

- ***The demand for data by contextual and predictive analytics will become insatiable.*** Consumer experiences will require a highly contextual understanding of users and their needs through data insight. Creative and innovative integration of transactional, behavioral and contextual data are necessary ingredients to produce value for customers. Organizations need the ability to capture, analyze and model data to extract – and then act upon – profound insights, and then make these insights available to partners. Information sharing and the ongoing process improvement will need to become 'business as usual' to gain operational efficiencies within and across partnerships.

- ***Open standards do not mean the end of intellectual property – successful organizations will protect what they do best and open up the rest.*** In the age of specialization, the imperative of protecting critical intellectual capital will need to be balanced against the imperative of being integrated into dynamic and flexible ecosystems. Secrecy will increasingly be replaced by openness within the context of strong and enforceable intellectual property rights.

THE NEW DIGITAL REINVENTION FRAMEWORK

A new innovation layer – beyond the traditional definition of digital transformation – is emerging. Organizations should continue to invest in individual-centricity while recognizing it is just the first step toward the radical digital reinvention in the future.

The E2E economy requires reinvention of markets, strategy and value from the ground up. And with the shift to E2E, the historical Digital Transformation Framework is being replaced by a new Digital Reinvention Framework (see Figure 11) which features orchestrated connectivity, symbiotic interactivity, contextual awareness and cognitive intelligence.

BECOMING ORCHESTRATED, SYMBIOTIC, CONTEXTUAL AND COGNITIVE

Successful organizations will be open to the challenges ahead and rethink all aspects of their business. Above all, they must decide where to focus. The future will be very different from the present.

Rethink how your organization interacts with consumers and markets. Do not allow what is possible today (given existing IT or other capabilities) to limit you. After defining compelling experiences, identify monetization opportunities and technical/ organizational requirements. Develop the business case and make investment decisions accordingly.

Next is the decision about how to focus. In the

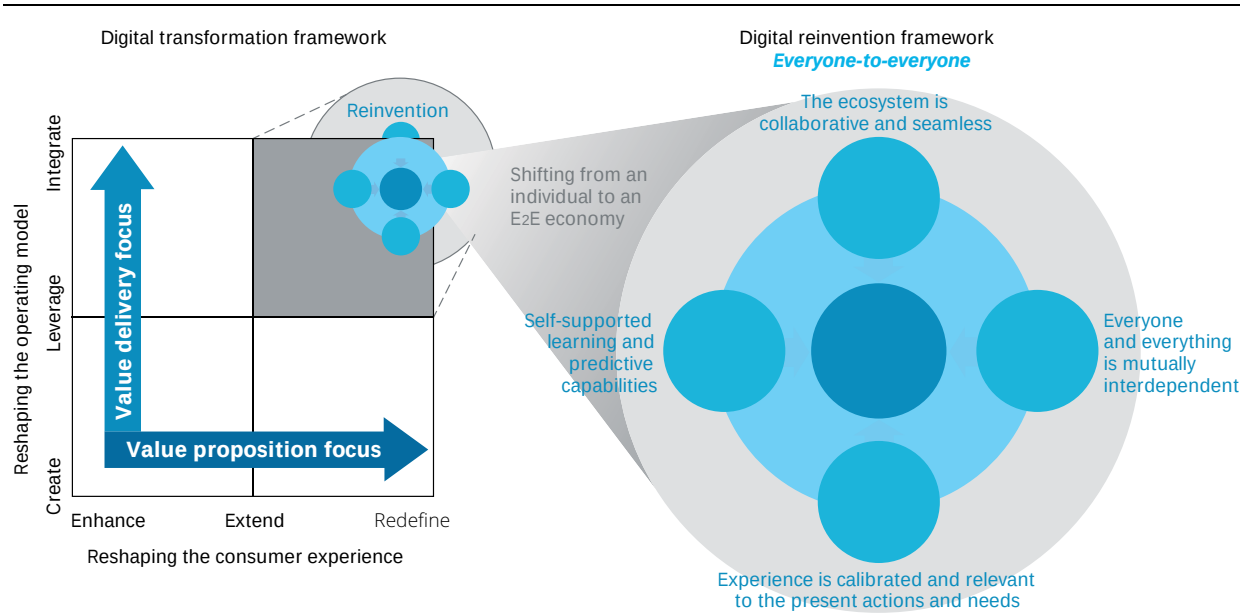


Figure 11: The new Digital Reinvention Framework supports the E2E economy.
Source: 2011 IBM Digital Transformation Study and 2013 IBM Institute for Business Value analysis.

future, organizations will become even more specialized than they are today. Understanding what you are good at will become essential. Take a highly critical, impartial look at what you do well, and what others do better. Agree to focus your efforts on those activities that truly differentiate you from your competition. Make investments there, to build and maintain a position of excellence. Source most or all of the other functions in your business to top providers. Focus on those activities that differentiate you.

The other facet of determining where to go is building and integrating new capabilities. Skills and capabilities required for business change through time – those required for success in the future will not necessarily be those that have contributed to success in the past. Take an objective look at what skills and capabilities you have today, what will be required in the future and move aggressively to retrain or recruit. Think through new models of investment, metrics and incentives, and begin building an organization designed for the future.

STEP ONE: OPEN UP TO EXTERNAL INFLUENCES

Turbocharge insight. For many organizations, market or competitive insight has struggled to keep up with new technologies around social media and big data. Yet insight will play an ever-more important role in understanding not only changes in consumer attitudes and behavior, but also looking across industries to scope business model possibilities and implications of new technologies. Upgrade insight to encapsulate capabilities such as social analytics and scenario envisioning. Build better processes to detect weak but potentially profound signals from supply chains or partner networks and channel them into IT and the business.

Embrace digital natives. Managers will need to look at their businesses differently. Markets are unlikely to incrementally evolve as they once did. Organizations will be much more susceptible to disruption coming from both inside and outside their industry parameters. Millennials and other digital natives are much more likely to anticipate the power of new

technologies and experiences. Build processes that channel insights directly from Millennials to permeate the C-suite and others.

Internalize consumer influence. Consumer influence in most organizations tends to be filtered through the sales organization or the CMO. Such filters inevitably create distortions. Invite consumers to participate in ideation, project evaluation and development processes, as well as in fundamental business strategy development. Establish processes for consumers to have a real say in key business decisions. Increase decision making permeability, and rethink key initiatives as consumer collaborations.

STEP TWO: CONNECT TO NEW ECOSYSTEMS AND PARTNERS

Conceptualize ecosystem parameters. In the future, organizations will operate in ecosystems of converging products, services and industries. By focusing on single products or transactions, organizations will miss the big picture. Become proficient in understanding new ecosystems as they emerge. Identify and assess new sources of value and define where your organization might sit and what role it might play. Develop mechanisms to identify new opportunities and train your people to anticipate emergent threats to your business.

Build systemic connectivity. Application programming interfaces (APIs, a set of protocols for building software applications) and cloud computing are the tissue connecting ecosystems of organizations and individuals. The influence of APIs and cloud go far beyond the IT department. If handled right, APIs and cloud can empower dynamic new business models, consumer interactions and organizational flexibility. To position strategically for the future, combine technology strategy with business strategy. Compel IT to work with the business and the business to work with IT. Test what is possible with new technologies and anticipate the unexpected by maintaining technical and operational flexibility.

Establish ecosystem partners. In the future, the most successful organizations are likely to be those who partner with the right organizations or people in the right ways. No single organization can hope to do everything required in new ecosystems. But partnering with anyone will introduce risk and confusion. Successful organizations will understand their capabilities and how to realize synergies with ecosystem partners. Find partners who can further your objectives and decide how you want to partner. Prioritize those that do things that are not easily replicable. Partner with world class organizations, even if they happen to be small. Explicitly align objectives both informally and contractually.

STEP THREE: INVEST IN DIGITAL MOBILIZATION ACROSS THE ORGANIZATION

Appoint digital torchbearers. Succeeding in the E2E economy will require fundamental rethinking of markets, consumers and products and services. It is likely that some business units and employees will struggle with understanding new imperatives and the change required. Appoint specific individuals to be digital torchbearers. In circumstances where the C-suite struggles to embrace new imperatives, consider appointing a Chief Digital Officer. Mandate these individuals with influencing strategy and educating other executives. Give them real authority, including a say in approving new projects and other investments.

Secure functional/business unit buy-in. Functional or business unit groups may become insular and self-focused, losing sight of overall strategic goals. Interactions between IT departments and business units can often be strained. Business complains that IT does not understand consumer imperatives; IT complains that the business does not

Key steps for reinvention: 1. Open up to external influences, 2. Connect to new ecosystems and partners, and 3. Invest in digital mobilization across the organization.

understand technical feasibility. Yet digital reinvention will require IT and the business to work together like never before. Compel a closer working relationship. Co-location, cross-functional tours of duty and combined planning exercises are among initiatives that might be pursued.

Pursue continuous innovation and experimentation. Investing in consumer-centricity remains necessary and desirable. Successful organizations are currently rethinking consumer imperatives and building compelling consumer experiences. But invest in consumer-centricity with knowledge and sensitivity to what will emerge beyond. As new technologies mature and businesses adapt, the economy will begin to shift from an individual-centric to an E2E paradigm. Think about how to shift as well – continuously identify opportunities, conceive business models and navigate new ecosystems. Pursue experimentation, and apply the results of experiments to the business if successful.

BEGIN REINVENTING: ASK THE RIGHT QUESTIONS

Organizations must be inquisitive and open to the challenges ahead. The following questions can help:

- What fundamental consumer needs have you been serving? What new experiences can address those needs?
- How will you identify your core strengths? What is the best way to increase investments in those true differentiators?
- In what ways can you identify new potential sources of value, and where in emerging ecosystems should you engage?
- What can you do to assess current skill levels and capabilities objectively? How should you acquire new skills to fill gaps?
- What sorts of digital torchbearers already exist in your organization? What can you do to incorporate their influence into strategy and education?

SEIZE THE FUTURE THROUGH DIGITAL REINVENTION

Until the turn of the century, the most powerful impacts of new technologies have taken years to emerge. Today, we're experiencing the transformative impacts of social media, mobile, analytics, cloud and other technologies at a highly-accelerated pace. Digital disruption has begun: it marks the start of a new technological and economic paradigm requiring the re-imagination of markets, strategy – and value itself.

Organizations must start reinventing themselves from the ground up to remain competitive. On one hand, rapid digitization is creating new value and new opportunities for organizations to gain influence and innovate. On the other, established norms are in peril due to the blurring of traditional industry definitions and formation of new ecosystems. To prepare for a radically different tomorrow, those who seek to prosper under digital disruption should constantly redefine strategy in terms of how best to open up to external influences, connect to new ecosystems and partners, and how they can drive digital mobilization across their organizations.

IBM INSTITUTE FOR BUSINESS VALUE

To learn more about this IBM Institute for Business Value study, please contact us at iibv@us.ibm.com. For a full catalog of our research, visit: ibm.com/iibv

Access IBM Institute for Business Value executive reports on your tablet by downloading the free "IBM IBV" app for iPad or Android from your app store.

RELATED PUBLICATIONS

"The Customer-activated Enterprise: Insights from the Global C-suite Study." IBM Corporation. October 2013. http://www-935.ibm.com/services/us/en/c-suite/ csuitestudy2013/

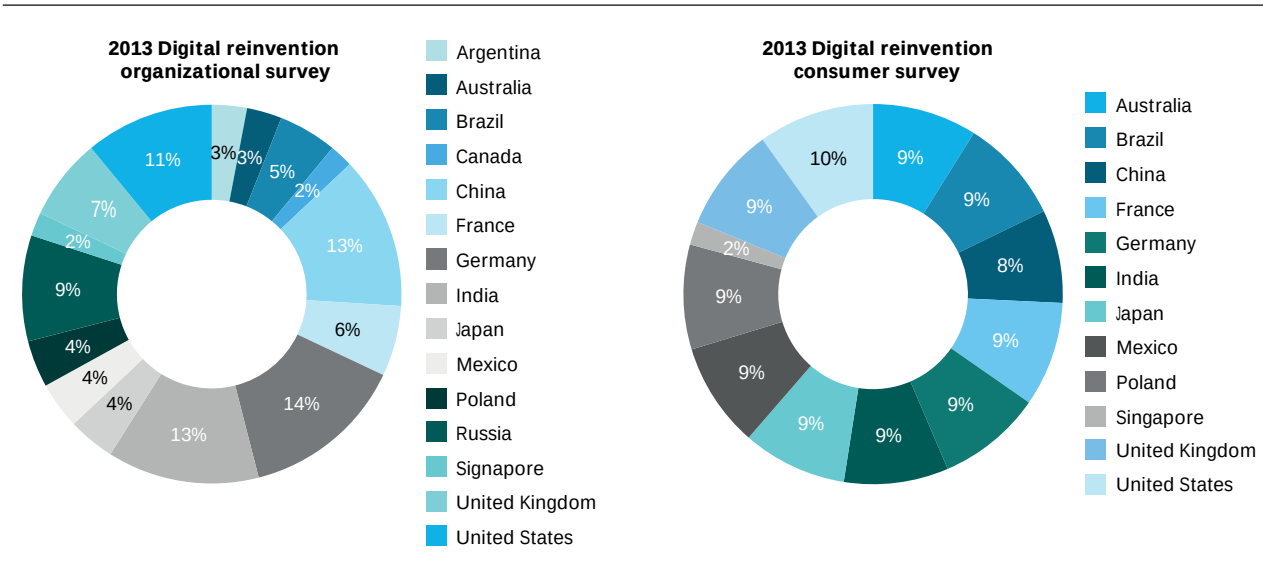
"Leading through Connections: Insights from the Global CEO Study." IBM Corporation. May 2012. http://www-935. ibm.com/services/us/en/c-suite/ceostudy2012/

Berman, Saul J. and Ragna Bell. "Digital transformation: Creating new business models where digital meets physical." IBM Institute for Business Value. April 2011. http://www-935. ibm.com/services/us/gbs/thoughtleadership/ibv-digitaltransformation.html

APPENDIX: METHODOLOGY OF THIS STUDY

For the 2013 IBM Digital Reinvention Study, we surveyed approximately 1,100 business and government executives and 5,000 consumers across 15 countries (see pie charts). Thirty leading futurists were also interviewed.

Of those interviewed for the executive study, 42 percent are C-level executives, with Chief Executive Officers comprising 10 percent of that group. More than three-fourths of the consumer study participants are university graduates, with 68 percent between the ages of 25 and 54.



Survey respondents by country.

ABOUT THE AUTHORS

Saul J. Berman, Ph.D. is Partner and Vice President, Global Service Area Leader for Strategy and Transformation within IBM Global Business Services. He works closely with major corporations around the globe on strategic business issues. He has more than 25 years of consulting experience advising senior management of large corporate and start-up organizations and was named as one of the Top 25 Consultants of 2005 by Consulting Magazine & Top 50 Marketing executives over 50 by Global CMO Magazine. Saul has authored numerous books and publications including Not For Free: Revenue Strategies for a New World and IBM Institute for Business Value executive reports, "Beyond digital: Connecting media and entertainment to the future" and "The power of cloud: Driving business model innovation." He can be reached at *saul.berman@us.ibm.com.*

Nadia Leonelli is part of the IBM Strategy and Transformation Center of Competency, a globally integrated team of senior strategic innovators and subject matter experts, advising global brands on marketing, digital and product development challenges. She has over fifteen years of managerial, entrepreneurial and consulting experience focused on corporate strategy, marketing and product development across consumer-driven industries. Nadia collaborated in 2011 on the two executive reports from the IBM Institute for Business Value, "Beyond Content" and "A Future in Content(ion)," which look at the business implications of digital content markets. She can be reached at *nleonelli@us.ibm.com.*

Anthony Marshall is Program Director of IBM's Global CEO Study, and Strategy and Transformation Leader in IBM's Institute for Business Value. Anthony has 20 years experience in consulting and analysis, working with numerous Global 1200 companies. He was Senior Managing Consultant in IBM's Strategy and Innovation Financial Services Practice, and has deep public sector experience, particularly in privatization and deregulation. Anthony has lectured in economics at Barnard College in New York City, and Universities in Australia. He is currently publishing in the areas of innovation, digital strategy, technology-enabled business models, ecosystems and partnering. He can be reached at *anthony2@us.ibm.com.*

CONTRIBUTORS

Paul Papas, Global Leader, Digital Front Office, IBM interactive and Smarter Commerce, IBM Global Business Services
Peter Korsten, Global Leader, Thought Leadership and Innovation, IBM Global Business Services
Eric Lesser, Research Director and North America Leader, IBM Institute for Business Value, IBM Global Business Services
Jennifer Kim, Strategy Consultant, IBM Global Business Services
Rachna Handa, Managing Consultant, IBM Institute for Business Value, IBM Global Business Services
Joni McDonald, Content Strategist for Thought Leadership, IBM Sales and Distribution
Artour Parmakian, Director of User Experience, IBM Interactive
Geoffrey Hamelin, Global Business Advisor, Strategy & Transformation, IBM Global Business Services
Steven Davidson, Global Leader, GMU Strategy and Transformation, IBM Global Business Services
Martin Harmer, Vice President and Senior Project Executive, IBM Global Business Services
Steve Peterson, Travel and Transportation Lead, IBM Institute for Business Value, IBM Global Business Services
Benjamin Stanley, Automotive Lead, IBM Institute for Business Value, IBM Global Business Services

ACKNOWLEDGMENTS

We would also like to thank Linda Ban, Kali Klena, Steve Ballou, Kathleen Martin, Henry Inman, John Calkins, Robert Murray, Alex Giammarco, Raghav Virmani, Corey Leong, Rebecca Shockley and Heather Fraser.

REFERENCES

1. "The Customer-activated Enterprise: Insights from the Global C-suite Study." IBM Corporation. October 2013. http:// www-935.ibm.com/services/us/en/c-suite/csuitestudy2013/
2. Ibid.
3. Ibid.
4. Berman, Saul J. and Ragna Bell. "Digital transformation: Creating new business models where digital meets physical." IBM Institute for Business Value. April 2011. http://www-935. ibm.com/services/us/gbs/thoughtleadership/ibv-digitaltransformation.html
5. The Ritz-Carlton Leadership Center. http://corporate.ritzcarlton.com/en/LeadershipCenter/. Accessed on December 2, 2013.
6. ARM: Growth Champions. Growth Champions, "ARM." http://growthchampions.org/growth-champions/arm-2/. Accessed on November 9, 2013
7. IBM Institute for Business Value analysis informed by existing home energy and security management solutions.
8. Knot Standard. "Use your webcam." http://www.knotstandard. com/use-your-webcam/. Accessed on November 7, 2013.
9. Schwartz, Ariel. "Kiva City: Using microloans to revitalize small businesses in struggling American cities." Fast Company. September 8, 2011. http:// www.fastcoexist.com/1678497/ kiva-city-using-microloans-to-revitalize-small-businesses-instruggling-american-cities; Kiva press release. "Kiva celebrates six years of online micro lending, honors its one million-strong community." October 19, 2011. http://www.reuters.com/ article/2011/10/19/idUS179849+19-Oct-2011+MW20111019.
10. "Revenue models: Low-value transactions." MaRS. http://www. marsdd.com/articles/revenue-models-low-value-transactions/. Accessed on November 1, 2013. ; Hurlburt, Ted. "A Tale of Two Business Models." 2013. http://www.businessknowhow.com/money/retail-model.htm. Accessed on November 1, 2013.
11. O'Toole, Mike. "Warby Parker, One Million Eyeglasses, And The Next Generation Of Brands." Forbes. CMO Network. July 22, 2013. http://www.forbes.com/sites/mikeotoole/2013/07/22/ warby-parker-one-million-eyeglasses-and-the-next-generationof-brands/. Accessed on November 1, 2013.
12. "Stick-On Tattoos Go Electric." National Science Foundation. August 11, 2011. http://www.nsf.gov/news/news_summ. jsp?cntn_id=121343. Accessed on November 1, 2013.
13. Wind, Jerry and David Bell. "Market Segmentation." The Marketing Book. October 3, 2007. https://marketing.wharton. upenn.edu/files/?whdmsaction=public:main.file&fileID=566. Accessed on November 1, 2013.
14. Clifford, Stephanie. "A New Step in Wrestling with the Bra." The New York Times. Business. May 30, 2013. http://www. nytimes.com/2013/05/31/business/a-new-step-in-wrestlingwith-the-bra.html. Accessed on November 1, 2013.
15. "From Transactions to Relationships, Winning over the empowered Consumer." IBM Corporation. January 8, 2013. http://www-935.ibm.com/services/us/gbs/thoughtleadership/ transitioningshopper/; "Analytics: The real-world use of big data in retail." August 8, 2013. http://www-935.ibm.com/ services/us/gbs/thoughtleadership/big-data-retail/
16. "The End of the Line." The Economist. Special Report. October 12, 2006. http://www.economist.com/node/7995301. Accessed on November 1, 2013.
17. Nest. http://www.nest.com; Henry, Alan. "What Can a Smart Thermostat Do that Mine Can't Already Do?" August 15, 2013. http://lifehacker.com/what-can-a-smart-thermostat-do-thatmine-can-t-already-472975733. Accessed on November 1, 2013.
18. Ibid.
19. Steadman, Ian. "IBM's Watson is better at diagnosing cancer than human doctors." Wired. Technology. February 11, 2013. http://www.wired.co.uk/news/archive/2013-02/11/ibm-watsonmedical-doctor. Accessed on November 1, 2013.

CHAPTER 6

MALAYSIA ICT 2014 TOP 10 PREDICTIONS: FLOODED WITH TECHNOLOGY BUT ANCHORED BY THE 3RD PLATFORM

ROGER LING
Associate Research Director
rling@idc.com

IDC
Analyze the Future

PREDICTIONS

This year's predictions — themed "Are We 3rd Platform Ready?" — Focuses on providing an understanding on local sentiments surrounding the market, business and technology trends, with reference to the four pillars of transformation (cloud, Big Data and analytics, social, and mobile) that will affect the nation in the next 12–18 months.

The following have been identified as the key predictions for the Malaysian market in 2014:

1. IT Spending Will Be Back on Track Surpassing the US$10 Billion Mark
2. Data Revenue Will Take Pole Position in 2014
3. Adoption of Cloud Solutions Will Move from Conceptual to Practical
4. Enterprise IT to Remain Unconvinced about Achieving "Returns on Mobility"
5. Malaysia's Big Data Market Anticipated to Hit US$24.2 Million But Will Remain Tactical in Nature
6. Enterprise Social Networking: Sandbox for Peak Internal Collaboration in 2014 Will Be a Priority
7. Channel Transformation in the 3rd Platform Will Be a Key Agenda in 2014
8. BYOD Is Real and Happening Now, and Organizations Will Need to Make a Stand on What It Means
9. Government to Connect to Citizens via Mobile Devices and Social Media, Accelerating a New Type of Citizen and Government Relationship
10. Innovation in the 3rd Platform Will Create Unique Mash-up Opportunities But May Also Create a Perfect Storm for Project Failure

This document serves as an update to the above set of predictions and highlighting where Malaysia is at as of June 2014.

SITUATION OVERVIEW

For the past 40 years, the IT industry has periodically refreshed itself on new solutions, business models, and industry structures — but always rooted to a platform, for ecosystem, solutions creation, and delivery. Looking at the bigger picture, what truly separates the different eras is a shift in platform, what clearly defines each growth platform is not so much the technologies but the scale and scope of users and uses the technologies enable.

Across Southeast Asia, there continues to be pockets of examples of the rise of the adoption of 3rd Platform technologies and solutions with Malaysia not being an exception. That said, the actual business use cases are few and far in between and, while the country takes key measures in the form of Digital Malaysia, there continues to be questions if the nation is in fact 3rd Platform ready.

IN THIS UPDATE

PREDICTION #1: IT SPENDING WILL BE BACK ON TRACK SURPASSING THE US$10 BILLION MARK

IN RETROSPECT

IDC predicts that in 2014, Malaysia's IT spending will be back on track, finally crossing the US$10 billion mark. While this was initially predicted for 2013, the Malaysian market was impacted by various forces that led to a landscape change resulting in a slowdown. Key to this is what IDC terms as "Technology Flood," a concept brought about by the hyper-compete landscape as introduced in the 2013 predictions. At the close of 2013, it is apparent that while technology spending still registered healthy growth, albeit lower than forecast, what was lacking was the transformative change agent that allows IT to enable business transformation. Sub-US$150 smartphones, traditional software and hardware spending to "keep the lights on" pushed the envelope for growth, but IT services spending saw a much slower growth.

IDC sees 2014 as a platform for a possible inflection point for growth, but it will not be without both challenges and opportunities. The following are IDC's expectations on IT spending for 2014:

- Malaysia's IT spending will surpass US$10.5 billion with the mix of technology segments remaining status quo with no disruption. Telecom equipment, IT services, and client systems will make up 79% of Malaysia's IT spending. With the flooding of technology, especially for smartphones and client systems, IDC sees opportunities for the ecosystem to evolve to cater to the increased demands for mobility.

- While double-digit growth is expected for both IT services and Telecom equipment moving into 2014, decline for both peripherals and client systems will be likely. IDC notes that for technology segments with services attached beyond break-fix support, there is increased demand for IT transformation, which leads to further IT spending opportunities.

- Malaysia's IT spending proportion to Southeast Asia's six economies will decline over the forecast period from 16.7% in 2014 to 15.5% in 2017. While it is noted that strong infrastructure buildup in emerging economies, such as Indonesia and Vietnam, leads to greater IT spend, Malaysia takes the same path of Singapore with the decline. IDC does not necessarily see this as positive, given Thailand is still heading toward increased IT spending growth on par with other Southeast Asia's six economies.

IDC sees overall IT spending for Malaysia as generally fragmented, so while IT spending is moving in the right growth direction, IDC also cautions that in 2014 and beyond without transformation anchored by the 3rd Platform, the nation may just be flooded with technology. In 2014, Malaysia is expected to hit a 24% IT services penetration and by 2017 only hitting 25%.

UPDATE

IDC's Version 1, 2014 of the IT Spending Blackbook points to Malaysia already crossing the U$ 10 Billion mark at U$ 10.3 Billion. On the onset, the numbers are positive but it is also reflective of a slowdown as the previous version of the Blackbook forecasted a 2014 close of U$ 10.7 Billion. IDC is of the opinion that while this is still positive the possibility of a technology flood is still a key point that needs to be addressed.

Looking back at the past 6 months of 2014 it is clear that the IT ecosystem as a whole is in the process of evolving to address the 3rd platform and while this is a continuous

process that takes time, the local IT ecosystem is impacted. Changes in strategic directions by global vendors will trickle down and impact local channels. It will be imperative for the local IT ecosystem to evolve in line to ensure both business continuity and gearing up for the transition in platform at the same time. Should this not take place the impact of the technology flood will be detrimental as questions on Return on Investment will plague decision making moving forward.

IDC is of the opinion that the current state is representative of growing pains as the transition takes place and it will be imperative for players in the IT ecosystem to work towards a business model and strategy that ensures sustainable growth in the face of disruption. IDC is also of the opinion that the current state of limbo will also eventually phase away as both the supply and demand side synergize to create win-win scenarios founded on technology.

PREDICTION #2: DATA REVENUE WILL TAKE POLE POSITION IN 2014

IN RETROSPECT

Telecom service providers (SPs) across the region, including Malaysia, continue to transform their business to remain relevant in this dynamically changing landscape. This collision of market forces, players, and ecosystems has made the landscape more complex for many telcos, with many remaining extremely cautious in moving into new territories and adjacent markets. IDC believes that the Telecom SP of the future will be, or should be, radically different from what it is today. The next trillion dollar opportunity for telcos in the region will come from value-added services (VASs) that will be built over their network infrastructure, which will be core to their service provisioning.

IDC expects the telecom services market to hit a steady 8% year-over-year (YoY) growth at the close of 2014, up by 1% from the previous 7% growth experienced in 2013. The positive outlook also represents a landmark theme where data revenue gains dominance by leading in contribution for the first time over voice. In 2014, expect data revenue to contribute over 53% of the telecom services market and by 2017 67%. IDC sees the growth in data revenue as a fundamental necessity for the 3rd Platform, as it provides the ubiquity in access necessary for proliferation. The shift also signifies the need for Telco SPs to innovate to succeed with dwindling voice revenue streams ahead.

The dominance of data is a direct result of a shifting technology landscape. It is to no surprise that 2014 will see the further collapse of feature phones with expected YoY decline of over 17%, while Smartphones and tablets will see healthy double-digit growth. Key to this will be the dominance of these devices, of which IDC predicts that by 2017, 32% or IT spending or US$4 billion will be driven purely by these two device segments.

While IDC sees the dominance of data revenue, as well as the growth of Smartphones and tablets, to be encouraging, key to avoiding just a "technology flood" will be the role the Telco SPs play in a larger ICT ecosystem. 2014 will be a pivotal year for not only planning on transformation but executing key successful initiatives that will enable business in the age of the 3rd Platform.

UPDATE

Fixed data has been dominating the overall fixed line services market since 2010. Network expansion and upgrades by Telco SPs and government initiatives has enabled more fixed services to larger areas. IDC's latest research indicates that businesses in Malaysia are beginning to look at solutions and managed services as a next step for growth and although Telco SPs have a slight upper hand due to their

incumbent status as connectivity providers the focus has been more reactive than anything else. IDC predicts fixed data to continue to grow strongly reaching 12% in 2014 compared to the previous year, with a CAGR of 11% by 2017. That said, IDC notes that the low hanging fruits as seen as the run rate provided through fixed data to also be the Achilles' heel, for Telco Service Provider transformation.

On the other hand, mobile data will still make up 42% of the total mobile services market at end of 2014, despite its strong growth in the last few years. As mobile voice service is expected to suffer a steady decline in the next five years, mobile data is now the key driver for mobile SPs in order to stay competitive and retain their revenue growth. IDC predicts mobile data to surpass mobile voice in 2017. The growth of mobile data in the next five years will be driven by the increase of low-tier smart devices, affordability of mobile data package, richer media contents especially by Over-The-Top-Players (OTTP) and enhanced user experience by 4G LTE.

IDC is of the opinion that growth either through coverage area or revenue will be a necessary fundamental for the proliferation of the 3rd platform. As Telco SPs look to competing on the traditional front, IDC also expects Telco SPs to take a keen step in transformation to be an end-to-end ICT provider. While it is unlikely that the impact will be drastic in 2014, IDC is of the opinion that the foundational layers are already being set in place for increased competition in 2015. The entrant of foreign Telco SPs with experience in providing end-to-end ICT solutions and the focus of local super regionals in expanding beyond Malaysia will also serve a catalyst for the transformation of local Telco SPs to compete. Moving forward IDC expects the landscape to change as Telco SPs focus on competing beyond the communication space and into other disciplines of IT.

PREDICTION #3: ADOPTION OF CLOUD SOLUTIONS WILL MOVE FROM CONCEPTUAL TO PRACTICAL

IN RETROSPECT

Building on from the 2013 cloud predictions, "Cloud Uptake Will Remain Lethargic, But Market Perception of the New Normal Will Provide Building Blocks for Enterprise Cloud Adoption," IDC sees 2014 as the next step forward in laying the foundations for an enterprise cloud. At the close of 2013, the uptake of cloud did remain lethargic with pockets of adoption but not nearing the critical mass needed for it to be a completely disruptive market force. IDC has observed some clear evidence of organizations moving into the cloud with cloud components being discussed as part of either IT services contract renewals or as new initiatives all together. With reference to IDC's 2013 Cloud Adoption Survey, 67% of local respondents agreed that a mindset change has already begun with cloud being perceived as a normal way to provide services within organizations, as well as externally. That said, IDC still perceives the nation as being at a relatively nascent stage of cloud adoption as the mere mindset change of perception does not garner actual real change.

IDCs research points to the nation being ranked at the starting point of Stage 2: Opportunistic based on IDCs Cloud Maturity model. According to IDC's 2013 C-Suite Barometer Study, one of the key imperatives for CIOs is to rely on proven technologies as opposed to bleeding edge technologies. With that, there is no surprise that the move to the cloud is somewhat lackluster in nature. The shift toward researching and testing is best explained by the following findings:

- 26% of organizations still see cloud as an unproven technology, therefore only used for restricted or limited workloads.

- A YoY comparison indicates that over 30% of organizations have increased concerns over the uncertainty of data hosting, reliability concerns in terms of service availability, IT governance and regulatory and compliance, and the difficulty of integration with existing systems or other vendors cloud services.

- Although the magnitude of importance may vary for both public and private, there is a clear callout by IT buyers for cloud providers to understand the core business and industry of organizations they are selling to.

With the findings from 2013, IDC is of the opinion that in 2014, the cloud will move from conceptual to practical with a strong focus by vendors to guide customers in building business cases. Fundamental to this idea is the notion that organizations in general are attracted to the cloud and the only safe and feasible thing to do before adopting it is by researching, and finding the practical business use cases.

With reference to IDC's 2013 Cloud Adoption Survey, 2012 saw no respondents indicate the focus to research and test the cloud, but an overwhelming percentage had plans to move to the cloud within the next 6–18 months. However, in 2013, over 32% of respondents indicate the focus to start researching and testing. IDC is of the opinion that those that were merely riding the cloud bandwagon are realizing a more detailed approach is necessary to move to cloud.

UPDATE

IDC is of the opinion that Cloud will disrupt the existing IT ecosystem. A key question for discussion will be how vendors in each cloud segment (IaaS, PaaS, and SaaS) will seek to extend and better differentiate what they bring to market and how they will face the changing landscape of who they intend to sell to -- in a world where more and more successful Software providers will need to act like service providers, and service providers will need to build software portfolios, and even develop their own new applications. With reference to the local market, IDC is of the opinion that the ecosystem is still in a learning/growing stage, testing both products and strategies to find a place in the 3rd platform. This cuts across the entire gamut of the ICT Ecosystem from IT Service Providers, Cloud Service Providers, Telco Service Providers as well as the channels ecosystem.

In view of the nascent yet disruptive state of cloud, it is clear that beyond the Supply side ecosystem, the Demand side along with the necessary enabling infrastructure and regulatory bodies are still grappling to fully understand and leverage the full potential of the Cloud. In part, this continues to create false positives resulting in a heightened state of awareness and acceptance of the Cloud yet with limited/little translation to actual adoption.

IDC views the end state of cloud proliferation gravitating towards being about cloud-enabled 3rd Platform solutions — ones that "mash up" cloud, mobile, social and big data technologies. The implication for players in the cloud services market is that they: 1) need to expand their expertise to encompass all of the disruptive technologies of the 3rd Platform, 2) recognize that at least half of the initiatives that will drive cloud spending will not actually be called "cloud" projects – they will be about solutions like "social mobile commerce", "mobile payments", "customer analytics", etc.

PREDICTION #4: ENTERPRISE IT TO REMAIN UNCONVINCED ABOUT ACHIEVING "RETURNS ON MOBILITY"

IN RETROSPECT

As companies grapple with an increasingly mobile workforce, and as more devices are

used for personal and business purposes (bring your own device [BYOD]), the organization of the future will need to evolve into a mobile organization. This is not just about implementing the use of tablets at the office; it is about rethinking the entire organization and business processes to take advantage of mobility.

This means that future development and integration of enterprise systems will need to be built for mobility and likely served from the cloud. Systems integrators will see a second wave of ICT investment projects as companies replace their existing traditional system with mobile systems. Thus, Malaysia vendors have to be prepared for this wave or lose out the opportunity. Enterprises will be looking for solutions to the aforementioned items as they implement their new architecture.

IDC is of the opinion that enterprise mobility is still in its nascent stage in Malaysia, as the mindset of the IT buyer is still primarily focused on the device or technology as opposed to a holistic solutions-based approach to enterprise mobility.

IDC's 2013 Future Workspace study defines the following as the lay of the land in Malaysia:

- On a scale of 1–5 (very important), the Malaysian mean is 3.14 (medium priority) for enterprise mobility.
- Looking ahead (12–18 months), 47.1% will increase spend on refreshing or increasing smartphones and only 19.6% on mobile device management.
- 80% of organizations see email and collaboration as core to its entire enterprise mobility strategy.
- 57% of organizations are currently deploying devices to their employees, but only 10% are currently using a mobility solution.

According to IDC's Enterprise Mobility Maturity Model, as of 2013, Malaysia remains in the 2nd of the 5 stages of Mobile Maturity, otherwise known as the "Opportunistic" stage. This means that organizations are currently employing a more tactical approach to mobility rather than strategic. They would have defined user requirements and crafted a structured approach to ensure successful delivery but, on the whole, governance of mobility within the organization would still be limited, and the benefits would still not have outweighed the implementation costs.

UPDATE

Given the vastness of the mobility pillar coverage, IDC is of the opinion that no tectonic shifts have come up in the last 6 months. IDC's latest research points to 35% of Tech Buyers in Malaysia having placed mobility as a high priority in 2014, compared to just 21% from the year before. This is a clear jump up from last year, and is in line with the other large countries in ASEAN except for Indonesia where they gave it the same priority as last year.

However, Malaysia ranks lowest in terms of budget allocations towards mobility. 64% in Malaysia only allocated less than 10% of their IT budget to mobility, compared to 38% in Indonesia, 57% in Singapore and 24% in Thailand. So there's definitely still a lot of caution around spending, and this indicates that enterprises are still unconvinced about ROI.

Malaysia also fared worse than other countries when it came to having a mobility strategy for organizational functions. 24% said their company still had no mobility strategy. The next closest was Indonesia at 12%. In last year's survey 39% said they were looking to develop a mobility strategy so this is a bit surprising. So this is probably where they need help and why they are still concerned about ROI, and once they have mapped out a clear strategy to mobilize their organizational functions

and even lines of business, they may start to become more convinced.

For Malaysian companies, the top strategic mobility initiatives they plan to undertake in the next 12 months would be to integrate mobility with existing IT infrastructure, develop / implement mobile network security, access and identity management solutions, and design / implement mobility centric KPIs / measurements. It shows that security is still important and companies don't want to overhaul their existing infrastructure. And companies are maturing as well because now they are defining measures for success.

PREDICTION #5: MALAYSIA'S BIG DATA MARKET ANTICIPATED TO HIT US$24.2 MILLION BUT WILL REMAIN TACTICAL IN NATURE

IN RETROSPECT

The Big Data market in Malaysia was valued at U$18.0 million at 2013 with an estimated YoY growth of 33.9%. Moving into 2014, the market is expected to grow at 34.4% reaching U$24.2 with a five-year compound annual growth rate (CAGR) (2012–2017) estimated at 32.1%. While the growth numbers look promising, IDC views the actual absolute figures as one which is less than desirable. While the interest and awareness of Big Data continues to grow, the actual adoption has yet to hit the necessary critical mass creating a "Big" impact on the nation's IT spending.

IDC's conservative view on the market size is also reflected in the stage the nation is at based on IDC's Big Data Maturity Model. IDC sees evidence of the nation as currently being at an opportunistic stage (Stage 2) with tactical being the key emphasis. IDC predicts that unless a wave of transformation envelopes the ecosystem, this will be the case for the coming year and with that the size of the market remains status quo. Key to this prediction are the following observations

- IT resources with Big Data skill sets are still limited. A review of the ecosystem reveals that solutions that require minimal IT support and expertise are typically positioned in favor of quick wins. The focus is currently on pre-configured appliances with enterprises mostly deploying either data warehousing that supports analytics or socialytics. With this, the actual realization of value based on Big Data solutions becomes limited.

- Beyond IT resources, the current ecosystem appears incomplete with gaps that need to be filled. Based on conversations with IT buyers, it is apparent that the ability to deliver end-to-end Big Data solutions and to provide the support of Hadoop-like environment is hard to come by. Even key vendors may not have local expertise and, therefore, limited skill sets transfer to local channel partners and end users. The skill set and resourcing issue is enough to cast doubt on total cost of ownership (TCO), given the high expense incurred to deploy.

- In some business cases, the adopted technology goes through an adaptive process of fine-tuning that appears continuous requiring substantial effort to maintain and tune to derive desired performance.
- The lack of business use cases and internal resources to drive Big Data requirements continues among organizations in Malaysia. It is evident that while the concept of Big Data has taken off, the next phase of creating a real business use case continues to be an impediment.

In order for the nation to move into the

next stage of the Big Data Maturity Model (repeatable stage), organizations need to adopt a strategic approach to Big Data adoption, as opposed to being tactical and siloed in nature as commonly seen. IDC predicts that the Big Data market will grow bigger and enter into next stage only when the issue of skill sets and resource is resolved, this in turn will lead to a complete ecosystem whereby channel partners with skill sets will have capability to deliver end-to-end Big Data solutions, including consultancy and other services.

UPDATE

In the last 6 months, IDC has observed increased activities that are making a positive impact to the Big Data ecosystem. IDC sees this as pivotal, as the maturity of the ecosystem will drive not only awareness but delivery capabilities as well. There appears to be increased synergy by enterprises in discovering Business Use Cases and the IT delivery ecosystem working to develop these Business Use Cases. The focus on developing talent is also apparent with collaborations between government, IT players, and education institutions to build awareness and talent in the country. The government has also taken a more proactive approach with aims to transform Malaysia into Big Data & Analytics (BDA) hub in Southeast Asia and currently there are 4 flagship initiatives spearheaded by the government as pilot projects.

IDC sees MDeC's initiative to fund local IT players to create 20 BDA applications (announced May 2014) as a positive sign to develop the local ecosystem. Its Technology Acceleration Program supports training, mentorship, and go-to-market strategies to MSC status companies that have interests in developing BDA applications and building data scientists.

Banking and Financial Services Industry

While IDC notes that governance, risk and compliance (GRC) is still the primary driver to adopt Big Data and Analytics this has also expanded to fraud detection and customer behaviors through cross-channel transactional behavior analysis. As an example a local bank is focusing on the correlation between Facebook data with internal transactional data as a monitor for both fraud detection and targeted marketing.

Telecommunications Industry

Most Telco SPs already have some form of BDA initiative with the priority set on increasing ARPU through the focus on customer behavior analysis and targeted marketing. What IDC believes will be next is location-based analytics for mobile and selling of subscriber behavior data in an anonymized form.

PREDICTION #6: ENTERPRISE SOCIAL NETWORKING: SANDBOX FOR PEAK INTERNAL COLLABORATION IN 2014 WILL BE A PRIORITY

IN RETROSPECT

Of all 3rd Platform technologies, social is generally regarded to have the most apparent manifestation in today's context of ICT, with the Web long moving from 1.0 to 2.0. To a certain extent, the pervasiveness and proliferation of social are akin to that of the mobility pillar. Both already have high levels of penetration, and what remains the glass ceiling is the ability to fully leverage on the vision of the technology to create a mashup of solutions, creating intelligent economies. This prediction essentially highlights the focus on creating a sandbox to explore the usage of social in an internal context for collaboration. IDC is of the opinion that this will be the key direction for social in the coming year, given the wide array of "social-" type solutions and purpose that continues to complicate

and make ROI a key challenge. Adding the complexity of fermiums in terms of a usage model has also made the realization of social in the enterprise more complex, as shadow IT becomes even more prevalent limiting enterprisewide strategies.

A review of the ecosystem for enterprise application vendors reveals that social enterprise features are not only new but are also gaining in focus. With that, major enterprise resource planning (ERP) vendors are now moving to this direction to encourage internal collaboration as a core function that allows IT to address key focus areas of the C-Suite. With reference to IDC's 2013 Software Study on features desired in future ERPs, embedded social and tools to support internal collaboration was ranked among the top 5. The transformation of internal collaboration creates a new definition and focal point that looks to leverage the platform to gain ideas or mindshare to drive sale and to create a smarter workforce environment, whereby it encourages employees internally to share documents, ideas, as well as collaboration.

UPDATE

Based on IDC's 2013 Social Enterprise Study, 75% of companies in Malaysia leverage social media for marketing outreach on a regular basis, with 90% having employees dedicated or having some job function related to social media. While the statistics appear high, based on conversations with local IT buyers, it is apparent that the current use of social mainly points to making use of consumer social media, such as Facebook and Twitter, for marketing and customer service purposes. Most of these enterprises do not deploy enterprise social software or social customer relationship management (CRM) to monitor or measure the marketing activities, to understand customer behavior, or to transform the communication and collaboration internally among employees and externally with customers and suppliers.

IDC is of the opinion that successful internal usage will be a necessary prerequisite for social to proliferate achieving the broad spectrum of capabilities it is intended to have. In the context of internal collaboration, a survey among early adopters as showcased in IDC's 2013 Social Enterprise Study highlights that more than 25% of organizations experienced an extremely low level of satisfaction based on existing investment of initiatives built on a social platform. That said, over 69% of these organizations will continue to invest, given the importance of getting it right.

IDC sees 2014 as the year where organizations put a high priority on improving internal collaboration using social solutions. IDC is also of the opinion that the IT Services ecosystem will play a large role in the development of Social Business. IDC's 2014 Continuum study highlights that 33% of organizations are looking to increase budgets in the coming year for Social related investments and of this budget a staggering 61% will be dedicated to procurement of related IT Services. It is therefore seen as imperative for IT Services players to hone skills beyond the traditional IT Services engagements to be relevant in the next phase of IT development.

PREDICTION #7: CHANNEL TRANSFORMATION IN THE 3RD PLATFORM WILL BE A KEY AGENDA IN 2014

IN RETROSPECT

The transition to the 3rd Platform is not a direct changeover but rather a parallel changeover. With that in mind, the IT channel ecosystem will have to exist in both platforms and transform accordingly with different channels playing different roles. IDC is of the opinion that this will be a key agenda in 2014 as the influencing power of channels is a double-edged sword

that can expedite or slow down the movement into the 3rd Platform.

In examining the local ecosystem, it is apparent that the majority of channels are taking a reactive approach to the 3rd Platform with most having not made a stand in terms of its future positioning on the 3rd Platform. The adage "don't fix it if it isn't broken" seems to represent the mentality of channels across ASEAN, including Malaysia. IDC sees the transformation that entails buy-in by channels to be pivotal for the success of the 3rd Platform in the country. IDCs global research indicates that 62% of channels are brought in on sales calls to address vendor-agnostic business cases, meaning the power to influence. This same influencing power to a certain extent is also expected to drive 3rd Platform discussions, hence the shift of power to either expedite or slow down the move.

Although this alludes to the idea of channels having a relatively strong influence, it is important to note that the channels themselves are also aware of the implications of the 3rd Platform and the shift of power, in the case of cloud, back to the vendor. With that, the key agenda that will be driven in 2014 will be the synergy that needs to be achieved by IT vendors and the channel ecosystem to be successful in the 3rd Platform.

UPDATE

IDC's observation of the first half of 2014 clearly points out that this has been a key agenda and will continue to be so. The Global IT Vendor community is proactively gearing up to welcome new partners into its ecosystem while earmarking selected channels in a bid to transform at the same time. IDC is of the opinion that while this may bode well for the Global IT Vendors, the local IT ecosystem will also need to play its part in the development as to not be left behind.

Lessons from leading global IT distributors showcase how dwindling margins and the threat of commoditization have necessitated strategies that allow IT Distributors to remain relevant. Case in point would be M&A activities to allow Distributors to play a role as IT Services enabler to its channels community. IDC is of the opinion that this same mindset of finding a place in a new ecosystem will be the strategy that the local IT ecosystem must take in order to survive. IDC also believes that while the changes are driven by technology, the fundamentals of any local IT player will also require both re-planning and re-strategizing.

PREDICTION #8:
BYOD IS REAL AND HAPPENING NOW, AND ORGANIZATIONS WILL NEED TO MAKE A STAND ON WHAT IT MEANS

IN RETROSPECT

The consumerization of IT, or BYOD, is real and happening now and will continue to become increasingly complicated as the whole notion of bringing a device also creates a pull through for the applications and solutions that envelop the device ecosystem. As individual employees pick their own applications and use them to access corporate data, managing data and applications is becoming ever more critical, and the likelihood of data loss is increasing at a very fast rate. While the numbers may be small now, employees or consumers are looking for solutions they find convenient and comfortable, which leads IDC to expect big growth in BYOD over the next few years. Also, cloud-based services, including DropBox, SkyDrive, and so on, are providing employees with their own personal data center. This is going to drive an increase in mobility in ways organizations need to be prepared for.

With reference to IDC's 2013 Future Workspace Study, over 50% of organizations are concerned that the BYOD reality is or will be one that creates numerous risks as it sprawls out of control. The same survey highlights security as the number 1 issue that needs to be addressed. With that IDC is of the opinion that BYOD is the current reality and tough decisions need to be made earlier rather than later. Key for this to happen will be the direction in which organizations see BYOD impacting its ecosystem.

UPDATE

IDC is of the opinion that in the last six months of 2014, the focus has been on organizations' "Mobilizing the People." This is where a call needs to be made on the move to BYOD or choose your own device (CYOD).

This is also the phase where organizations make investments to ensure the right infrastructure is in place to allow mobile device access into the enterprise network. IDC notes that this will be the phase where thorough planning will take center stage as the focus to date has been device driven without addressing the complete solutions portfolio. As organizations get their acts together, IDC sees the next two phases truly transforming organizations as the focus will then evolve to "Mobilizing the Processes" and lastly "Mobilizing the Channels."

The market movements IDC has observed also points to a fundamental question which organizations will soon need to address, that being the question on funding for devices. Should organizations take the BYOD path, there will be no need to apportion a dedicated budget for devices, but should the CYOD route be taken, the possibility of funding will be there. Either way both will require organizations to dedicate budget with and end goal of a mobility fist strategy.

PREDICTION #9: GOVERNMENT TO CONNECT TO CITIZENS VIA MOBILE DEVICES AND SOCIAL MEDIA, ACCELERATING A NEW TYPE OF CITIZEN/GOVERNMENT RELATIONSHIP

IN RETROSPECT

The four pillars of the 3rd Platform create unique ecosystems and solutions, as well as a collaborative ecosystem that creates mashups of solutions, both of which enable the transformation from traditional to intelligent economies. In 2014, IDC predicts that the mashup of both mobile and social will create the platform for government transformation connecting citizens via mobile devices and social media, accelerating a new type of citizen/government relationship.

The use of social and mobile mashups has been utilized as an alternative channel in retail and commercial areas to engage with targeted customers as part of go-to-customer strategies. This same mantra is expected to be adopted by the government to connect with citizens. Beyond traditional channels like the call center or Web sites for self-service, citizens now expect to be able to access and interact with government via devices, social media sites, and applications. This is especially true, given the way that citizens and business want, and need, to connect with city governments while they are on the move. The following are key trends to note based on IDC's Social Maturity Index, 2013:

- 67% of organizations highlighted the use of social media on a regular basis.
- 78% of organizations have policies in place regarding social media of which 37% have policies that support the use of social media in the workplace.
- 61% of organizations see social media as having a key impact on organizational business performance.

UPDATE

While IDC has yet to observe game changing initiatives in 2014, IDC is still of the opinion that more services will be provided on mobile devices in Malaysia as the local ecosystem matures. A turning point to this will be the development of the ecosystem beyond the current technology silos and embracing mash-ups of converged pillars as highlighted in this report. In order for this to be possible, players in the ecosystem will need to reach a level of maturity where the hype of focusing on one form of service delivery in a technology pillar is replaced by embracing the total value of the pillar. As an example moving up the cloud stack from IaaS to embracing a Hybrid Cloud solution portfolio. Current research points to a lack of such maturity, but as the ecosystem is exposed beyond selling to the IT organization and into the Line of Business the changes needed will be more apparent. This will be a catalyst for growth allowing for the government to connect with citizens.

PREDICTION #10: INNOVATION IN THE 3RD PLATFORM WILL CREATE UNIQUE MASHUP OPPORTUNITIES BUT MAY ALSO CREATE A PERFECT STORM FOR PROJECT FAILURE

IN RETROSPECT

While the potential for the four pillar technologies to enable new business value continues to receive attention, IDC predicts that the increasingly frequent application of these technologies to meet business demands will increase the risks of project failures, forcing CIOs to adopt new risk mitigation strategies. The ready availability of new business solutions based on mobile technologies designed for social consumption, large-scale analytics, and delivered by cloud infrastructure is creating complex applications that are often dependent on relatively untried technology and immature vendors. Also, once the new application is ready for user consumption, there remains the challenge of ongoing management of a service delivery chain that is often provisioned across multiple providers. While a project may successfully reach production-ready status, ROI targets risk being missed due to inadequate planning for service management. When combined with the impact of "cloud speed" and a regionwide drought of IT skills, then the potential for serious project failure is large.

UPDATE

Building on the concept of a "Technology Flood," IDC views this as an example of how the continued consumption of IT, if not managed or planned strategically, creates a possible avenue for failure. It is therefore critical for IT buyers, as well as vendors, to address the grass root problems, as showcased in Predictions #3, 4, 5, and 6, as each pillar has unique challenges. All this should be done with pillar mash-ups in mind as the next step forward will be uncharted territory.

IDC is of the opinion that while technologies of the 3rd platform are still in nascent stages of adoption, there is room for the IT ecosystem in Malaysia to observe and learn from other more mature countries. As an example, lessons from early adopters for Cloud Services point to the fact that the idea of zero up-front investment may not always be the case. These early adopters have highlighted IT services investment as essential to ensure the progression of cloud projects. In view of this, local cloud providers can potentially avoid possible project failures by ramping up on Service management capabilities. With that in mind, while IDC believes that there will always be risk involved; there are steps that the local IT Ecosystem can take to minimize the risk.

ESSENTIAL GUIDANCE

GUIDANCE FOR THE IT BUYERS

As showcased through the various IDC Maturity Models, the adoption for 3rd Platform technologies in Malaysia is at a relatively nascent stage. It is therefore important for IT buyers to take the long view of things understanding the bigger picture and strategically planning ahead. If not addressed, IT buyers run the risk of contributing to a technology flood that continues to make IT less relevant to the organization as a whole, as the ability to support and enable business goals becomes only a vision with IT being just a "cost center" a reality.

The nascent stage of the 3rd Platform in Malaysia means vendors are still getting their act together. For the IT buyer, it means running the risk of becoming an early adopter and paying the price for trial and errors. That said, the whole notion of moving to the 3rd Platform is not seen as a revolution but an evolution. With that, IT buyers are in the position to work closely with vendors to discover business use cases that can be measured to address specific key performance indicators (KPIs). IT buyers should take advantage of this unique point in time when the solutions are not a commodity but a possible game changer.

The ability to identify and address skill shortages continues to be a major differentiator. With the onset of cloud and Big Data, in particular, the required skill sets are fast becoming very different from what CIOs are used to hiring and managing, but CIOs will need to grow and stretch themselves as necessary to meet this challenge. CIOs must, in particular, begin to assess the suitability of staff for new roles focused on service management and relationship management. Suitable staff must be retrained; new IT organizational responsibilities defined and new hire profiles adjusted.

GUIDANCE FOR THE IT VENDORS

Transformation on the 3rd Platform impacts the entire ecosystem and is not just a product that should be marketed as is. Failure to get the entire delivery ecosystem in place creates a loophole that may delay or at worst completely disrupt the 3rd Platform initiative all together. Based on IDC Channels Research, it is evident that channels have a strong power to influence; IDC sees the need for increased effort to address the channel ecosystem as pivotal for success with velocity.

The low-hanging fruits may be lucrative now but, without a strategy to address intelligent economics, the flooding of technology will have limited purpose and benefit in the long run. The focus for vendors in the near term should be on identifying the partnerships needed to create implementable business use cases. As identified in this report, what is important to IT buyers is identifying the right 3rd Platform solution, but with that in mind comes the idea that the solution will be a coordinated effort across various technology offerings and expertise. It is therefore essential to start bridging solutions that create mashups earlier than latter.

As IDC stated in last year's ICT predictions, 3rd Platform technologies are emphasizing the problems that customers are facing with regard to talent shortage and lack of know-how. The selling point will increasingly be how well vendors and SPs can mitigate and alleviate these concerns. The sales process for most 3rd Platform projects will thus become increasingly consultative by nature. This may lengthen the sales process but can also help drive ongoing service and consulting business.

CHAPTER 7

INTERNET SECURITY THREAT REPORT 2014

Coordinated by
NIGEL TAN
Director, Systems Engineering
nigel_tan@symantec.com

Symantec Malaysia

Symantec

ABOUT SYMANTEC

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

MORE INFORMATION

- Symantec Worldwide: http://www.symantec.com/
- ISTR and Symantec Intelligence Resources: http://www.symantec.com/threatreport/
- Symantec Security Response: http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/
- Norton Cybercrime Index: http://us.norton.com/cybercrimeindex/

INTRODUCTION

Symantec has established the most comprehensive source of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of more than 41.5 million attack sensors and records thousands of events per second. This network monitors threat activity in over 157 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services, Norton™ consumer products, and other third-party data sources.

In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 60,000 recorded vulnerabilities (spanning more than two decades) from over 19,000 vendors representing over 54,000 products.

Spam, phishing, and malware data is captured through a variety of sources including the Symantec Probe Network, a system of more than 5 million decoy accounts, Symantec.cloud, and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology, is able to detect new and sophisticated targeted threats before they reach customers' networks. Over 8.4 billion email messages are processed each month and more than 1.7 billion web requests filtered each day across 14 data centers.

Symantec also gathers phishing information through an extensive anti-fraud community of enterprises, security vendors, and more than 50 million consumers. Symantec Trust Services provides 100 percent availability and processes over 6 billion Online Certificate Status Protocol (OCSP) look-ups per day, which are used for obtaining the revocation status of X.509 digital certificates around the world. These resources give Symantec analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the annual Symantec Internet Security Threat Report, which gives enterprises, small businesses, and consumers essential information to secure their systems effectively now and into the future.

EXECUTIVE SUMMARY

In 2013 much attention was focused on cyber-espionage, threats to privacy and the acts of malicious insiders. However the end of 2013 provided a painful reminder that cybercrime remains prevalent and that damaging threats from cybercriminals continue to loom over businesses and consumers. Eight breaches in 2013 each exposed greater than 10 million identities, targeted attacks increased and end-user attitudes towards social media and mobile devices resulted in wild scams and laid a foundation for major problems for endusers and businesses as these devices come to dominate our lives.

This year's ISTR once again covers the wide-ranging threat landscape, with data collected and analyzed by Symantec's security experts. In this summary, we call out seven areas that deserve special attention.

THE MOST IMPORTANT TRENDS IN 2013 WERE:

2013 WAS THE YEAR OF MEGA BREACH

Our Internet Security Threat Report 17 reported 2011 as the Year of the Data Breach. The year was extraordinary because in addition to increased cybercrime-driven breaches, Anonymous in acts of hactivism breached dozens of companies. With Anonymous less active, breach numbers returned to more predictable growth in 2012. And then came 2013. If 2011 was the year of the breach, then 2013 can best be described as the Year of the Mega Breach.

The total number of breaches in 2013 was 62 percent greater than in 2012 with 253 total breaches. It was also larger than the 208 breaches in 2011. But even a 62 percent increase does not truly reflect the scale of the breaches in 2013. Eight of the breaches in 2013 exposed more than 10 million identities each. In 2012 only one breach exposed over 10 million identities. In 2011, only five were of that size.

2011 saw 232 million identities exposed, half of the number exposed in 2013. In total over 552 million identities were breached in 2013, putting consumer's credit card information, birth dates, government ID numbers, home addresses, medical records, phone numbers, financial information, email addresses, login, passwords, and other personal information into the criminal underground.

TARGETED ATTACKS GROW AND EVOLVE

While targeted attacks continue to rise, Symantec observed an interesting evolution in these attacks. As first reported in last year's Internet Security Threat Report, attackers added watering- hole attacks to their arsenal. But reports of the death of spear phishing are greatly exaggerated. While the total number of emails used per campaign has decreased and the number of those targeted has also decreased, the number of spear-phishing campaigns themselves saw a dramatic 91 percent rise in 2013.

This "low and slow" approach (campaigns also run three times longer than those in 2012) are a sign that user awareness and protection technologies have driven spear phishers to tighten their targeting and sharpen their social engineering. We have also observed the addition of real world social engineering, combining virtual and real world attacks, being employed to increase the odds of success.

This year's Internet Security Threat Report also introduces a new calculation. Using epidemiology concepts commonly applied to public health issues, we have estimated the risk industries and users face of being targeted for

attack. It sends a warning to some industries that may view the volume of attacks against them as no cause for concern. For instance, while the most targeted attacks in 2013 were against Governments and the Services industry, the industries at most risk of attack were Mining, Governments and then Manufacturing. Their odds of being attacked are 1 in 2.7, 1 in 3.1 and 1 in 3.2 respectively.

ZERO-DAY VULNERABILITIES AND UNPATCHED WEBSITES FACILITATED WATERING-HOLE ATTACKS

More zero-day vulnerabilities were discovered in 2013 than any other year Symantec has tracked. The 23 zero-day vulnerabilities discovered represent a 61 percent increase over 2012 and are more than the two previous years combined.

Zero-day vulnerabilities are coveted because they give attackers the means to silently infect their victim without depending on social engineering. And by applying these exploits in a watering-hole attack they avoid the possibility of anti-phishing technology stopping them. Unfortunately legitimate web sites with poor patch management practices have facilitated the adoption of watering hole attacks. 77 percent of legitimate websites had exploitable vulnerabilities and 1-in-8 of all websites had a critical vulnerability. This gives attackers plenty of choices in websites to place their malware and entrap their victims.

Typically cutting-edge attackers stop using a vulnerability once it is made public. But this does not bring an end to their use. Common cybercriminals rapidly incorporate zero-day vulnerabilities to threaten all of us. Even though the top five zero-day vulnerabilities were patched on average within four days, Symantec detected a total of 174,651 attacks within 30 days of these top five becoming known.

RANSOMWARE ATTACKS GREW BY 500 PERCENT IN 2013 AND TURNED VICIOUS

Scammers continued to leverage profitable ransomware scams – where the attacker pretends to be local law enforcement, demanding a fake fine of between $100 to $500. First appearing in 2012 these threats escalated in 2013, and grew by 500 percent over the course of the year.

These attacks are highly profitable and attackers have adapted them to ensure they remain profitable. to ensure they remain profitable. The next step in this evolution was Ransomcrypt, commonly known as Cryptolocker. This is the most prominent of these threats and turns ransomware vicious by dropping all pretence of being law enforcement and is designed to encrypt a user's files and request a ransom for the files to be unencrypted. This threat causes even more damage to businesses where not only the victims' files are encrypted but also files on shared or attached network drives.

Holding encrypted files for ransom is not entirely new, but getting the ransom paid has previously proven problematic for the crooks. With the appearance of online payment methods ransomcrypt is poised for growth in 2014. Small businesses and consumers are most at risk from losing data, files or memories. Prevention and backup are critical to protecting users from this type of attack.

SOCIAL MEDIA SCAMS AND MALWARE FLOURISH ON MOBILE

While the prevalence of mobile malware is still comparatively low, 2013 showed that the environment for an explosive growth of scams and malware attacks is here. Our Norton Report, a global survey of end-users, showed that 38 percent of mobile users had

already experienced mobile cybercrime. Lost or stolen devices remain the biggest risk, but mobile users are behaving in ways that leave themselves open to other problems.

Mobile users are storing sensitive files online (52 percent), store work and personal information in the same online storage accounts (24 percent) and sharing logins and passwords with families (21 percent) and friends (18 percent), putting their data and their employers' data at risk.

Yet only 50 percent of these users take even basic security precautions.

The number of brand new malware families created slowed as malware authors worked to perfect existing malware. In 2012 each mobile malware family had an average of 38 variants. In 2013 each family had 58. However several events in 2013 showed that mobile users are highly susceptible to scams via mobile apps. It might be said that mobile malware has not yet exploded because the bad guys have not needed it to get what they want.

PREVALENCE OF SCAMS FAIL TO CHANGE USER BEHAVIOUR ON SOCIAL MEDIA

Surrounded by their friends, users continue to fall for scams on social media sites. Fake offers such as free cell phone minutes accounted for the largest number of attacks of Facebook users in 2013 – 81 percent in 2013 compared to 56 percent in 2012. And while twelve percent of social media users say someone has hacked into their social network account and pretended to be them, a quarter continue to shared their social media passwords with others and a third connect with people they don't know.

As social media becomes more and more of an activity done on mobile devices these bad behaviours are likely to have worse consequences.

ATTACKERS ARE TURNING TO THE INTERNET OF THINGS

Baby monitors, as well as security cameras and routers, were famously hacked in 2013. Furthermore, security researchers demonstrated attacks against smart televisions, automobiles and medical equipment. This gives us a preview of the security challenge presented by the rapid adoption of the Internet of Things (IoT).

The benefit to attackers of compromising these devices may not yet be clear, and some suspect claims about hacked devices (refrigerators for instance) are to be expected. But the risk is real. IoT devices will become access points for targeted attackers and become bots for cybercriminals.

Of immediate concern are attacks against consumer routers. Computer worms like Linux.Darlloz are making a comeback as attackers target devices without users to social engineer, but with unpatched vulnerabilities they can remotely exploit. Control of these devices can prove profitable for attackers, using DNS redirection to push victims to fake websites, usually to steal financial details.

Today the burden of preventing attacks against IoT devices falls on the user; however this is not a viable long-term strategy. Manufacturers are not prioritizing security – they need to make the right security investments now. The risk gets even higher with the proliferation of data being generated from these devices. Big data is big money and unless the right security steps are taken it's all available for an enterprising cybercriminal.

2013 SECURITY TIMELINE

01 JANUARY

- Elderwood Project found using new Internet Explorer Zero-Day Vulnerability (CVE-2012-4792)
- Java Zero-Day found in Cool Exploit Kit (CVE-2013-0422)
- Android.Exprespam potentially infects thousands of devices • Backdoor.Barkiofork used to target Aerospace and Defense industries

02 FEBRUARY

- Bamital botnet taken down
- Adobe zero-day used in "LadyBoyle" attack (CVE-2013-0634)
- Cross-platform toolkit for creating the remote access tool (RAT) "Frutas" discovered
- Fake Adobe Flash update discovered installing ransomware and performing click fraud
- Bit9 suffers security breach, codesigning SSL certificates stolen

03 MARCH

- Android Malware spams victims' contacts
- "Facebook Black" scam spreads on Facebook
- Blackhole Exploit Kit takes advantage of financial crisis in Cyprus • Several South Korean banks and local broadcasting organizations impacted by cyber attack.

04 APRIL

- #OpIsrael hacktivism campaign targets Israeli websites
- NPR, Associated Press, and various Twitter accounts hacked by Syrian Electronic Army (SEA)
- Distributed Denial of Service attacks hit Reddit and European banks
- WordPress plugin vulnerability discovered, allowing PHP injection
- LivingSocial resets passwords for 50 million accounts after data breach

05 MAY

- A US Department of Labor website becomes victim of a watering-hole attack
- Cybercriminals steal more than $1 million from a Washington state hospital
- SEA hacks twitter accounts of The Onion, E! Online, The Financial Times, and Sky
- New Internet Explorer 8 Zero-Day Vulnerability used in watering-hole attack (CVE-2012-4792)
- #OpUSA hacktivism campaign launches against US websites
- Seven men were arrested in New York in connection with their role in international cyber attacks which resulted in theft of $45 million across 26 different countries.

06 JUNE

- Microsoft and FBI disrupt Citadel botnets
- A surveillance scandal emerges in the United States, as a former Government security contractor releases classified documents
- Zero-day vulnerability found in most browsers across PC, Mac, mobile, and game consoles
- Anonymous launches #OpPetrol attack on international oil and gas companies
- 65 websites compromised to host malicious ads with ZeroAccess Trojan
- FakeAV discovered on Android phones

07 JULY

- Ubisoft hacked: user account information stolen
- France caught up in PRISM scandal as data snooping allegations emerge
- New exploit kit targets flaws in Internet Explorer, Java, and Adobe Reader
- FBI-style ransomware discovered targeting OSX computers
- Android Master Key vulnerability used in the wild
- Viber and Thomson Reuters latest victims of SEA attacks

08 AUGUST

- Channel 4 blog, New York Post, SocialFlow, Washington Post, New York Times, impacted by SEA attacks
- DNS hijack caused thousands of sites to redirect users to exploit kit
- Two new ransomware scams found: One that changes Windows login credentials on Chinese systems, another that takes advantage of the NSA PRISM controversy
- Fake 'Instagram for PC' leads to survey scam
- Attackers targeted banks' wire payment switch to steal millions
- Francophoned social engineering ushers in a new era of targeted attacks

09 SEPTEMBER

- Syrian Electronic Army compromises US Marine Corps' website, Fox Twitter accounts, supposedly using Mac Trojan
- ATMs discovered that dispense cash to criminals
- Ransomware called "Cryptolocker" surfaces that encrypts victims' files and demands payment to decrypt them
- Symantec lifts lid on professional hackers-for-hire group Hidden Lynx
- Belgian telecom compromised in alleged cyber espionage campaign
- Symantec Security Response sinkholes ZeroAccess botnet

10 OCTOBER

- The Silk Road marketplace taken offline, resurfaces by end of month
- SEA attacks GlobalPost and Qatar websites, US Presidential staff emails
- Adobe confirms security breach, 150 million identities exposed
- Blackhole and Cool Exploit Kit author arrested
- WhatsApp, AVG, Avira defaced by hacker group KDMS
- New ransomware demands Bitcoins for decryption key

11 NOVEMBER

- Second Android master key vulnerability discovered
- Microsoft zero-day vulnerability being used in targeted attacks and e-crime scams (CVE-2013-3906)
- SEA hacks VICE.com in retaliation for article that supposedly names members
- Anonymous claims to have hacked UK Parliament Wi-Fi during London protest
- Linux worm that targets "Internet of Things" discovered
- Target confirms data breach leading to the exposure of 110 million identities.

12 DECEMBER

- Data of 20 million Chinese hotel guests leaked
- Cross-site scripting vulnerability found in wind turbine control application
- Imitation versions of Cryptolocker discovered, attempt to capitalize on original's success
- 105 million South Korean accounts exposed in credit card security breach

2013 IN NUMBERS

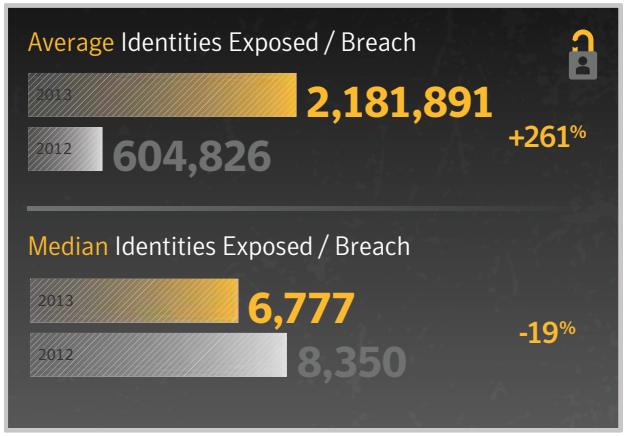
BREACHES

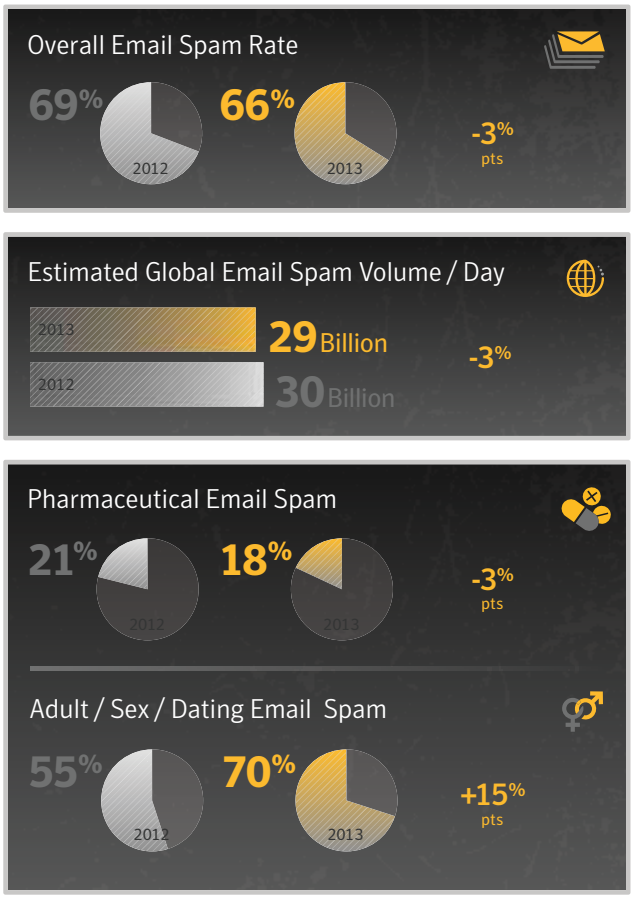
- Mega Breaches were data breach incidents that resulted in the personal details of at least 10 million identities being exposed in an individual incident. There were eight in 2013, compared with only one in 2012.

- Hacking continued to be the primary cause of data breaches in 2013. Hacking can undermine institutional confidence in a company, exposing its attitude to security and the loss of personal data in a highly public way can result in damage to an organization's reputation. Hacking accounted for 34 percent of data breaches in 2013.

- In 2013, there were eight data breaches that netted hackers 10 million or more identities, the largest of which was a massive breach of 150 million identities. In contrast, 2012 saw only one breach larger than 10 million identities.

- Although overall average size of a breach has increased, the median number of identities stolen has actually fallen from 8,350 in 2012 to 6,777 in 2013. Using the median can be helpful in this scenario since it ignores the extreme values caused by the notable, but rare events that resulted in the largest numbers of identities being exposed.



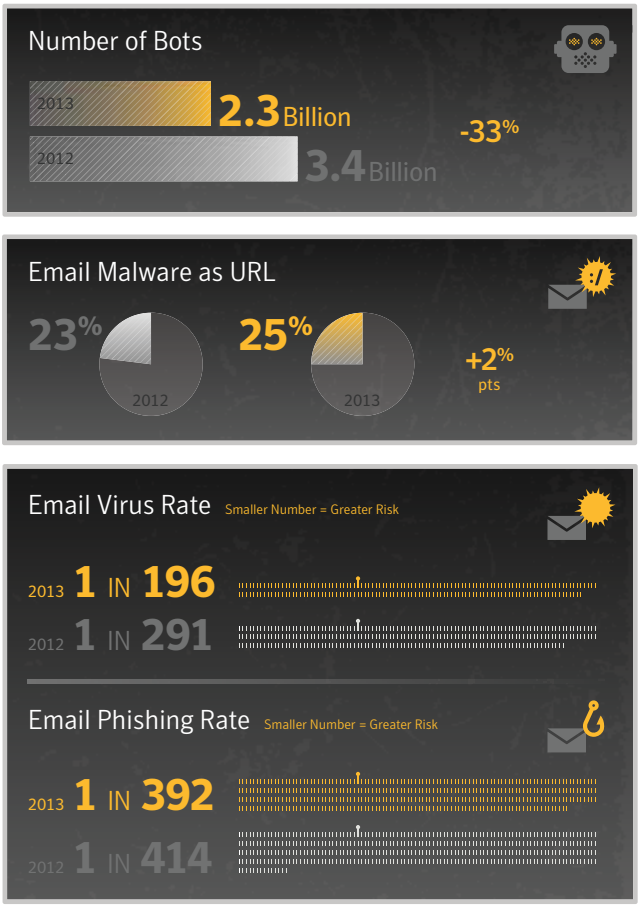


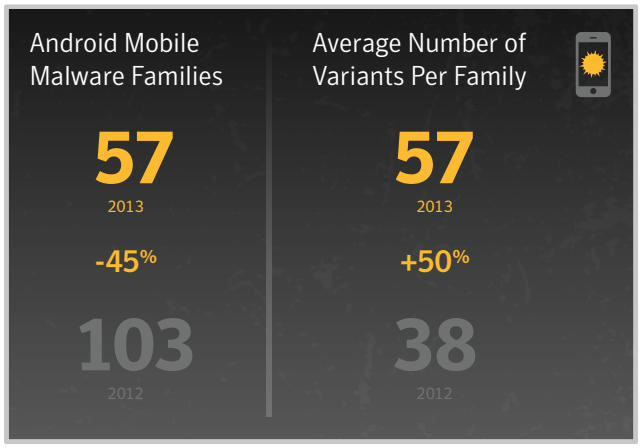
SPAM

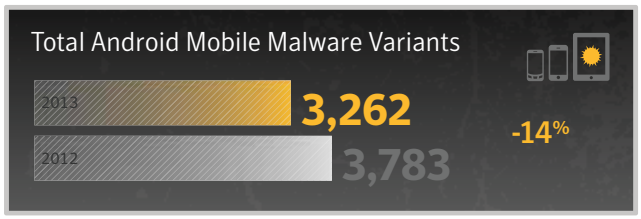
- Approximately 76 percent of spam email was distributed by spam-sending botnets, compared with 79 percent in 2012. Ongoing actions to disrupt a number of botnet activities during the year have helped to contribute to this gradual decline.
- In 2013, 87 percent of spam messages contained at least one URL hyperlink, compared with 86 percent in 2011, an increase of 1 percentage point.
- Adult Spam dominated in 2013, with 70 percent of spam related to adult content. These are often email messages inviting the recipient to connect to the scammer through instant messaging, or a URL hyperlink where they are then typically invited to a pay-perview adult-content web cam site. Often a bot responder, or a person working in a low-pay, offshore call center would handle any IM conversation.

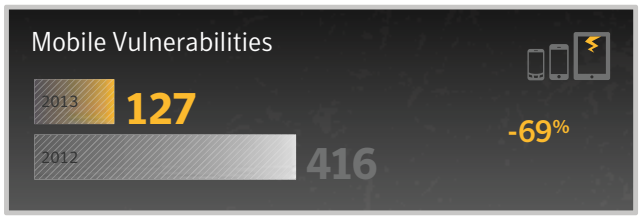
BOTS, EMAIL

- Bot-infected computers, or bots, are counted if they are active at least once during the period. Of the bot-infected computer activities that Symantec tracks, they may be classified as actively-attacking bots or bots that send out spam, i.e. spam zombies. During 2013, Symantec struck a major blow against the ZeroAccess botnet. With 1.9 million computers under its control, it is one of the larger botnets in operation at present. ZeroAccess has been largely used to engage in click fraud to generate profits for its controllers.
- In 2013, more emailborne malware comprised hyperlinks that referenced malicious code, an indication that cybercriminals are attempting to circumvent security countermeasures by changing the vector of attacks from purely email to the web.
- 71 percent of phishing attacks were related to spoofed financial organizations, compared with 67 percent in 2012. Phishing attacks on organizations in the Information Services sector accounted for 22 percent of phishing attacks in 2013







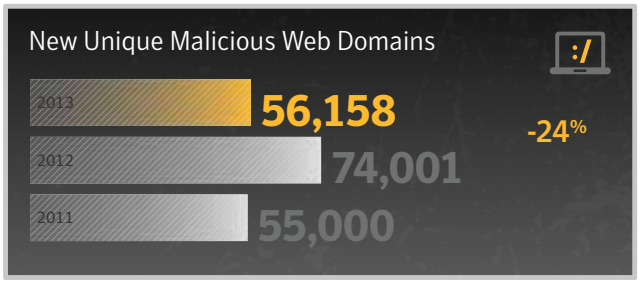


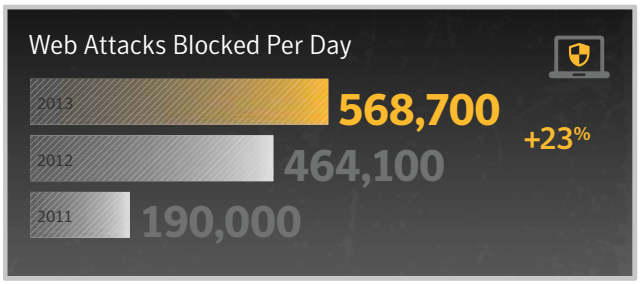
MOBILE

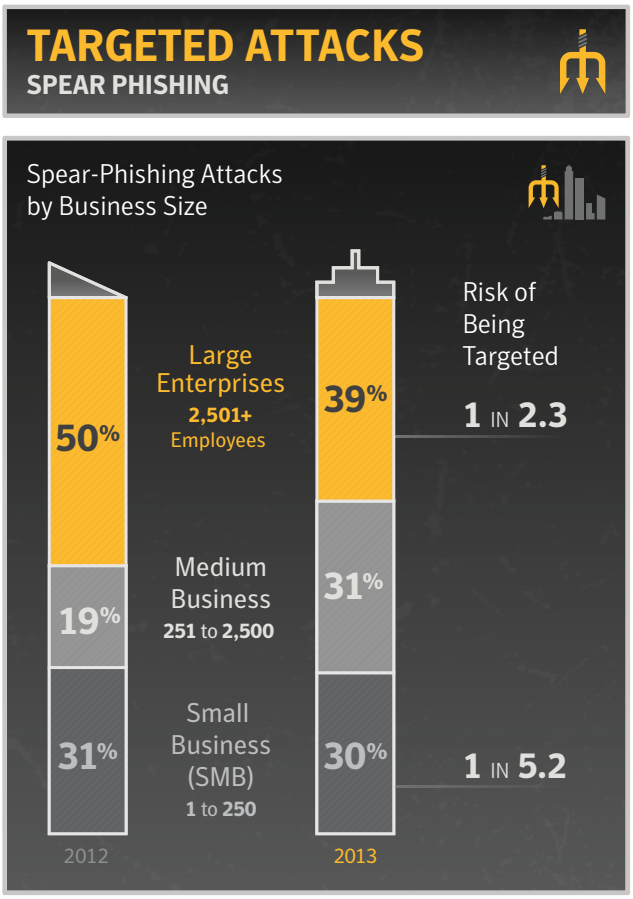
- Currently most malicious code for mobile devices consists of Trojans that pose as legitimate applications. These applications are uploaded to mobile application ("app") marketplaces in the hope that users will download and install them, often trying to pass themselves off as legitimate apps or games.
- Attackers have also taken popular legitimate applications and added additional code to them. Symantec has classified the types of threats into a variety of categories based on their functionality
- Symantec tracks the number of threats discovered against mobile platforms by tracking malicious threats identified by Symantec's own security products and confirmed vulnerabilities documented by mobile vendors

WEB

- Approximately 67 percent of websites used to distribute malware were identified as legitimate, compromised websites.
- 10 percent of malicious website activity was classified in the Technology category, 7 percent were classified in the Business category and 5 percent were classified as Hosting.
- 73 percent of browserbased attacks were found on Anonymizer proxy websites, similarly, 67 percent of attacks found on Blogging websites involved browser-based exploits



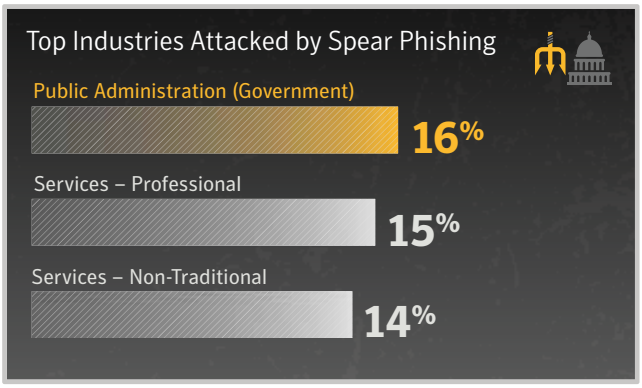




TARGETED ATTACKS – SPEAR PHISHING

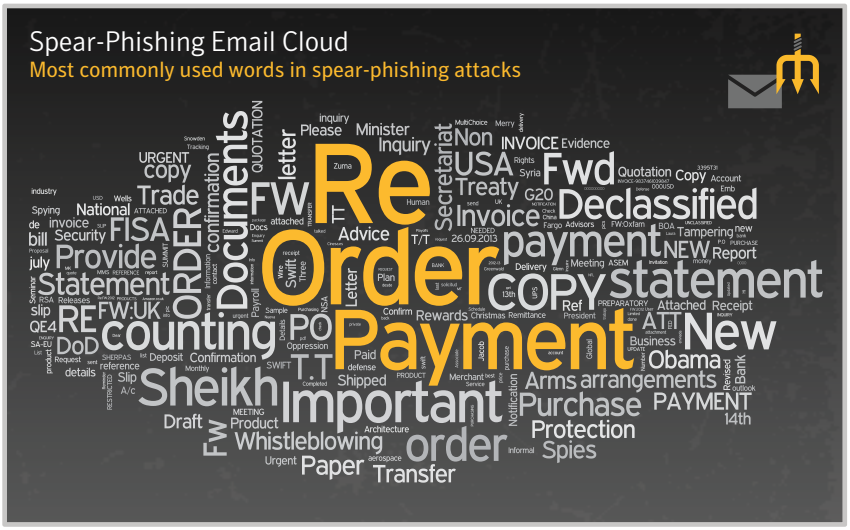
- Targeted attacks aimed at Small Businesses (1-250) accounted for 30 percent of targeted spear-phishing attacks. 1 in 5 small business organizations was targeted with at least one spear-phishing email in 2013.
- 39 percent of targeted spear-phishing attacks were sent to Large Enterprises comprising over 2,500+ employees. 1 in 2 of which were targeted with at least one such attack.
- The frontline in these attacks is moving along the supply chain and large enterprises may be targeted though webbased watering-hole attacks should emailbased spear-phishing attacks fail to yield the desired results.

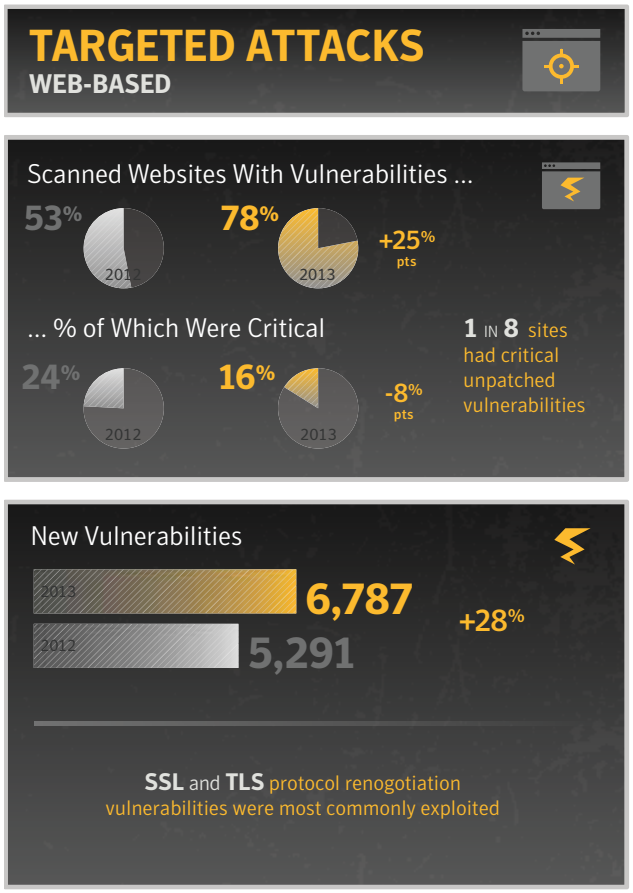
- Approximately 1 in 3 organizations in the Mining, Public Administration and Manufacturing sectors were subjected to at least one targeted spearphishing attack in 2013.
- The Government and Public Sector (aka. Public Administration) accounted for 16 percent of all targeted spear-phishing email attacks blocked in 2013, compared with 12 percent in 2012.



- Attackers may target both the personal and professional email accounts of individuals concerned; a target's work-related account is likely to be targeted more often and is known as spear phishing.
- Over the past decade, an increasing number of users have been targeted with spearphishing attacks and the social engineering has grown more sophisticated over time.
- In 2013 the volume and intensity of these attacks had changed considerably from the previous year, prolonging the duration over which a campaign may last, rather than intensifying the attacks in one or two days as had been the case previously. Consequently, the number of attacks seen each day has fallen and other characteristics of these attacks suggest this may help to avoid drawing attention to an attack campaign that may be underway

- This word cloud shows the most frequently occurring words that have been used in targeted spear-phishing email attacks throughout 2013. The larger the size of the font, the more frequently that word was used.

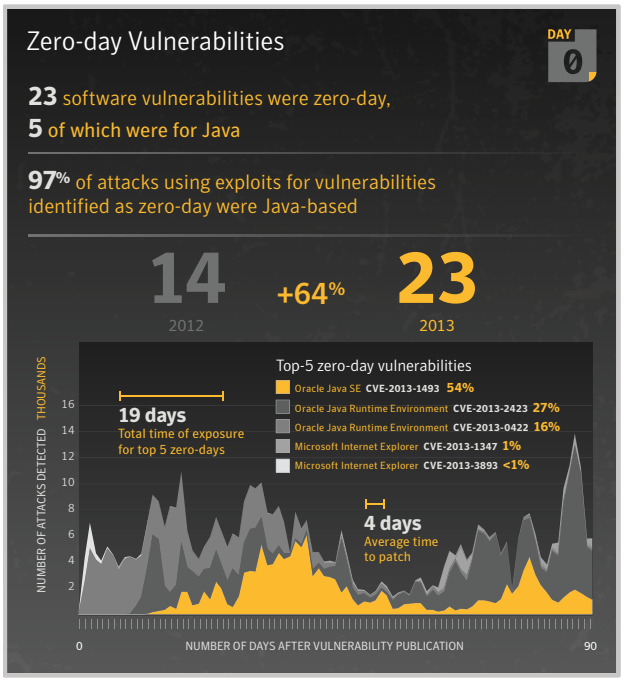




TARGETED ATTACKS – WEB-BASED

- Attackers generally have to find and exploit a vulnerability in a legitimate website in order to gain control and plant their malicious payload within the site. Compromising a legitimate website may seem to be a challenge for many, but vulnerability scans of public websites carried out in 2013 by Symantec's Website Vulnerability Assessment Services found that 78 percent of sites contained vulnerabilities.
- Of this, 16 percent were classified as critical vulnerabilities that could allow attackers to access sensitive data, alter the website's content, or compromise visitors' computers. This means that when an attacker looks for a site to compromise, one in eight sites makes it relatively easy to gain access.
- The most commonly exploited vulnerabilities related to SSL and TLS protocol renegotiation

- Malware was found on 1 in 566 websites scanned by Symantec's Website Vulnerability Assessment Service in combination with the daily malware scanning service.
- 97 percent of attacks using exploits for vulnerabilities initially identified as zero-days were Java-based. The total time between a zero-day vulnerability being published and the required patch being published was 19 days for the top-5 most-exploited zeroday vulnerabilities. The average time between publication and patch was 4 days.
- Zero-day vulnerabilities are frequently used in watering-hole web-based targeted attacks. Attackers can quickly switch to using a new exploit for an unpublished zero-day vulnerability once an attack is discovered and the vulnerability published.



TARGETED ATTACKS + DATA BREACHES

TARGETED ATTACKS

The use of malware specifically to steal sensitive or confidential information from organizations isn't a new trend; it's been around for at least the past decade. However the scale of these attacks has always been relatively low in order to remain below the radar of security technology used to safeguard against them. A targeted attack uses malware aimed at a specific user or group of users within a targeted organization and may be delivered through a spear-phishing email, or a form of drive-by download known as a watering-hole attack. No matter how these attacks are delivered they are designed to be low in volume, often with malicious components used exclusively in one attack. Their ultimate goal is to provide a backdoor for the attacker to breach the targeted organization.

In the past these targeted attacks have relied primarily on the spear-phishing element, an emailbased phishing attack is often aimed at an individual or small group of individuals, because they may have access to sensitive information through their role at a targeted organization. An important detail with a spear-phishing email is that it often appears to come from someone the recipient knows, a source they would trust, or contain subject matter the target would be interested in or is relevant to their role. The social engineering is always refined and well-researched, hence the attack may be very difficult to recognize without the right technology in place to safeguard against it.

However, targeted attacks no longer rely as heavily on spear-phishing attacks in order to penetrate an organization's defenses. More recently the attackers have expanded their tactics to include watering-hole attacks, which are legitimate websites that have been compromised for the purpose of installing targeted malware onto the victim's computer. These attacks rely almost exclusively on client-side exploits for zero-day vulnerabilities that the attackers have in their arsenal. Once the vulnerability the hackers are using has been published, they will often quickly switch to using another exploit in order to remain undetected.

CHANGES IN 2013

It's worth looking back at the last few years to see how previous attack trends compare to the ones in 2013. In 2012 we witnessed a 42 percent increase in the targeted-attack rate when compared to the previous year. This was a measure of the average number of targeted-attack spear-phishing emails blocked each day. In 2013 the attack rate appears to have dropped 28 percent, returning to similar levels seen in 2011.

What appears to have happened is that attacks have become more focused as the attackers have solidified and streamlined their attack methods. Looking at email-based attack campaigns in particular,01 the number of distinct campaigns identified by Symantec is up by 91 percent compared to 2012, and almost six times higher compared to 2011. However, the average number of attacks per campaign has dropped, down 76 percent when compared to 2012 and 62 percent from 2011. This indicates that while each attack campaign is smaller, there have been many more of them in 2013.

The number of recipients of spear-phishing emails during a campaign is also lower, at 23 recipients per campaign, down from 111 in 2012 and 61 in 2011. In contrast, these campaigns are lasting longer. The average duration of a campaign is 8.2 days, compared to 3 days in 2012 and 4 days in 2011. This could indicate that the attack campaigns are becoming more focused and persistent, with a reduced number of attempts over a longer period of time in order to better hide the activity.

AT A GLANCE

- Targeted attacks have become more focused as attackers have streamlined their attack methods.
- The global average number of spear-phishing attacks per day in 2013 was 83.
- Zero-day vulnerabilities, often used in wateringhole attacks, reached their highest levels since Symantec began tracking them.
- Hackers were once again responsible for more data breaches than any other source. However, accidental exposure, as well as theft or loss, grew significantly in 2013. • There were over 552 million identities exposed in data breaches during 2013.

SPEAR PHISHING

Spear-phishing attacks rely heavily on social engineering to improve their chances of success. The emails in each case are specially tailored by the attackers to spark the interest of the individual being targeted, with the hope that they will open them. For example, an attacker may send someone working in the financial sector a spear-phishing email that appears to cover some new financial rules and regulations. If they were targeting someone working in human resources, they might send spear-phishing emails that include malware-laden résumé attachments.

We've also seen some fairly aggressive spear-phishing attacks. In these cases the attacker sent an email and then followed up with a phone call directly to the target, such as the "Francophoned" attack from April 2013.02 The attacker impersonated a high-ranking employee, and requested that the target open an attachment immediately. This assertive method of attack has been reported more often in 2013 than in previous years.

Attackers will often use both the personal and professional accounts of the individual targeted, although statistically the victim's work-related account is more likely to be targeted.

Over the past decade, an increasing number of users have been targeted with spear-phishing attacks, and the social engineering has grown more sophisticated over time. In analyzing the patterns and trends in these attacks it is important to look at the profile of the organizations concerned, most notably to

Their ultimate goal is to provide a backdoor for the attacker to breach the targeted organization.

which industry sector they belong, and how large their workforce is. The net total number of attacks blocked in 2013 is broken down by industry in figure 4 and organization size in figure 5.

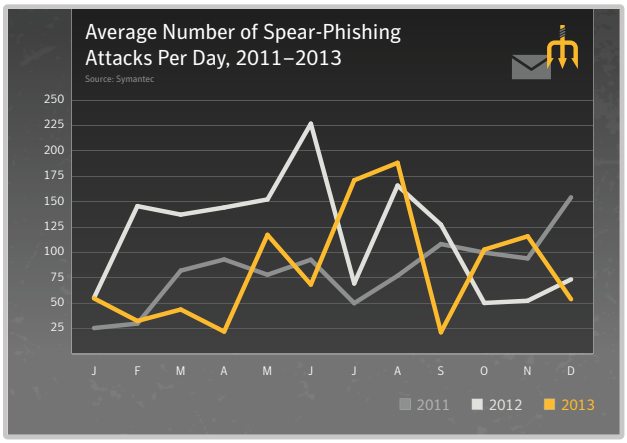


Fig. 1

- The global average daily rate of targeted spearphishing attacks is 28 percent lower than in 2012, but two percent higher than 2011. The figure for 2012 was unusually high, and attackers seem to have adjusted their tactics in 2013 in an attempt to reduce their footprint. The average rates for 2013 returned to levels on par with previous years.
- The global average number of spear-phishing attacks per day in 2013 was 83, compared with 116 in 2012 and 82 in 2011.
- The spear-phishing attack rate reached a peak of 188 attacks per day in the month of August, compared with the peak of 227 in June of the previous year

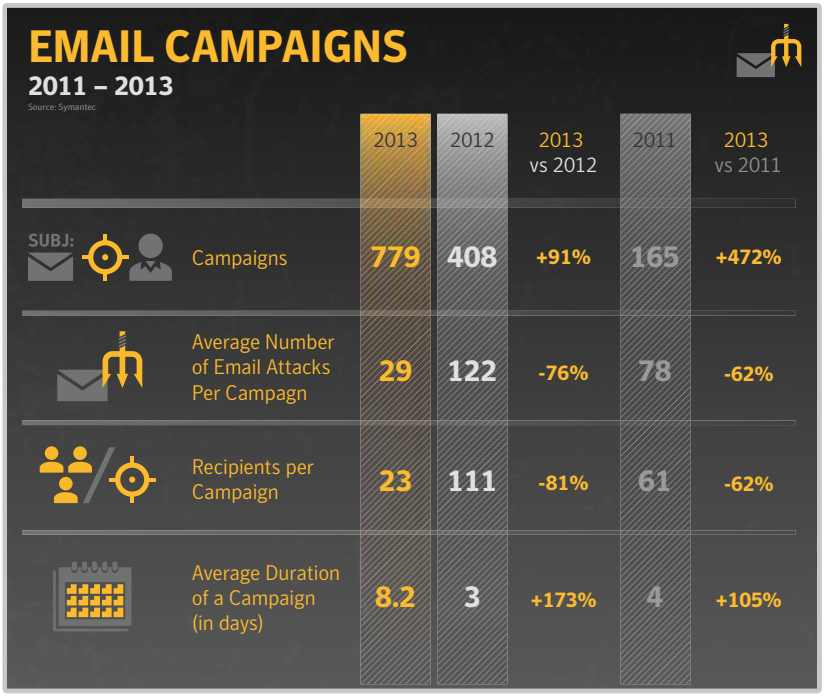


Fig. 2

- In 2013 the volume and intensity of spear phishing targeted email campaigns changed considerably from the previous year, extending the duration over which a campaign may last, rather than intensifying the attacks in one or two days as had been the case previously. Consequently, the number of attacks seen each day has fallen and other characteristics of these attacks suggest this may help to avoid drawing attention to an attack campaign that may be underway.

Fig. 3

However just because an industry or organization of a particular size receives a large number of attacks doesn't necessarily mean that it was at an elevated risk, or that someone working in that industry or organization had a high probability of being targeted. The probability was determined by looking at a group of people who have been targeted and comparing this number against a control group for that industry or organization size. Furthermore, it was important to look not only at the attacks themselves, but also to examine the email traffic of other customers in the same sectors and of the same organizational size. In this way, for the first time, Symantec was able to report on the odds of any particular organization being targeted in such an attack, based on their industry and size.

POLITICS AND TARGETED

Attacks While correlation doesn't always equal causation, it's often quite interesting never-the-less. This is especially true in the amalgamous region of targeted attacks, where it's difficult to prove motive. A good example of this came this year after negotiations concerning an energy partnership between two nation states. Sadly the negotiations broke down, but what followed was a significant increase in the number of targeted attacks against the Energy sector.

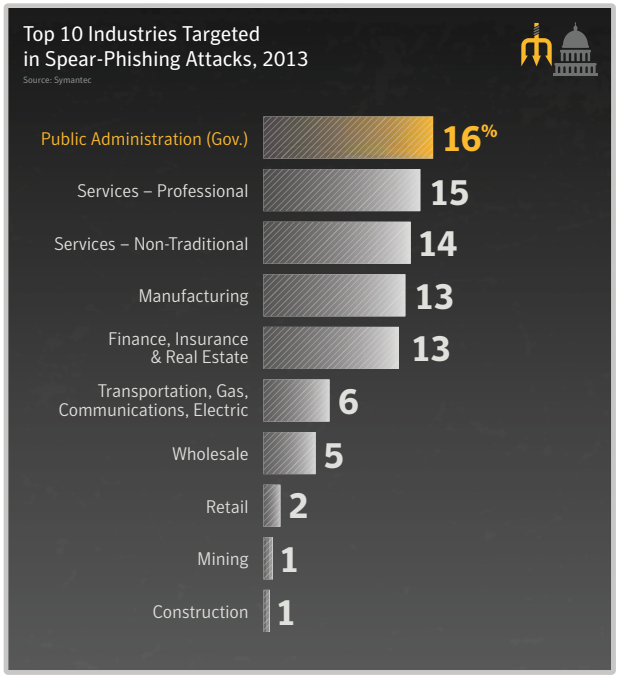


Fig. 4

- Public Administration03 topped the industries targeted in 2013, comprising 16 percent of all attacks.
- Services, both professional and non-traditional,04 came in second and third, respectively, in the overall number of attacks.

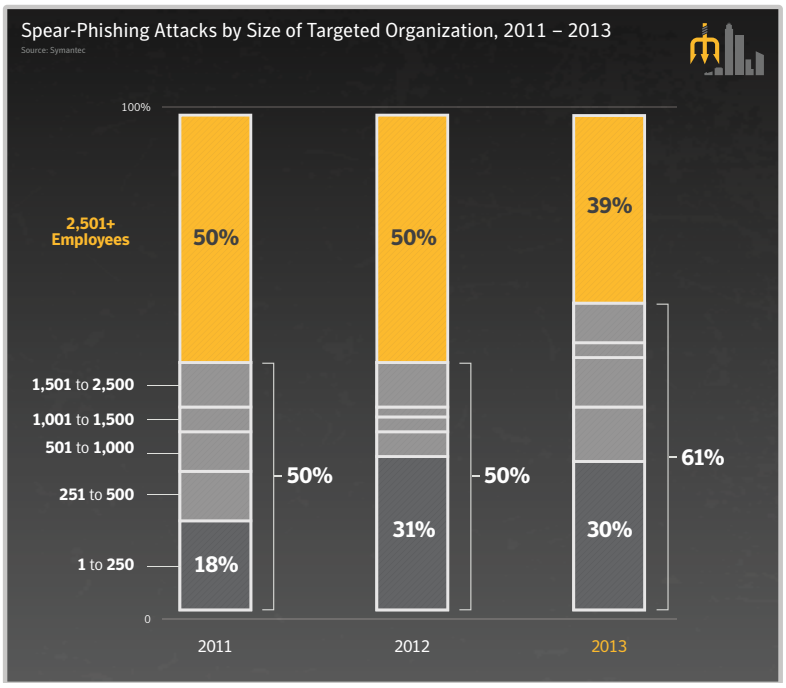


Fig. 5

- Targeted attacks aimed at small businesses (1-250 employees) in 2013 accounted for 30 percent of all such attacks, compared with 31 percent in 2012 and 18 percent in 2011. Despite the overall average being almost unchanged, the trend shows that the proportion of attacks at organizations of this size was increasing throughout the year, peaking at 53 percent in November.
- If businesses with 1-250 and 251-500 employees are combined, the proportion of attacks is 41 percent of all attacks, compared with 36 percent in 2012.
- Large enterprises comprising over 2,500+ employees accounted for 39 percent of all targeted attacks, compared with 50 percent in 2012 and 2011. The frontline in these attacks moved along the supply chain department. Large enterprises were more likely to be targeted though watering-hole attacks than through spear phishing.

For example, in 2013, 1 in 54 Symantec. cloud customers were targeted with at least one spearphishing email. The seriousness of attempted spear-phishing attacks is even clearer, using the same methodology, when comparing these numbers to the annual risk of an office fire. The odds of a building catching fire are, at worst, around one in 161.[05]

These odds change depending on the industry, the size of the organization, and an individual's role within the organization. This risk can be calculated using epidemiology concepts commonly applied to public health issues,06 in this case applying them to the industry and job role. Epidemiology is frequently used in medicine to analyze how often diseases occur in different groups of people and why. In this way, if targeted attacks are considered to be disease agents, it is possible to determine which groups are more or less at risk based on exposure to the disease. In this case, we were not just focused on the organizations being targeted within a particular sector, but on other organizations within the same industry which may not be targeted. In this way we were able to more accurately determine the odds ratio for any one type of organization being targeted. It's similar to the way risk is calculated for diseases such as lung cancer, and calculating the probability of developing the disease from exposure to tobacco smoke.

Of course an organization's risk will either rise or fall depending on their industry and number of employees (figure 8). For the individual, another factor will be their job role, as shown in figure 6.

THEFT IN THE MIDDLE OF THE NIGHT

On occasion, evidence of a cybercrime comes from an unexpected source. One company in the financial sector noticed an unusual early morning money transfer on a particular day, and from a particular computer. The company decided to check the CCTV footage and discovered that there was no one sitting at the computer at the time of the transaction. A back door Trojan was discovered during the examination of the computer. The threat was removed, but not before the attackers behind the attack made off with more than €60,000.

Fig. 6

- Personal assistants, people working in the media, and senior managers are currently most at risk of being targeted by a spearphishing campaign, based on observations in 2013.
- C-level executives, recruitment, and research and development are less likely to be targeted in the near future solely because of their job role.

Fig. 7

- Mining, Manufacturing, and Public Administration were high-risk industries based on observations made in 2013. For example, approximately 1 in 3 Symantec. cloud customers in these sectors were subjected to one or more targeted spearphishing attacks in 2013.
- Although only 0.9 percent (1 in 110) of all spearphishing attacks were aimed at the Mining sector in 2013, one-third of Mining organizations were targeted at least once. This indicates a high likelihood of being targeted, but the frequency and volume of attacks is relatively low compared to other sectors.
- Similarly Wholesale, Transportation, and Finance may be classified as medium-risk industries.
- Non-traditional services, Construction, and Agriculture fell below the base line, which means that the organizations in these industry sectors were unlikely to have been targeted solely for being in that sector.

Fig. 8

- The larger the company, the greater risk of receiving a spear-phishing email.
- One in 2.3 organizations with 2500+ employees were targeted in at least one or more spear-phishing attacks, while 1 in 5 small or medium businesses were targeted in this way

Analysis of Spear-Phishing Emails Used in Targeted Attacks

Source: Symantec

Executable type	2013	2012
.exe	31.3%	39%
.scr	18.4%	2%
.doc	7.9%	34%
.pdf	5.3%	11%
.class	4.7%	<1%
.jpg	3.8%	<1%
.dmp	2.7%	1%
.dll	1.8%	1%
.au3	1.7%	<1%
.xls	1.2%	5%

Fig. 9

- • More than 50 percent of email attachments used in spearphishing attacks contained executable files in 2013.
- Microsoft Word and PDF documents were both used regularly, making up 7.9 and 5.3 percent of attachments respectively. However, these percentages are both down from 2012.
- Java .class files also made up 4.7 percent of email attachments used in spear-phishing attacks.

WATERING HOLES

In 2013, the most sophisticated form of targeted attacks made use of "watering holes". First documented in 2011,08 this attack technique requires the attackers to infiltrate a legitimate site visited by their target, plant malicious code, and then lie in wait. As a drive-by download tactic, it can be incredibly potent. For example, the Hidden Lynx09 attacks infected approximately 4,000 users in one month alone. In some cases other visitors to a watering-hole site may not be the intended target, and are therefore either served with other forms of malware or no malware at all, rather than being subjected to the attack reserved for the primary target. This illustrates that while effective, watering holes may be used as a longer-term tactic, requiring a degree of patience on the part of the attackers as they wait for their intended target to visit the site unprompted.

To set up a watering hole, attackers generally have to find and exploit a vulnerability in a legitimate website in order to gain control and plant their malicious payload within the site. Compromising a legitimate website may seem to be a challenge for many, but vulnerability scans of public websites carried out in 2013 by Symantec's Website Security Solutions division10 found that 77 percent of sites contained vulnerabilities. Of these, 16 percent were classified as critical vulnerabilities that allow attackers to either access sensitive data, alter website content, or compromise a visitor's computers. This means that when an attacker looked for a site to compromise, one in eight sites made it relatively easy to gain access.

When a website is compromised, the attackers are able to monitor the logs of the compromised site in order to see who is visiting the website. For instance, if they are targeting organizations in the defense industry, they may look for IP addresses of known defense contractors. If these IP addresses are found in the traffic logs, they may then use the website as a watering hole.

Attackers generally have to find and exploit a vulnerability in a legitimate website in order to gain control and plant their malicious payload within the site.

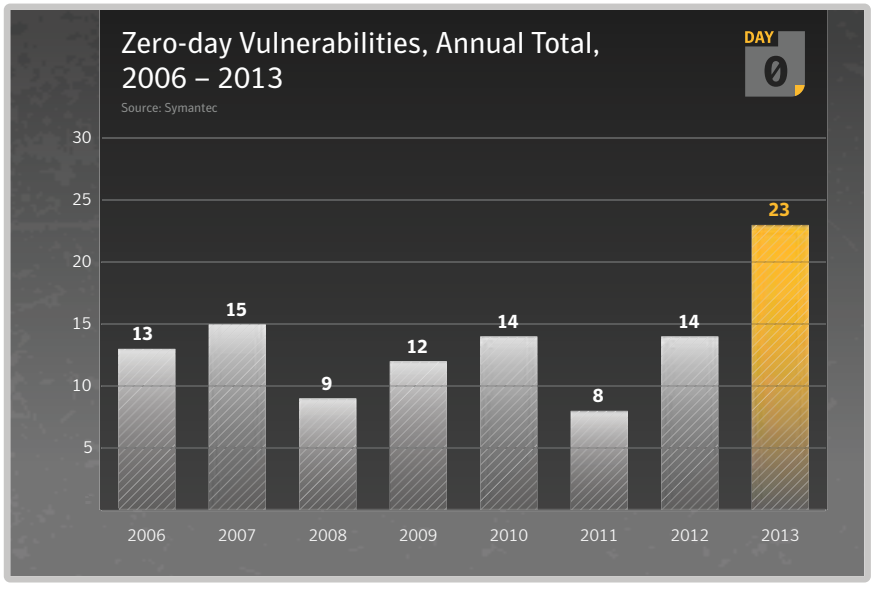


Fig. 10

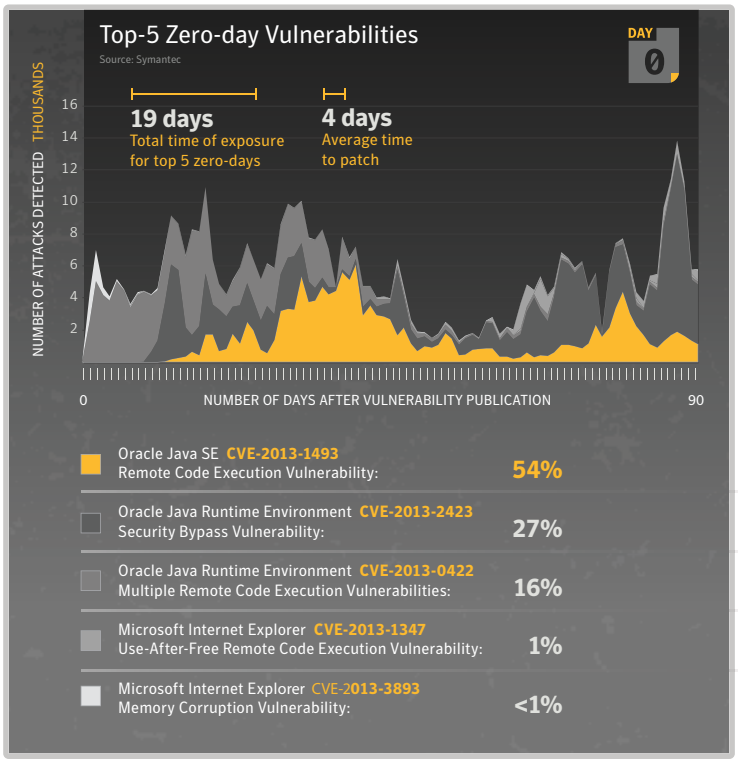


Fig. 11

- The chart above shows the malicious activity blocked by Symantec endpoint technology for the most frequently exploited vulnerabilities that were identified as zero-days in 2013.
- Within the first 5-days after publication, Symantec blocked 20,813 potential attacks, which grew to 37,555 after 10 days. Within 30 days the total for the top five was 174,651.
- For some zero-day vulnerabilities, there was a higher amount of malicious activity very soon after publication, an indication of exploits being available in the wild before the vulnerability was documented. For example, with CVE-2013-0422 after five days Symantec had blocked 20,484 malicious actions against that vulnerability, and 100,013 after just 30 days.

Attackers can even send the malicious payloads to particular IP address ranges they wish to target, in order to minimize the level of collateral damage from other people visiting the site which potentially draws attention to the existence of the attack.

Watering holes rely heavily on exploiting zero-day vulnerabilities because the chances of the attack being discovered are low. The number of zero-day vulnerabilities which were used in attacks during 2013 increased, with 23 new ones discovered during the year. This is an increase from the 14 that were discovered in 2012, and the highest figure since Symantec began tracking zero-day vulnerabilities in 2006.

In 2013 the majority of attacks that used zero-day vulnerabilities focused on Java. Java held the top three spots in exploited zero-day vulnerabilities, responsible for 97 percent of attacks that used zero-day vulnerabilities after they were disclosed. When looking at the top five zero-day vulnerabilities, the average exposure window between disclosure and an official patch was 3.8 days, and comprised a total of 19 days where users were left exposed.

One reason why watering-hole attacks are becoming more popular is that users aren't instinctively suspicious of legitimate websites that they know and trust. In general such attacks are set up on legitimate websites that contain specific content of interest to the individual or group being targeted. The use of zero-day vulnerabilities on legitimate websites made watering holes a very attractive method for attackers with the resources to orchestrate such an attack.

NETWORK DISCOVERY AND DATA CAPTURE

If attackers successfully compromise an organization they may traverse the network, attempt to gain access to the domain controller, find documents of interest, and exfiltrate the data. Downloaders were popular tools used to gain further control within an organization's network. Often referred to as "stage-one back doors", these highly versatile

forms of malicious code allow the download of other different malware, depending on what may be needed to carry out their objectives. The main reason that attackers use downloaders is that they're lightweight and easy to propagate. Once a downloader enters a network it will, by definition, download more traditional payloads such as Trojan horses to scan the network, keyloggers to steal information typed into compromised computers, and back doors that can send stolen data back to the attacker.

Once on the network, an attacker's goal is generally to traverse it further and gain access to various systems. Info-stealing Trojans are one of the more common payloads that an attacker will deliver. These Trojans quietly sit on compromised computers gathering account details. Password-dumping tools are used as well, especially when encountering an encrypted cache of passwords. These tools allow an attacker to copy encrypted (or "hashed") passwords and attempt to "pass the hash," as it is known, to exploit potentially vulnerable systems on the network.

The goal for the attacker is to gain elevated privileges on systems on the network that appeal to them, such as FTP access, email servers, domain controllers, and so on. Attackers can use these details to log into these systems, continue to traverse the network, or use them to exfiltrate data.

CASE STUDY: POINT OF SALE ATTACKS

One of the most notable incidents in 2013 was caused by a targeted attack exploiting a retailer's point of sale (PoS) systems. This resulted in a significant breach of confidential customer records. These PoS systems handle customer transactions through cash or credit cards. When a customer swipes their credit or debit card at a PoS system, their data is sent through the company's networks in order to reach the payment processor. Depending on how the system is set up, attackers could take advantage of a number of flaws within the networks to ultimately allow them to get to their targeted data.

1. First, the attacker needs to gain access to the corporation's network that provides access to the PoS systems.

2. Once the attacker has established a beachhead into the network, they will need to get to their targeted systems. To achieve this, the attacker needs to either attempt to exploit vulnerabilities using brute-force attacks or steal privileged credentials from an employee through an informationstealing Trojan.

3. The attacker must then plant malware that steals sensitive financial data, such as network-sniffing tools, which steal credit card numbers as they move through internal unencrypted networks, or RAMscraping malware, which gather credit card numbers as the computer reads them.

It's Not Just a Game Anymore Video game companies have become the target of attackers, but for more than just to steal virtual currencies, as we've seen in previous years. It appears there has been a concerted effort by hacking groups to steal the source code of popular games, particularly those in the massively-multiplayer online role-playing game (MMORPG) genre. The hackers appear to have gained access through forged digital certificates, after which point they stole source code. The motive for doing so remains unclear, though it could be to monitor game users or simply to steal the intellectual property.

4. Once the malware is planted, the attacker needs to wait until enough financial data is collected before exfiltrating it. The stolen data is stored locally and is disguised by obfuscating file names and encrypting data. The attacker can also use the stolen administrator credentials to delete log files or disable monitoring software to cover their tracks.

5. When the time comes for the attacker to exfiltrate the data, they may use a hijacked internal system to act as their staging server. The stolen data will be passed to this server and when the time comes, the details will be transferred through any number of other internal systems before reaching an external system under the attacker's control.

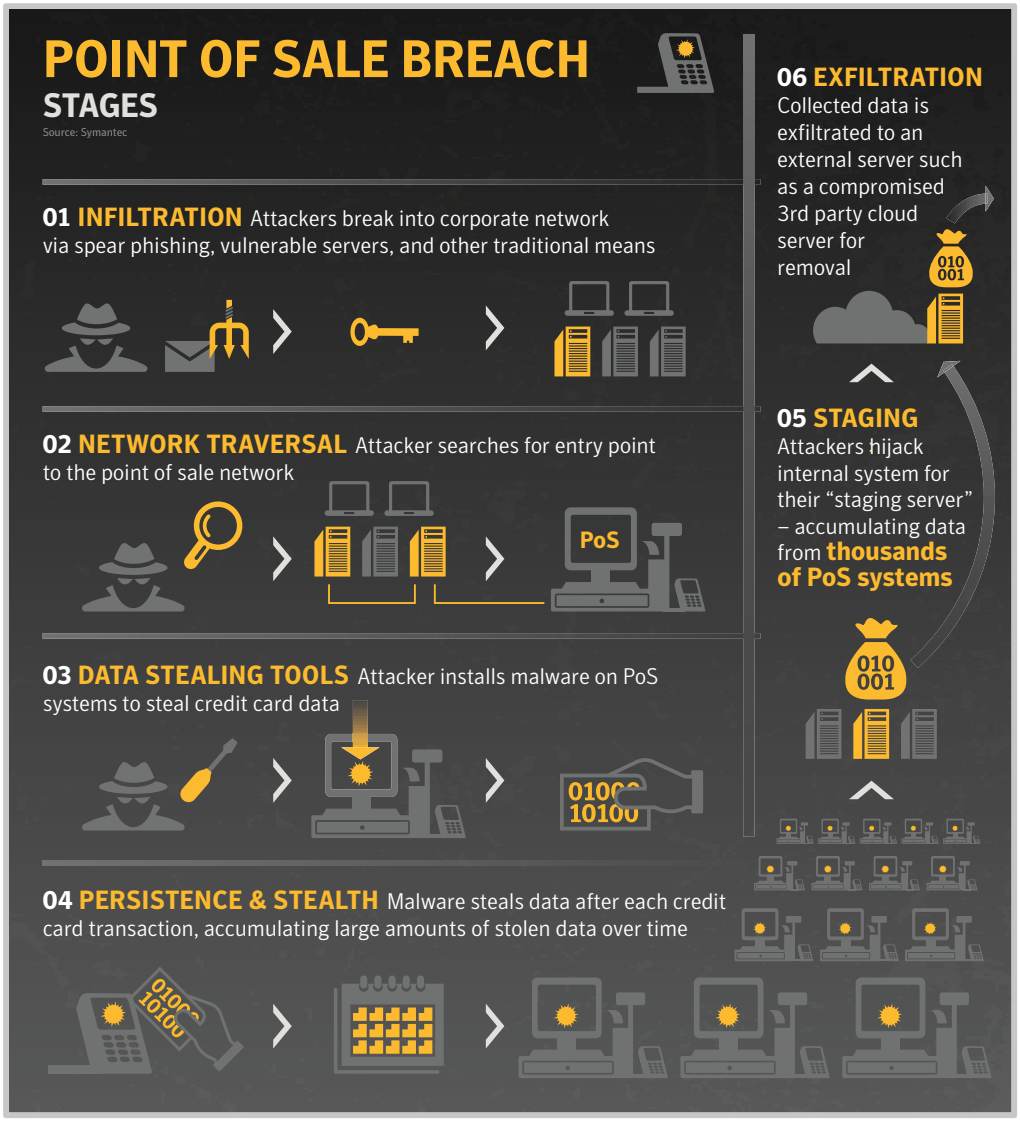


Fig. 12

DATA BREACHES

We've seen a shift in 2013 in the causes of data breaches. When thinking of a data breach, what often comes to mind are outside attackers penetrating an organization's defense. Hacking continues to lead in terms of the number of breach causes, comprising 35 percent of data breaches in 2013, but this is down from 2012. At 28 percent, accidental disclosure is up 5 percentage points from 2012 and theft or loss is close behind it, up 4 percentage points to 27 percent.

There are many situations where data is exposed by the information leaving the organization silently. Sometimes it's a well-meaning employee simply hoping to work from home by sending a spreadsheet through third-party web-based email, a cloud service, or simply by copying the files to a USB drive.

Alternatively system glitches may expose data to users who should not be able to see or share such material. For instance, users may be granted permissions on company storage resources that are higher than necessary, thus granting them too much access rather than just enough to do what they need. Privileged users, such as those granted administrative rights on work computers, are often more responsible for breaches than external hackers. These

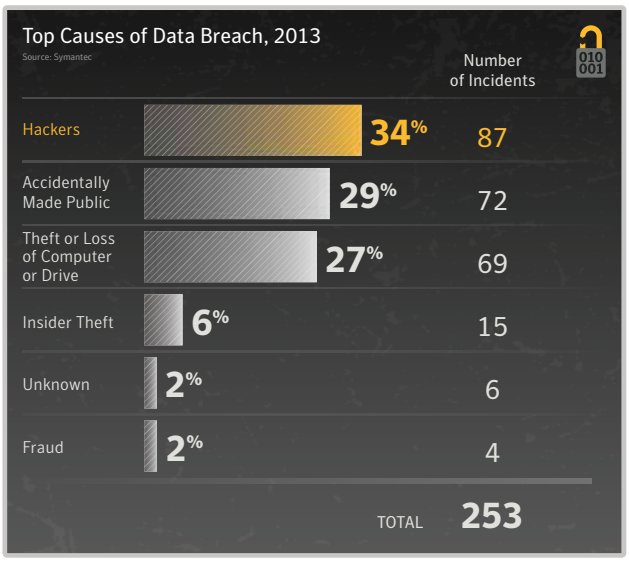


Fig. 13

- There were 253 data breach incidents recorded by the Norton Cybercrime Index for 2013, and a total of 552,018,539 identities exposed as a result
- The average number of identities exposed per incident was 2,181,891, compared with 604,826 in 2012 (an increase of over 2.5 times)
- The median number of identities exposed was 6,777 compared with 8,350 in 2012. The median is a useful measure as it eliminates extreme values caused by the most notable incidents, which may not necessarily be typical.
- The number of incidents that resulted in 10 million or more identities being exposed in 2013 was eight, compared with only one in 2012.
- Hacking was the leading source for reported identities exposed in 2013: Hackers were also responsible for the largest number of identities exposed, responsible for 35 percent of the incidents and 76 percent of the identities exposed in data breach incidents during 2013.
- The average number of identities exposed per data breach for hacking incidents was approximately 4.7 million.
- Theft or loss of a device was ranked third, and accounted for 27 percent of data breach incidents.

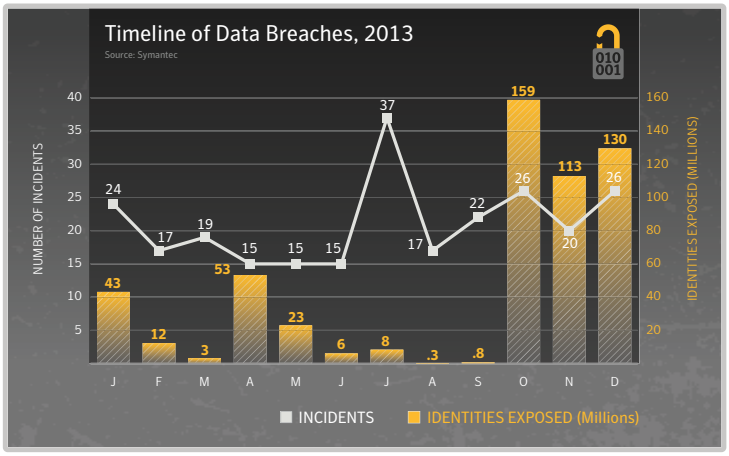


Fig. 14

users try to access data they shouldn't have access to or tamper with protections, such as data loss prevention software meant to keep sensitive data from leaving the organization's network.

In many of these cases the employee does not believe that they are putting the company at risk. In fact, according to a survey conducted by Symantec and The Ponemon Institute, 53 percent of employees believe this practice is acceptable because it doesn't harm the company.[11]

That's not to say that attacks from hackers have suddenly slowed. In 2013 there were three recordbreaking data breaches, where the numbers of identities exposed was in the hundreds of millions. These massive beaches highlight the importance of having defenses in place to keep outside intruders out as well as systems set up to stop sensitive information from leaving the network.

According to the 2013 Cost of a Data Breach study, published by Symantec and the Ponemon Institute,12 the cost of the average consolidated data breach incident increased from US$130 to US$136. However, this number can vary depending on the country, where German and US companies experienced much higher costs at US$199 and US$188, respectively.

CONSEQUENCES OF A DATA BREACH

Data theft is not a victimless crime. Data breaches pose major consequences for both the corporations that experience them and the consumers who are victims of them.

RISKS FOR THE CORPORATIONS

If a company suffers a major data breach, it can face severe repercussions that could impact its business. First, there are the reputational damages that come with a data breach. The incident could cause consumers to lose trust in the company and move to their competitors' businesses. If the company suffered a large data breach it's likely to receive extensive media coverage, further damaging the corporation's reputation.

Data theft is not a victimless crime. Data breaches pose major consequences for both the corporations that experience them and the consumers who are victims of them.

If the customers decide that the company was at fault for failing to protect their information from theft, they could file a class action lawsuit against the breached firm. For example, a class action lawsuit is being taken against a health insurer over the theft of two unencrypted laptop computers which held data belonging to 840,000 of its members.

Affected corporations could have other financial concerns beyond legal matters. We believe that on average, US companies paid US$188 per breached record over a period of two years. The only country hit with a bigger price tag was Germany, at US$199 per breached record. This price rose if the data breach was caused by a malicious attack. In these cases, US firms paid US$277 per breached record over two years, while German firms paid US$214 per record. These expenses covered detection, escalation, notification and after-the-fact response, such as offering data monitoring services to affected customers.

One US medical records company was driven to bankruptcy after a break-in which led to the exposure of addresses, social security numbers, and medical diagnoses of 14,000 people. When explaining its decision to file for Chapter 7 bankruptcy protection, the company said that the cost of dealing with the data breach was "prohibitive."

RISKS FOR THE CONSUMERS

Ultimately, consumers are the real victims of data breaches, as they face many serious risks as a result of this cybercrime.

One unintended risk for consumers whose data was stolen in this way is that their other online accounts could be compromised. Attackers use a victim's personal details to try to gain access to other accounts of more value, for example, through password reset features on websites. Depending on the stolen information, attackers could use the data to authorize bank account transfers to accounts under their control. They could also use victims' financial details to create fraudulent credit or debit cards and steal their money.

Consumers' own lax password habits could also cause several of their accounts to be compromised as the result of a data breach. If an attacker manages to obtain email addresses and passwords for one service as a result of a data breach, they could use this data to attempt to log in to other online services.

Medical identity theft could have a huge impact on the consumer, potentially costing victims thousands of dollars, putting their health coverage at risk, causing legal problems, or leading to the creation of inaccurate medical records. Attackers can use health insurance information, personal details, and social security numbers to make false claims on their victims' health insurance. They could take advantage of this data to get free medical treatment at the victims' cost, or even to obtain addictive prescription drugs for themselves or to sell to others. According to our data, the healthcare sector contained the largest number of disclosed data breaches in 2013 at 37 percent of those disclosed.

Why does it appear that the Healthcare sector is subject to a higher number of data breaches? One consideration is that few other industries can lay claim to needing to store such a variety of personally identifiable information about clients. By targeting a hospital's records, an attacker can easily gather a lot of personal information from these sources, especially if their goal is identity theft.

Medical identity theft could have a huge impact on the consumer, potentially costing victims thousands of dollars, putting their health coverage at risk, causing legal problems or leading to the creation of inaccurate medical records.

On the other hand, the healthcare industry is one of the most highly regulated industries, and required to disclose when and where a breach occurs. These sorts of disclosures garner lots of media attention. In contrast, many industries are less forthcoming when a breach occurs. For instance, if a company has trade secrets compromised, which doesn't necessarily impact clients or customers directly, they may not be quite as forthcoming with the information. Whatever the case, at 44 percent Healthcare continues to top our list of industries most impacted by data breaches.

DIGITAL PRIVACY CONCERNS

If there ever was any question that governments are monitoring Internet traffic, a spotlight was cast on the subject in 2013. A variety of leaks during the year showed that, for better or for worse, there are agencies in the world who are largely gathering anything and everything they can.

In some cases it's one nation state monitoring another. In others it's a nation state monitoring the communications of its own citizens. While some governments have been thrust into the spotlight more than others, there's no question that it is happening in many places. Online monitoring was a major security and privacy talking point in 2013.

If there ever was any question that governments are monitoring Internet traffic, a spotlight has been cast on the subject in 2013

From June 2013, several news reports were released containing new information on the US National Security Agency's (NSA) data surveillance programs. More are yet to come, considering the sheer magnitude of documents leaked by Edward Snowden, the former NSA contractor who released the data. The documents claimed that over the course of several years the NSA collected metadata from phone calls and major online services, accessed the fiber-optic networks that connected global data centers, attempted to circumvent widely-used Internet encryption technologies, and stored vast amounts of metadata gathered as part of these programs.

The US wasn't the only country engaged in cyber-espionage activities in 2013. The Snowden leaks also pointed the finger at the United Kingdom's Government Communications Headquarters (GCHQ), and the monitoring activities of other European spying agencies have come to light as well. In other parts of the globe, Symantec uncovered a professional hackers-for-hire group with advanced capabilities known as Hidden Lynx. The group may have worked for nation states, as the information that they targeted includes knowledge and technologies that would benefit other countries. Russia's intelligence forces were also accused of gaining access to corporate networks in the US, Asia, and Europe.

What's important to note is that the released data leading to many of the year's online monitoring stories was brought to the public from someone who was a contractor rather than a full-time employee, and considered a trusted member of the organization. These organizations also appeared to lack strong measures in place to prevent such data leaks, such as data loss prevention systems.

Unlike external attackers, insiders may already possess privileged access to sensitive customer information, meaning they don't have to go to the trouble of stealing login credentials from someone else. They also have knowledge of the inner workings of a company, so if they know that their organization has lax security practices they may believe that they could get away with data theft unscathed. Our recent research conducted with the Ponemon Institute says that 51 percent of employees claim that it's acceptable to transfer corporate data to their personal computers, as their organizations don't strictly enforce data security policies. Insiders could earn a lot of money for selling customer details, which may be motivation enough to risk their careers.

There are two big issues with online monitoring today, not just for governments, but also for organizations and ordinary citizens: Personal digital privacy, and the use of malware or spyware. It's clear that governments are monitoring communications on the internet, leading more Internet users to look into encryption to protect their communications and online activities. What's more troubling for those concerned about safeguarding their privacy is that nation states have largely adopted the same techniques as traditional attackers, using exploits and delivering malicious binaries. From a security perspective, there is very little difference between these techniques, targeted attacks, and cybercrime in general.

E-CRIME + MALWARE DELIVERY TACTICS

E-CRIME AND CYBER SECURITY

The use of computers and electronic communications equipment in an attempt to commit criminal activities, often to generate money, is generally referred to as e-crime and it continues to play a pivotal role in the threat landscape. The scope of what is covered by e-crime has also changed and expanded over the years and now includes a variety of other potentially illegal activities that may be conducted online, such as cyber bullying, the hijacking of personal data, and the theft of intellectual property.

The threats used to carry out the more traditional e-crime attacks rely heavily on social engineering in order to succeed, and may be delivered in one of two ways; through web-based activity, drive-by downloads, or by email; similar to the way spam campaigns are conducted.

The criminals behind these e-crime attacks are well organized, having a sophisticated malicious distribution network behind them. This plays out in a format where different attackers carry out different tasks. One group will focus on compromising computers, another will configure and administer those computers to carry out various malicious activities, while yet another will broker deals for renting the use of those compromised computers to other cybercriminals.

BOTNETS AND THE RENTAL MARKET

Cybercriminals involved in e-crime generally start out by working to get malware onto computers, turning them into "zombies" with the aim of adding them to larger networks of similarly compromised computers, called botnets, or "robot networks". A botnet can be easily controlled from a central location, either through a command and control (C&C) server or a peer to peer (P2P) network. Zombie computers connected to the same C&C channels become part of the same botnet.

Botnets are an extremely potent asset for criminals because they can be used for a wide variety of purposes, such as sending spam emails, stealing banking information, conducting a distributed denial-of-service (DDoS) attacks against a website, or a variety of other malicious activities. They have also become a core tool for administering compromised computers that are rented to yet another third party for malicious purposes.

Adding a computer to a botnet is generally just the first step. The attackers seek out other cybercriminals in the hope that they can lease the botnets for various purposes. This rental style gives the initial attacker a lot of leverage and flexibility concerning how they monetize and use the computers they've compromised and look after. Configurations can vary widely, focused on types of computers, regions, languages, or other features that the buyer is looking to gain access to. Prices also vary depending on the length of rental and the job for which the computers are to be used.

For example, infections in some countries are considered more valuable than others. In the case of click fraud, an infection will create fake user clicks on advertisements to earn affiliate fees. American and UK computers tend to be preferred because pay-per-click advertisers in these countries will pay more. The same applies to banking Trojans, which are generally more focused on targeting Western bank accounts.

The good news is that there were a number of takedowns that occurred in 2013. Of particular note are the efforts to take down the Bamital and ZeroAccess botnets.

Bamital was taken down in February, thanks to a cooperative effort on the part of Symantec, Microsoft, Spain's Civil Guardia, and Catalunyan CERT (CESICAT).This botnet had been responsible for a significant amount of click-fraud traffic, generating upwards of three million clicks per day at its peak.13 To perform click fraud, the botnet would hijack the search results typed into compromised computers, redirecting the users to predetermined pay-per-click sites, with the goal of making money off those clicks. When a computer is used to perform click fraud, the user will rarely notice. The fraud consumes few computer resources to run, and at the most takes up extra bandwidth with the clicks. The attackers make money from pay-per-click advertisers and publishers— not from the user. This is in contrast with other forms of malware such as ransomware, where it is clear that an infection has occurred. A computer may be used in a click-fraud operation for an extended period of time, performing its activity invisibly during the daily operation of the computer.

The partial takedown during the year made a lasting impact on the operations of the ZeroAccess botnet. Symantec security researchers looking at the threat discovered a flaw in ZeroAccess that could allow them to sinkhole computers within the botnet. The operation succeeded in liberating approximately half a million ZeroAccess clients from the botnet network.[15]

At that time, ZeroAccess was one of the larger botnets in existence, and one that used P2P communications to maintain links between clients. These types of P2P botnets tend to be quite large overall; Helios and Zbot (a.k.a. GameOver Zeus) are two other examples of large botnets that use similar communication mechanisms. It isn't entirely clear if these botnets are big because they utilize P2P, or they utilize P2P because they're big. However, using P2P for communications does make it more difficult to take down a botnet, given the lack of a centralized C&C server.

AT A GLANCE

- The criminals behind e-crime have set up sophisticated malicious distribution networks.
- The monthly volume of ransomware has increased by over six times since the beginning of 2013.
- Web attack toolkits continue to be a primary method for compromising computers, even with the arrest of the alleged creator of the Blackhole exploit kit in 2013.
- The number of vulnerabilities disclosed has reached record levels in 2013.

Botnets are an extremely potent asset for criminals because they can be used for a wide variety of purposes

Large botnets like Cutwail and Kelihos have made their presence felt in the threat landscape this year by sending out malicious attachments. The threats are generally like banking Trojans or downloaders, such as Downloader.Ponik and Downloader.Dromedan (also called Pony and Andromeda respectively), which download more malware.

Trojan.Zbot (a.k.a. Zeus) continues to make an impact in the botnet world. Having its malicious payload based on easy-to-use toolkits has allowed Zbot to maintain its popularity with threat actors. In 2013 we've seen Zbot being packed in different ways and at different times in order to evade detection. These packing techniques appear almost seasonal in their approach to evading detection, but underneath it all it's always the same Zeus code base.

Malicious Activity by Source: Bots, 2012–2013

Source: Symantec

Country/Region	2013 Bots Rank	2013 Bots %	2012 Bots Rank	2012 Bots %
United States	1	20.0%	1	15.3%
China	2	9.1%	2	15.0%
Italy	3	6.0%	5	7.6%
Taiwan	4	6.0%	3	7.9%
Brazil	5	5.7%	4	7.8%
Japan	6	4.3%	6	4.6%
Hungary	7	4.2%	8	4.2%
Germany	8	4.2%	9	4.0%
Spain	9	3.9%	10	3.2%
Canada	10	3.5%	11	2.0%

Fig. 1

- Unsurprisingly, the US and China have the most densely populated bot populations, largely owing to their large Internet populations. The US population are avid users of the Internet, with 78 percent Internet penetration, but undoubtedly their keen use of the Internet contributes to their popularity with malware authors. China also has the largest population of Internet users in the Asia region, with 40 percent Internet penetration and accounting for approximately 50 percent of the Internet users in the Asia region.14

- Italy has a lower percentage of bots in the country, but is ranked third highest in 2013, compared with fifth in 2012.

- The US, Germany, Spain and Canada all increased their relative proportions of the world's bots in 2013, while the proportions in the other geographies listed has diminished.

Top-Ten Botnets, 2013

Source: Symantec

Spam Botnet Name	% of Botnet Spam	Estimated Spam Per Day	Top Sources of Spam From Botnet		
KELIHOS	46.90%	10.41BN	Spain 8.4%	United States 7.2%	India 6.6%
CUTWAIL	36.33%	8.06BN	India 7.7%	Peru 7.5%	Argentina 4.8%
DARKMAILER	7.21%	1.60BN	Russia 12.4%	Poland 8.3%	United States 8.1%
MAAZBEN	2.70%	598.12M	China 23.6%	United States 8.2%	Russia 4.8%
DARKMAILER3	2.58%	573.33M	United States 18.2%	France 10.4%	Poland 7.5%
UNKNAMED	1.17%	259.03M	China 35.1%	United States 10.0%	Russia 7.5%
FESTI	0.81%	178.89M	China 21.9%	Russia 5.8%	Ukraine 4.7%
DARKMAILER2	0.72%	158.73M	United States 12.6%	Belarus 8.3%	Poland 6.6%
GRUM	0.53%	118.00M	Russia 14.5%	Argentina 6.9%	India 6.9%
GHEG	0.35%	76.81M	Poland 17.4%	Vietnam 12.1%	India 11.5%

Fig. 2

- 76 percent of spam was sent from spam botnets, down from 79 percent in 2012.

- It is worth noting that while Kelihos is the name of a spam-sending botnet, Waledac is the name of the malware used to create it. Similarly, Cutwail is another the spam-sending botnet and Pandex is the name of the malware involved.

RANSOMWARE: WHEN DATA BECOMES A HOSTAGE TO FORTUNE

In October 2013, the US Federal Bureau of Investigation issued a warning about a new type of malware that had appeared. The threat, known as CryptoLocker, encrypted a victim's documents and demanded payment in return for the decryption key. Two weeks later, the UK equivalent of the FBI, the National Crime Agency, also issued a public warning about CryptoLocker. It isn't often that one piece of malware mobilizes law enforcement agencies across the world, and it is indicative of the level of panic created by CryptoLocker during 2013.

Despite the hype, CryptoLocker is not a completely new malware. Instead it is the latest evolution of a family of threats known as ransomware. Ransomware first came to prominence a decade ago. The business model usually involves the victim's computer being locked. Attackers demand a ransom in order to remove the infection.

However, CryptoLocker has managed to capture the public imagination because it represents the perfect ransomware threat: It encrypts the user's data and, unlike most malware infections, no fix can rescue it. CryptoLocker uses strong encryption, meaning the victim is left with the unpalatable choice of saying goodbye to their valuable personal data or paying the attackers a ransom fee.

Symantec noticed a significant upsurge in the number of ransomware attacks during 2013. During January we stopped over 100,000 infection attempts. By December that number had risen more than six-fold. There was a noticeable uptick in detection from the month of July onwards, peaking in November.

CryptoLocker first began to circulate in September, and while CryptoLocker detections grew quickly (by 30 percent in December alone), the number of definitive CryptoLocker detections is still a very small proportion of overall ransomware detections. For example, in December only 0.2 per cent (1 in 500) of all ransomware detections by Symantec was indisputably identified as CryptoLocker.

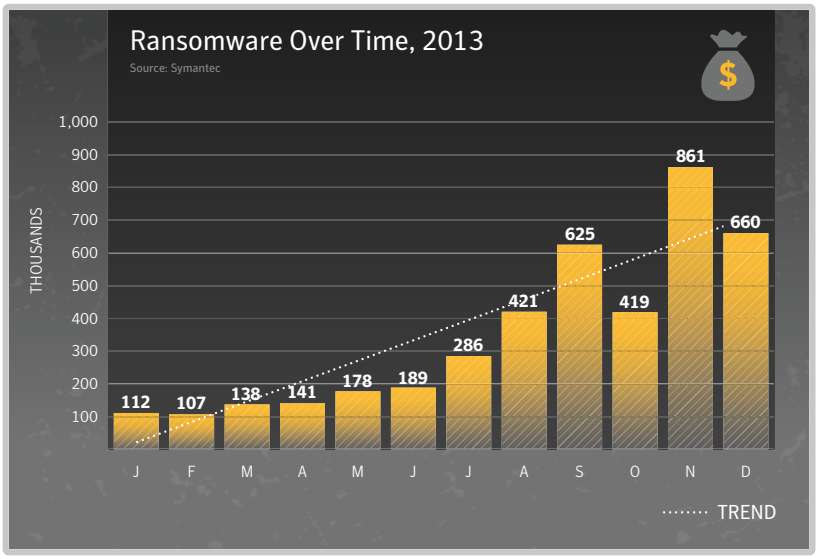


Fig. 3

- Monthly ransomware activity increased by 500 percent from 100,000 in January to 600,000 in December, increasing to six times its previous level.

Ransomware, including CryptoLocker, continues to prove lucrative for attackers. Symantec research indicates that on average, 3 percent of infected users will pay the ransom.

However, this statistic only tells part of the story, and its prevalence may be higher. CryptoLocker is often blocked by intrusion prevention systems (IPS) which may simply identify it as generic ransomware rather than a specific variant.

Ransomware, including CryptoLocker, continues to prove lucrative for attackers. Symantec research indicates that on average, 3 percent of infected users will pay the ransom. These figures tally with work done by other researchers.[16]

Analysis by Symantec of the ransoms demanded by CryptoLocker infections indicates that most variants demand US$100 to $400 for a decryption key. This is roughly in line with the ransom amount demanded by other ransomware variants. Although CryptoLocker is a more effective threat, attackers have yet to take advantage of this by demanding larger ransoms.

The amount of money being paid in ransom is difficult to assess, however some efforts have been made to track payments made through Bitcoin. All Bitcoin transactions are logged as public record, and searching for Bitcoin addresses used to collect ransom can yield some insight. From the small number of Bitcoin addresses analyzed, it is clear that ransomware distributors have without a doubt earned tens of millions over the last year.

Analysis of ransom amounts is complicated somewhat by the fact that many variants demand payment in Bitcoin. Our analysis of CryptoLocker ransom demands found that attackers generally seek between 0.5 and 2 Bitcoin. Lower ransom demands began appearing near the end of 2013. This reduction had less to do with any newfound altruism on the part of attackers and more to do with the soaring value of Bitcoin. The virtual currency was trading at just over US$100 when CryptoLocker first appeared in September. By December its value had increased to over US$1,000.

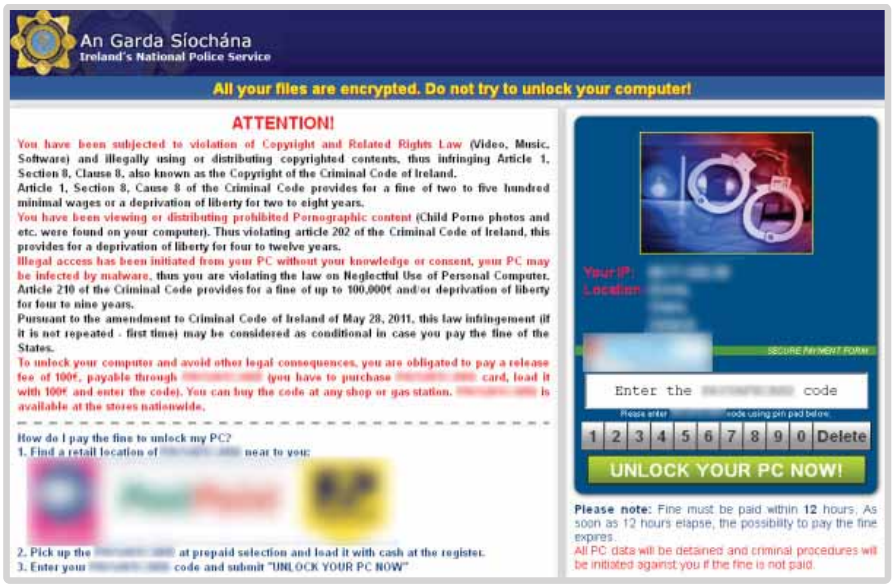


Fig. 4 Browser-based ransomware threat, Browlock.

This suggests that attackers have concluded that US$100 to $400 is the optimum ransom amount, and they will move to adjust their demand to avoid pricing themselves out of the market. Some attackers have also refined their ransom tactics by introducing a second, larger ransom of 10 Bitcoin for victims who miss the original 72 hour deadline. The attackers appear to have concluded that some potential opportunities were left unexploited by their original business model, with some victims willing to pay significant amounts for the return of valuable data. This higher ransom tier may also have the secondary purpose of exerting additional pressure on victims to pay within the deadline.

Meanwhile, older ransomware attack techniques have started to seep into markets previously unexploited. More localized content, based on location data, has started to appear in Latin American countries. In many ways, this form of ransomware is similar to what has been seen in English-speaking countries in previous years. The reasons behind this are likely precipitated by the increasing availability of online payment providers in these regions. With easy options for payment, ransomware has begun to appear in these areas, with the Reventon and Urausy versions already having been discovered with Spanish variants.

In the grand scheme of the threat landscape, ransomware does not make up a huge percentage of overall threats, but it clearly does serious damage particularly to the victims who may not have backed-up their data to begin with. In the future, new ransomware schemes may emerge. Since some groups have had success with it, others may jump on the bandwagon. Toolkits for creating these types of ransomware have been developed. Browser-based ransomware also began to appear near the end of the year, which uses JavaScript to prevent a user from closing the browser tab,17 and more of these ransomware-type scams will likely be seen in the future.

In the grand scheme of the threat landscape, ransomware does not make up a huge percentage of overall threats, but it clearly does serious damage, particularly to the victims who may not have backedup their data to begin with.

BANKING TROJANS AND HEISTS

Banking Trojans are a fairly lucrative prospect for attackers. Today's threats continue to focus on modifying banking sessions and injecting extra fields in the hope of either stealing sensitive banking details or hijacking the session. Some of the more common banking Trojans include Trojan. Tiylon18 and a variant of the Zbot botnet, called Gameover Zeus. Symantec's State of Financial Trojans 2013 whitepaper19 concluded that in the first three quarters of 2013, the number of banking Trojans tripled. More than half of these attacks were aimed at the top 15 financial institutions, though over 1,400 institutions have been targeted in 88 countries. While browser-based attacks are still common, mobile threats are also used to circumvent authentication through SMS messages, where the attacker can intercept text messages from the victim's bank.

The most common form of attack continues to be financial Trojans which perform a Man-In-The- Browser (MITB) attack on the client's computer during an online banking session. Symantec analyzed 1,086 configuration files of 8 common financial Trojans. The malware was configured to scan for URLs belonging to 1,486 different organizations. All of the top 15 targeted financial institutions were present in more than 50 percent of the analyzed configuration files.

In addition to those attacks, Symantec observed an increase in hardware-supported attacks in 2013. Besides the still popular

Attackers are trying to extract every last bit of money possible by utilizing every monetization option at their disposal with the compromised computers they control.

skimming attacks, a new piece of malware was discovered named Backdoor. Ploutus which targeted ATMs. Initially discovered in Mexico, the malware soon spread to other countries, with English versions emerging later.

The malware allows for criminals to effectively empty infected ATMs of cash. The malware is applied to the ATM by physically inserting a malicious CD-ROM and causing the machine to boot from it. While booting, the malware is installed onto the system. The attacker can then use specific key combinations on the keypad to interact with the malware and initiate the ultimate goal – to dispense all available cash from the cassettes. Later variants allow cash to be dispensed by sending a special SMS to an installed GSM modem at the ATM.

Meanwhile in Britain, a gang attempted to steal millions from a bank in London by attaching a KVM wireless switch to computers at one of the bank's branches. They infiltrated the branch by posing as computer repair personnel. This allowed them to remotely control these computers over a wireless link, most likely with intent to leverage this access to defraud the bank. However, the attack was foiled and the police arrested 12 men involved in this scam. A similar attack on another bank in London resulted in eight arrests. In this case the attackers were successful in transferring funds of around £1.3 million from the bank through KVM-controlled machines. The wireless transmitter packages were installed a day earlier by an attacker disguised as an IT technician.

These examples highlight the trend that attackers are increasingly targeting physical systems directly at financial institutions. This is similar to the trend that what we have observed with attacks against point of sale (PoS) systems at retailers.

Another popular method employed last year was to use DDoS attacks as distractions while the attackers conducted the fraudulent transactions. A construction company and its bank in California were attacked using this method: While a classic Zeus Trojan started to transfer US$900,000 out of clients' accounts, the attackers started a DDoS attack against the bank to obfuscate their actions and to keep the bank's Computer Emergency Readiness Team (CERT) busy.

MONETIZATION: MALWARE AS A COMMODITY

E-crime in 2013 can be summed up as follows: Attackers are trying to extract every last drop of cash available, using every monetization option at their disposal with the compromised computers they control. Compromised computers have essentially become just another commodity, where attackers work to maximize the ways they make money from them.

Top-10 Malware, 2013

Source: Symantec

Rank	Name	% Overall
1	W32.Ramnit	15.4%
2	W32.Sality	7.4%
3	W32.Downadup	4.5%
4	W32.Virut	3.4%
5	W32.Almanahe	3.3%
6	W32.SillyFDC	2.9%
7	W32.Chir	1.4%
8	W32.Mabezat	1.2%
9	W32.Changeup	0.4%
10	W32.Xpaj	0.2%

Fig. 5

The attackers will generally monitor the compromised computers, often through a back door connection to an administration tool such as a botnet dashboard, to determine what malicious faucets they can tap. For instance, they may start with a banking Trojan and wait to see if they can gather any banking details entered into the compromised computer. If nothing is captured by the banking Trojan, they may try ransomware with a pornographic theme, in the hope that they can extort money from the user through the ransom attempt.

The attackers will generally monitor the compromised computers, often through a back door connection to an administration tool such as a botnet dashboard, to determine what malicious faucets they can tap.

In one such scenario, an attack group may compromise computers and initially install a downloader followed by a banking Trojan. The attackers monitor to see what financial institutions the user interacts with, in the hopes they connect to a bank in a specific region. If they don't see any banking activity over a period of a week or two, the attack group will change tactics and install ransomware using the original downloader. If the victim pays the ransom, they'll then install a spam Trojan and convert the computer into a spam bot, which will run behind the scenes without the user's knowledge.

While the payouts from cybercrime can be high, so too can the punishment for getting caught. 2013 saw several cases where arguably harsh punishments were handed out to cybercriminals. While punishments like the 18-year sentence given to a Ukrainian cybercriminal found guilty of running a website where stolen financial data was bought and sold may seem deserved, others have been more questionable. For instance a man from the US was given two years federal probation and a hefty fine of US$183,000 for his part in a DDoS attack against a multinational corporation. The guilty man in this case used the Low Orbit Ion Cannon DDoS tool for approximately 60 seconds as part of a larger group of hacktivists taking part in an Anonymous campaign. Whether or not people think these punishments are fitting of the crimes, one thing is clear—Law makers and enforcers now realize the potential and actual impact cybercrime can have.

THREAT DELIVERY TACTICS

TOOLKITS

A major shift in the realm of toolkits happened in early October of 2013 with the arrest of the Blackhole and Cool Exploit Kit author, nicknamed "Paunch". The Blackhole exploit kit has dominated the web attack toolkit charts for the last few years and looked poised to do so again, based on the numbers leading up to and including October.

It appears that Blackhole has largely fallen off the map, while other toolkits have stepped in to take its place. For instance, the attackers behind the Cutwail botnet, who used to rely heavily on Blackhole, appear to have switched to the Magnitude exploit kit (a.k.a. Popads).20 The Styx and Nuclear kits have been picked up by the attackers distributing Trojan.Shylock.[21] The authors of the ransomware threats such as Revention (Trojan.Ransomlock.G) have moved to the WhiteHole kit.[22]

It's possible that in the near future, the source code for the Blackhole toolkit will appear online and new people will pick it up, create their own version, and help to develop it. Releasing source code like this can help someone mask their trail from investigators.

Eventually, the void left by Blackhole will be filled by another toolkit. Much like the arrest of a drug kingpin causes lower ranking criminals to scramble to fill the void, so too will the chaos caused by the arrest of the apparent Blackhole author eventually settle and a new toolkit will take its place.

BUSINESS MODEL

Years ago, web-attack toolkits were sold on underground forums, where one person would sell it for a set amount to an associate, who would sell it on to another associate, and so on. The distribution worked in a black market sense, but the developer of the attack toolkit would miss a large percentage of revenue,

Eventually, the void left by Blackhole will be filled by another toolkit. Much like the arrest of a drug kingpin causes lower ranking criminals to scramble to fill the void, so too will the chaos caused by the arrest of the Blackhole author eventually settle and a new toolkit will take its place.

where someone who simply possessed the code could profit without doing much work.

In the last few years, the Blackhole toolkit changed all that by introducing a service model that has grown to become the dominate way toolkits operate. In this service-style model, the web-attack toolkit developer maintains control of the code and administers the toolkit.

The kit can be locked down to a compromised computer of the attacker's choice, but the owners of the toolkit will offer access as a service where they will administer the kit. This way the developer maintains control of the kit code, rather than releasing it in underground forums.

WEB ATTACKS BLOCKED PER DAY

This sort of setup has allowed toolkit owners to experiment with different service offerings. This ranges from end-to-end coverage where the toolkit administrator sets everything up, to a less hands-on approach where tech support services are available to help the purchaser if they encounter configuration issues.

For advanced attacker clientele with some level of technical know-how, there is access to redirect their traffic from computers they've compromised to the web attack toolkit. However, in the case of setups like Blackhole, the toolkit uses legitimate PHP obfuscators, protecting the toolkit developers "intellectual property." This means that even if someone has access to a system running Blackhole, the

code is unreadable without the proper keys to decode it.

When the primary work is handled by the toolkit owner, it requires far less administration on the attacker's side, or even knowledge of how to set up the attacks. In fact today's toolkit clients are usually of limited technical expertise when compared to those offering toolkit services. At most they know enough to set up and administer the kit, but probably don't have the skills to write the code themselves. They're simply out to make money through using the services being provided.

Of course, the Achilles heel for this system is the locked-down software-as-a-service model. This is exactly what led to the colossal disruption that the Blackhole toolkit experienced when "Paunch" was arrested.

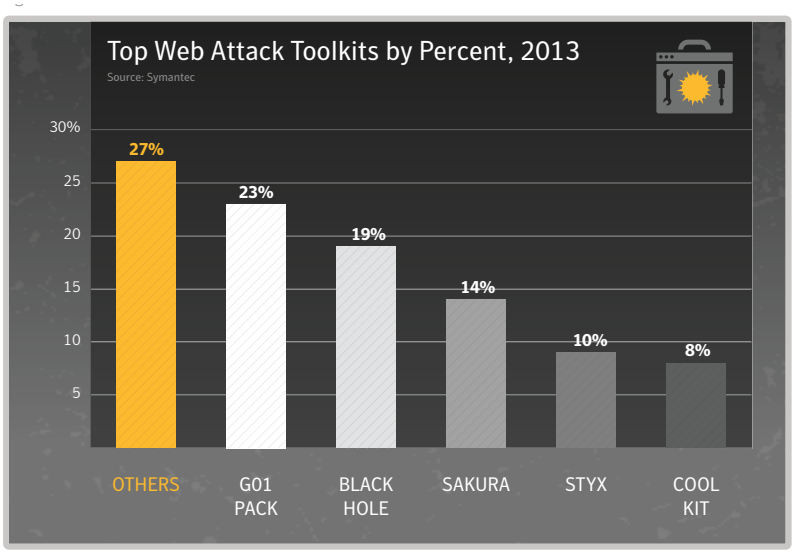


Fig. 6

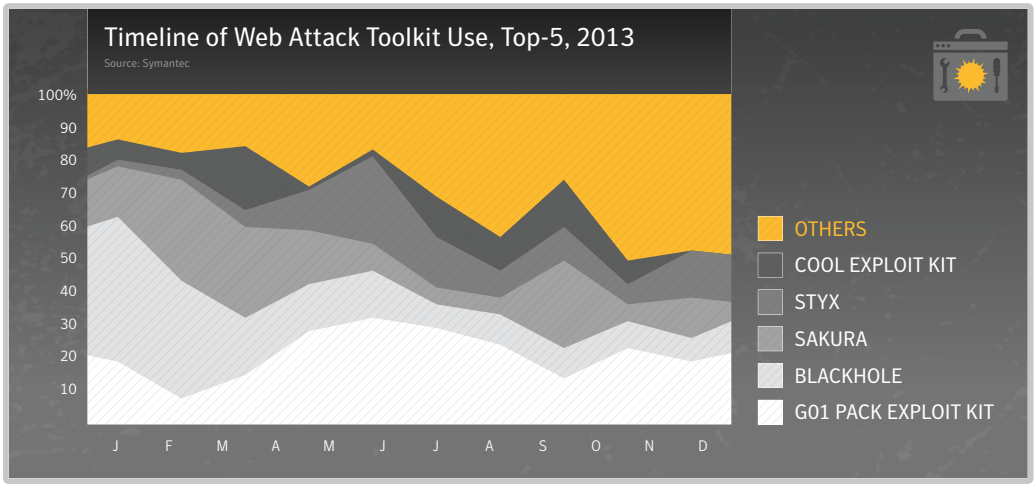


Fig. 7

- The earlier dominance of the Blackhole toolkit had all but disappeared by the end of 2013 when the alleged person responsible for it was arrested in October. Blackhole was ranked first in 2013 with 44.3 percent of total attacks blocked; however, The G01Pack Exploit Kit was ranked first in 2013 with 23 percent of attacks blocked.

- The Sakura toolkit that ranked second in 2012, accounting for 22 percent of attacks is now ranked third with 14 percent in 2013.

- Many of the more common attack toolkits were updated in 2013 to include exploits for the Java Runtime Environment, including CVE-2013-0422, CVE-2013- 2465 and CVE-2013-1493 and the Microsoft Internet Explorer vulnerability CVE-2013-2551.

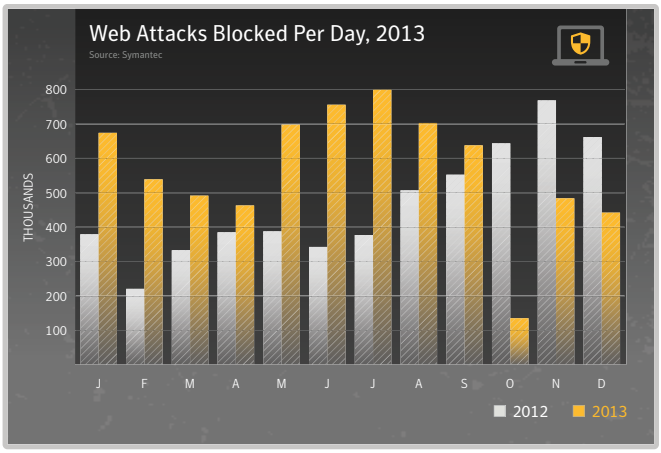


Fig. 8

- The average number of malicious websites blocked each day rose by approximately 22.5 percent from approximately 464,100 in 2012 to 568,700 in 2013.
- The highest level of activity was in July, with approximately 799,500 blocks per day.
- The lowest rate of malicious activity was 135,450 blocks per day in October 2013; this is likely to have been connected to the arrest in Russia of "Paunch," the alleged author of the Blackhole and Cool Exploit web attack toolkits. Blackhole operated as a software-as-a-service toolkit, which was maintained in the cloud. With no one around to update it, Blackhole quickly became less effective, leaving a space for other operators to move in

CLASSIFICATION OF MOST FREQUENTLY EXPLOITED WEBSITES IN 2013

- The malicious URLs identified by the Norton Safe Web technology were classified by category using the Symantec Rulespace23 technology, and the most frequently abused sites for malicious code were listed in the table above.
- Approximately 67 percent of websites used to distribute malware were identified as legitimate, compromised websites that could be classified, compared with 61 percent in 2012. This figure excludes URLs that contained just an IP address and did not include general domain parking and pay-perclick websites.
- The Technology category accounted for 9.9 percent of malicious Website activity identified
- The Illegal category is for sites that fall into the following sub-categories: Activist Groups, Cyberbullying, Malware Accomplice, Password Cracking, Potentially Malicious Software and Unwanted Programs, Remote Access Programs, and several other phishing and spam-related content.
- Analysis of websites that were used to deliver drive-by fake antivirus attacks revealed that four percent of threats found on compromised Art and Museum sites were related to fake antivirus software. Moreover, 50 percent of fake antivirus attacks were found on compromised Art and Museum sites. Additionally, 42 percent of attacks found on compromised Shopping sites were fake antivirus software.
- Analysis of websites that were used to deliver attacks using browser exploits revealed that 21 percent of threats found on compromised Anonymizer sites were related to browser exploits. Furthermore, 73 percent of browser-exploit attacks were found on compromised Anonymizer sites and 67 percent of attacks found on compromised Blogging sites involved browser exploits.
- Finally, 17 percent of attacks used on social networking sites were related to malware hosted on compromised Blogging sites. This is where a URL hyperlink for a compromised website is shared on a social network. Similarly, hosting websites accounted for 4 percent of social networking related attacks. Hosting covers services that provide individuals or organizations access to online systems for websites or storage, often using free cloud-based solutions.

Most Frequently Exploited Websites, 2013

Source: Symantec

Rank	Top 10 Most Frequently Exploited Categories of Websites	% of Total Number of infected Websites
1	Technology	9.9%
2	Business	6.7%
3	Hosting	5.3%
4	Blogging	5.0%
5	Illegal	3.8%
6	Shopping	3.3%
7	Entertainment	2.9%
8	Automotive	1.8%
9	Educational	1.7%
10	Virtual Community	1.7%

Fig. 9

Since the toolkit was run and administered by a small group of developers, the toolkit collapsed when they were arrested.

SPAM, COMPROMISED SITES, AND MALVERTISING

The vast majority of infections that occur through web attack toolkits are spam-relays, compromised websites, and malvertisments. None of these techniques are new, pointing again to the fact that age-old techniques continue to reap rewards for attackers.

The area of the most growth in 2013 has been in malvertising. Malvertising is the process of serving up malicious code through advertising programs. When successful, this allows attackers to serve up specially-crafted ads on legitimate websites, often bypassing security mechanisms that may be set up on the primary site because the content comes from a third party.

For instance, near the end of the year a large malvertising campaign was used to spread the Browlock ransomware threat.24 This form of attack is extremely difficult to block, because attackers are signing up with advertisers, and initially serve up perfectly legitimate ads on legitimate websites. After a few weeks of apparent legitimate activity, the attackers switch over to serving up malicious ads. It's a long-term strategy that pays off due to the large amount of traffic it can gather very quickly. Lots of hits may come through within a few hours before the website discovers the malicious ad in question and blocks it from their advertising network.

Advertising companies are aware of this behavior and are taking action to prevent it, including forming organizations to investigate this behavior such as the Online Trust Alliance.25 Ad companies check IP addresses of registered accounts and share suspicious addresses. They also look for activity on registered domain names which domains

The vast majority of infections that occur through web attack toolkits are spam, compromised websites, and malvertisments. None of these techniques are new, pointing again to the fact that ageold techniques continue to reap rewards for attackers.

advertisers direct their ads towards. If the domain has only recently been registered a week or two, they may deny access to the ad network.

SOCIAL ENGINEERING TOOLKITS: FROM RATS TO CREEPWARE

While web-attack toolkits tend to dominate the discussion in the threat landscape, they are not the only type of toolkits out there. There are also toolkits designed for penetration testing and detecting vulnerabilities that are open to exploits, often used legitimately by the whitehat community, but are often also employed by blackhat cybercriminals.

Probably the second most commonly known type of toolkit is the remote administration tool (RAT). These toolkits have been around for many years, such as the RATs behind the Zeus botnet, and are often used to create payload Trojans with various features as well as to obfuscate the binaries in an attempt to evade antivirus detection.

Social Engineering toolkits can be used to create phishing sites such as fake Facebook login pages. These are essentially web-design tools with extra features for hacking. For instance, an attacker can specify the type of information they want to collect on the back end of the website.

Creepware is a type of threat that uses toolkits. These threats are usually installed through social engineering and allow attackers to spy

on the victims.26 In many cases, the attackers administer their creepware by using toolkits that allow them to carry out various activities through the toolkit control panel.

VULNERABILITIES: THE PATH TO EXPLOITATION

Vulnerabilities continue to be one of the core choices for the delivery of malicious code. Vulnerabilities are being exploited to serve up all sorts of threats such as ransomware, Trojans, backdoors, and botnets. The total number of vulnerabilities disclosed in 2013 supports this - at 6787 vulnerabilities disclosed, the number is higher than any year previously reported.

The number of vulnerabilities being exploited in zero-day attacks was up in 2013, often used in watering-hole attacks. This increase in the number of zero-day vulnerabilities occurred for the most part in the first half of the year. The reduction in the latter half of the year could have a lot to do with the complexity of exploitation for the zero-days discovered later in the year. This could point to a future landscape where vulnerability exploitation becomes more difficult.

Once a zero-day is disclosed, further exploits are developed and incorporated into toolkits within a matter of days, as attackers scramble

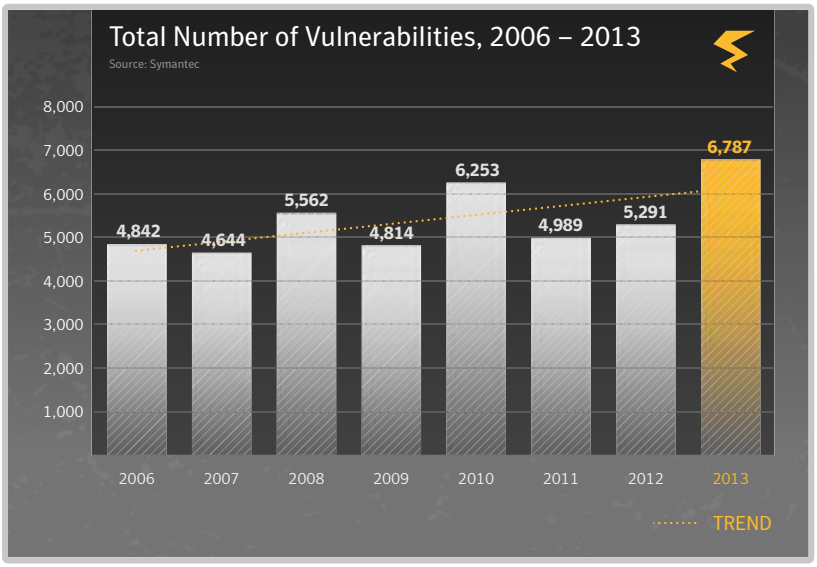


Fig. 10

- There were 6,787 vulnerabilities disclosed in 2013, compared with 5,291in 2012.
- In 2013 there were 32 public SCADA (Supervisory Control and Data Acquisition) vulnerabilities, compared with 85 in 2012 and 129 in 2011
- A zero-day vulnerability is one that is reported to have been exploited in the wild before the vulnerability is public knowledge and prior to a patch being publicly available.

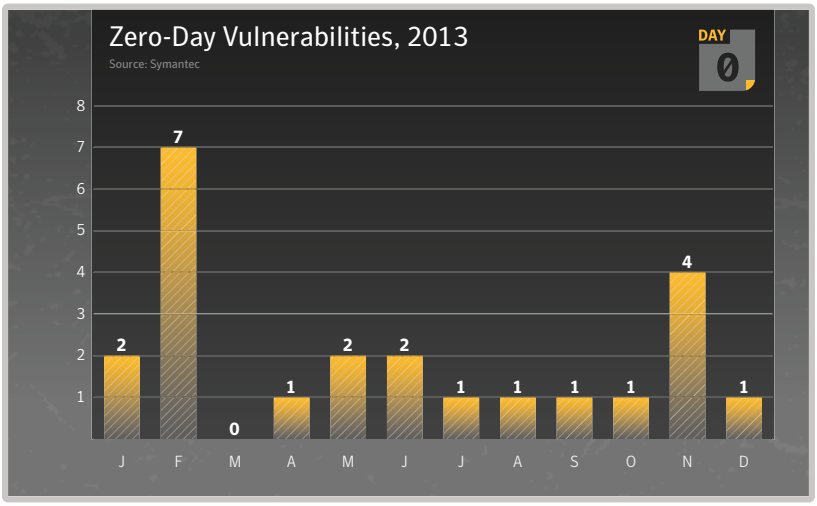


Fig. 11

- The total number of zero-day vulnerabilities reported in 2013 was 23, compared with 14 in 2012.
- The peak number reported in one month for 2013 was 7 (in February), compared with a monthly peak of 3 (June) in 2012.

to take advantage of the window of exploitation between disclosure, the patch release, and the time it takes organizations and individuals to patch their computers.

For the top 5 zero-day vulnerabilities disclosed in 2013, the top 3 accounted for 97 percent of all attacks against zero-day vulnerabilities in 2013. Moreover, for the top 5 zero-day vulnerabilities, the average time between publication and the requisite patch being made available by the vendor was approximately 4 days; however, there were a total of 19 days during which time no patch was available.

Bug bounties are also bringing more researchers out of the underground and allowing them to participate in the public dialog, where finders can get paid through discovery bounties rather than be tempted to sell them to malicious actors for use in attacks.

Vulnerabilities continue to be one of the core choices for the delivery of malicious code. Vulnerabilities are being exploited to serve up all sorts of threats, ranging from ransomware, Trojans, backdoors, and botnets.

Browser vulnerabilities have declined this year, where four of the top five browsers reported fewer vulnerabilities than they did in 2012. The exception is Internet Explorer, which saw an increase in reported vulnerabilities from 60 to 139. While Safari reported the most vulnerabilities in 2012, the Chrome browser came out on top in 2013, with 212 vulnerabilities.

Oracle's Java platform had the highest number of reported plug-in vulnerabilities. However, this may not point to an increased weakness

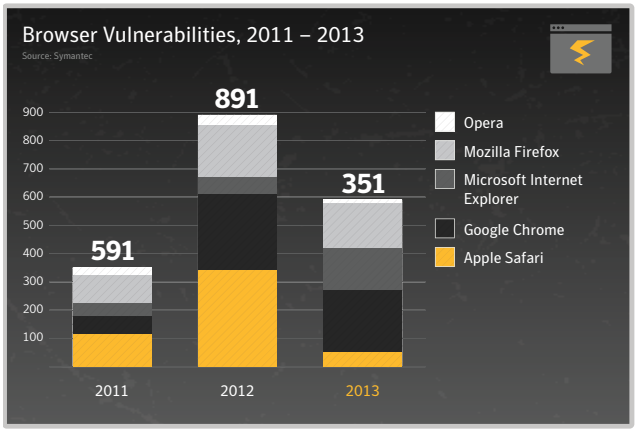


Fig. 12

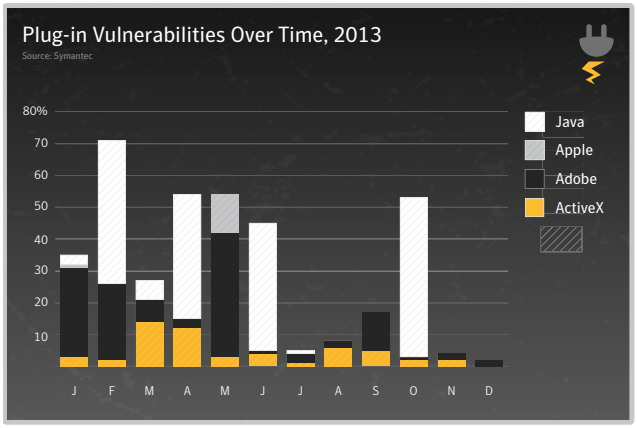


Fig. 13

- In 2013, 375 vulnerabilities affecting browser plug-ins were documented by Symantec, an increase compared to 312 vulnerabilities affecting browser plug-ins in 2012.
- ActiveX vulnerabilities decreased in 2013.
- Java vulnerabilities increased in 2013. This upward trend was already visible in 2012, and is also reflected in its usage in attack toolkits which have focused around Adobe Flash Player, Adobe PDF Reader and Java in 2013.
- Although the number of Java vulnerabilities was significantly higher in 2013, the number of new vulnerabilities being reported against the other plug-ins decreased throughout the year.
- Java is a cross-platform application, and as such any new vulnerability may potentially be exploited on a variety of different operating systems and browsers. This makes Java especially attractive to cyber-criminals and exploits against Java are likely to quickly find their way in the various webattack toolkits.

in the Java platform, but rather to the way in which Oracle has responded to Java security issues, increasing the release of security patches. Security improvements in other popular browser plug-ins have also contributed to this, with attackers continuing to exploit Java vulnerabilities where users have not upgraded to newer, more secure Java versions. Adobe added sandboxing technology to its products a few years ago, and has seen the benefits of such a strategy. Sandboxing executes code within a controlled environment, preventing an application for making programmatic calls outside its own environment. This has made it increasingly difficult to run malicious code within environments using the latest versions of the software. On top of that, Google has created mechanisms that actively test the Flash content being served up in search results to determine if exploits are being used on sites before showing it to users. This effectively limits the use of the platform as an easily-exploitable piece of the threat landscape.

EMAIL MALWARE

Windows executable files still dominate the realm of malicious email attachments, and Java attachments have grown in number. In fact, attackers have found these attachments so successful that they're no longer trying to mask them within web attack toolkits. In 2013, Symantec identified executable Java files being sent through email both as .jar and .class attachments because, assuming a Java runtime environment is installed, both file types are launched by double-clicking them. It's possible this shift could be based on a desire to get past attachment restrictions in large corporations where traditional executables are not allowed as attachments, or it could simply be taking advantage of the average user's lack of awareness of the threat.

Malware sent through email increased in 2013, where 1 in 196 emails contained a malicious attachment. This is up from 1 in 290.7 in 2012. December saw the largest ratio for the year, at 1 in 112.7, generally during a time of year when the virus rate is in decline.

APPLE MACS UNDER ATTACK

There has been an increase in Enterprise-level adoption of Macs as many organizations are allowing their work force to choose between PCs and Macs.

Although Macs still represent a small proportion of the overall operating system market, Macs could be considered more valuable if higher profile targets adopt the

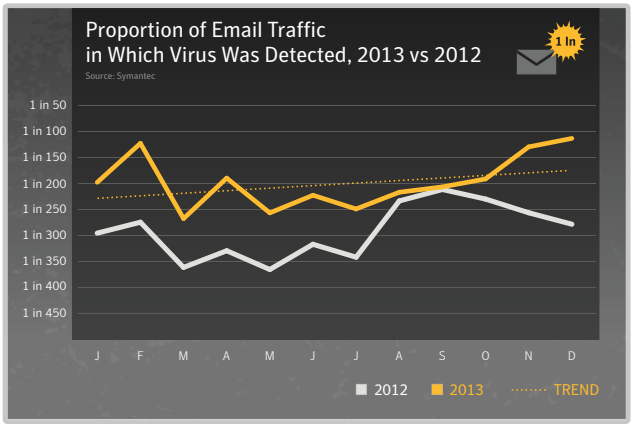


Fig. 14

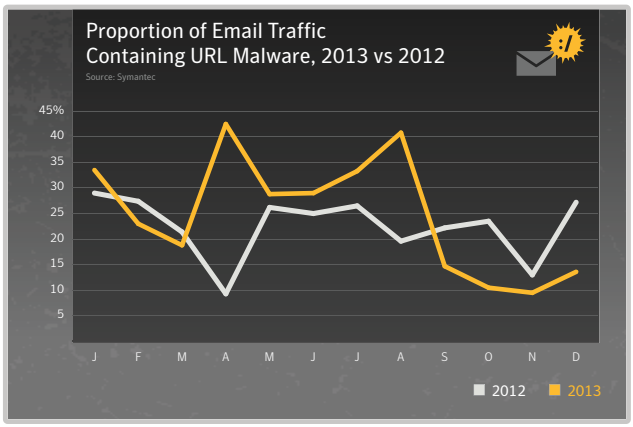


Fig. 15

- Overall email-based malware numbers increased in 2013, with 1 in 196 emails containing malware, compared with 1 1 in 50 in 291 in 2012.
- The proportion of email traffic that contains a malicious URL has increased in 2013 from 23 to 25 percent.
- There were two spikes in 2013 where more than 40 pecent of malicious emails contained URL links to malicious websites, rather than attachments, resulting in a higher rate for 2013 overall.

operating system for work purposes. Since the data available on these Macs may be considered more valuable, more resources are being turned towards attacking the Mac platform.

The challenge for Macs is similar to the challenges surrounding BYOD (bring your own device) initiatives within an organization. How do you manage the risk of another device type without compromising user performance? Unfortunately many Mac end users may still be under the impression that they are protected against malware attacks and don't require basic protection. As with any Internet-connected device that is used to access sensitive information, security countermeasures should always be included for Macs.

Ultimately, Macs are an accepted part of the IT fabric for an organization, and any strong security architecture plans must include them. As the demand for Macs in the Enterprise increases and they are used to access sensitive data, so too will the amount of Mac malware.

Top-10 Mac OSX Malware Blocked on OSX Endpoints, 2013

Source: Symantec

Malware Name	% of Mac Threats Detected on Macs
OSX.RSPlug.A	35.2%
OSX.Flashback.K	10.1%
OSX.Flashback	9.0%
OSX.HeIIRTS	5.9%
OSX.Crisis	3.3%
OSX.Keylogger	3.0%
OSX.MacControl	2.9%
OSX.FakeCodec	2.3%
OSX.Iservice.B	2.2%
OSX.Inqtana.A	2.1%

Fig. 16

- Approximately 1 in 924 (0.11 percent) of malware detected on Mac OSX endpoints was actually Mac-based malware. The remainder was mostly Windows based (i.e. Mac computers encountering Windows-based malware). This figure was 2.5 percent in 2012, largely due to the initial spread of the Flashback malware in 2012, which exploited a vulnerability in Java and reportedly affected as many as 600,000 Macs at the time.
- Flashback was first identified in 2012 and was still being detected on Macs in 2013.

SOCIAL MEDIA

Social media continued to work its way deeper into our digital lives in 2013. The importance of social media has also grown in the past year, and its cultural significance has been reflected in the financial markets' acceptance of mobile as an increasingly popular platform for global business. During 2013 a number of newer, niche platforms garnered enough users to make their way into popular consciousness, while more-established platforms realized the financial success that comes with IPOs. Popularity and profit appear to be central to the social media world this year.

Many of the recent entrants into social media have grown by narrowing their focus in comparison with better-established platforms, fulfilling an apparent desire for straightforward, simple-to-use social media apps, such as time-limited photos, short videos, micro blogging, or free alternatives to text messaging. The sites are often designed specifically for mobile use and the target audience is generally younger. It is these early adopters—the "cool kids" — who often start new trends, quickly bringing more users with them. These are the sort of users that scammers identify as their prime targets. Unfortunately, widespread popularity draws scammers to these social networking platforms, as per the saying, "If you build it, they will come." If a social network attains a certain level of popularity, scammers will find a way to exploit it. In 2012 the shift in spam and phishing towards social media was already underway, although these threats were harder to recognize than their email counterparts. Symantec identified new scams targeting some of these up-and-coming social networks during 2013.

The central goal of the scammer is profit. A lot of scam activity is carried out through traditional click-through campaigns that lead to survey scams, in contrast to the more complex setups found in other areas of the threat landscape. While they aren't making such large amounts of money as the hackers behind threats such as ransomware, a scammer in the world of social media can still make thousands of dollars in a month, thereby providing a regular income.

It is easy for a scammer to get started in this field because setting up social media accounts is largely free. A scammer can set up accounts on the sites, cultivate a group of followers, create and release free apps or browser plug-ins, and even host external pages on free sites. From there all the scammer has to do is figure out a topic that users might click on and then deploy the campaigns.

AT A GLANCE

- Fake offers lead the types of scams on social media again this year, accounting for 81 percent of scams identified in 2013.
- Click-through campaigns that lead to online surveys are a common tactic used by scammers.
- Mobile attackers are repackaging their threats more often, as the average number of variants per family is up in 2013.
- Tracking users is most common type of activity found in mobile threats.

Phishing and spam is evolving, moving further and further away from email and into the social media landscape. The campaigns include the same lures that are seen in phishing and spam email.

TECHNIQUES

Phishing and spam is evolving, moving further away from email and into the social media landscape. These social media campaigns include the same lures that are seen in phishing and spam email. The types of material being offered remains similar to past years: gift cards, electronics, concert tickets, and DVD

box sets are just a few of the fake offers seen this year. The fake profiles set up by scammers include pictures of attractive people looking to be friends and more. In other cases, a scam may center around posting a single photo or theme on a series of compromised accounts.

One example that came to light involved a login- and password-stealing scam that advertised a cool app for users to check out, or offered a download of a song from a favorite artist. If a user clicked on it, the scam asked the user to enter their social media credentials. They then stole this and redirected the user back to the social network without providing the promised app, download, or service.

In addition to stealing credentials, phishing sites encouraged victims to spam information about supposed phishing apps. This appeared to work well as a propagation technique for the scam, allowing it to spread from the original victim to their friends. These were often coupled with supposed incentives, like credits or points to be given to the users within the fake app.

For example, phishers offered a bogus app that claimed to deliver free cell phone minutes to social media users. The offer allegedly was available only if a user entered their login credentials and then forwarded it to at least ten friends. Thus, phishers aimed at multiplying the number of victims exponentially by blending their phishing attack with spam.

Social media scams are generally delivered through posts in the social network's feed, though if the service offers it they may also spread through private messages. Scammers

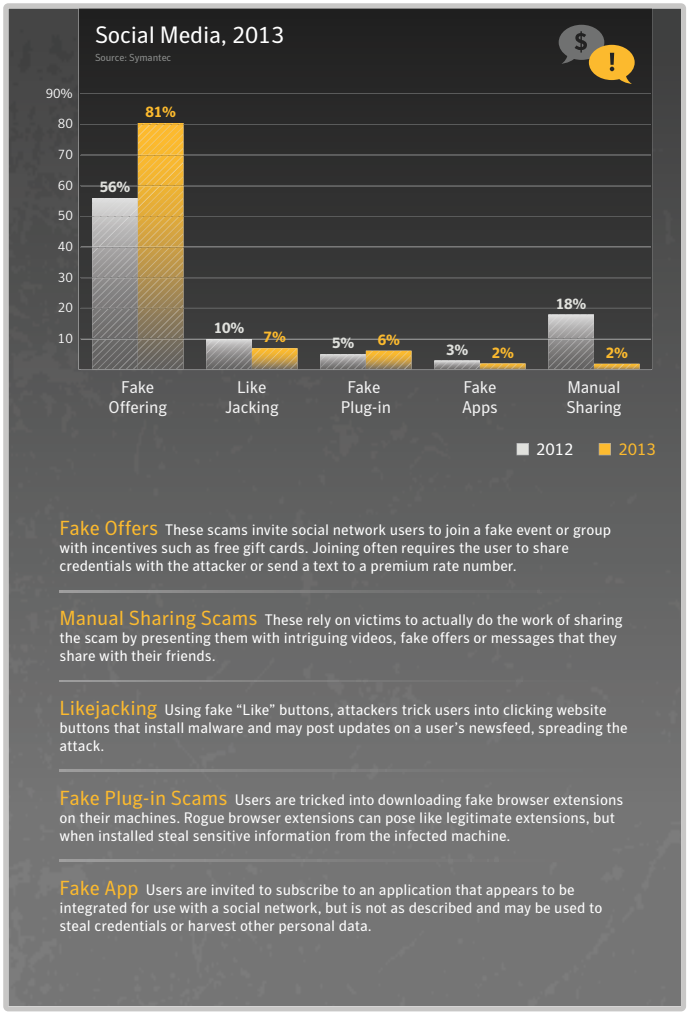


Fig. 1

A scam could be advertised as a cool app to check out, or offer a download of a song from a favorite artist. If a user clicks on it, the scam often asks the user to enter his or her social media login details.

- Fake Offers accounted for the largest number of social media based attacks in 2013, with 81 percent, compared with 56 percent in 2012.
- Manual sharing scams have also increased in 2013, from two percent in 2012 to 18 percent.
- Micro-blogging based scams accounted for one percent of total attacks detected for the social media category, for both 2012 and 2013.

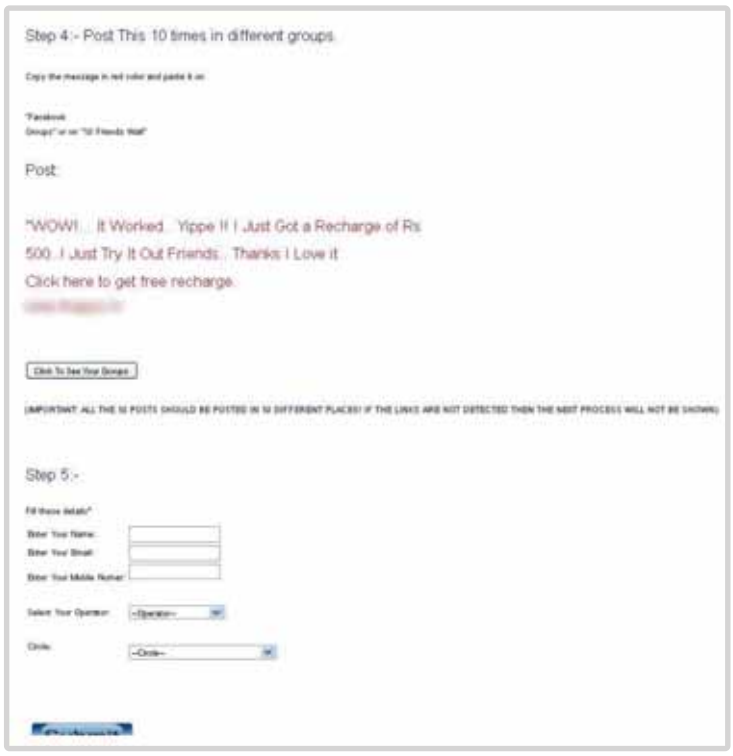


Fig. 2 Social media scam offering free cell phone minutes.

Fig. 3 Dating scam, where scammers send racy photos if the user agrees to install apps of their choosing.

don't limit their messages to the latest posts either, often replying to posts across the user's history sometimes months, if not years earlier. The messages generally linked to resources outside of the social network, such as compromised websites that the scam is being promoted upon.

Social media attackers were often seeking account credentials in the hope of using the account as a platform to spread their scams. A compromised profile allowed them to send messages to the victim's friends which appear to come from a reliable source. Another area of concern wasn't just a user's friends; it's who they chose to follow. Celebrities and other popular accounts or pages became prime targets of scammers who have hacked into their accounts. A simple word of caution in these cases: If the material posted seems contrary to the celebrity in question (e.g. A well-known academic hawking miracle diets) a user should not click any links presented.

Social media sites with a particular activity focus, like dating, also continued to be a location where scammers attempted to prey upon users. Fake users will often send messages to those genuinely attempting to meet a romantic partner. However, a common tell is that they generally come on quite strong. For instance, a scammer may send a user a message saying "Hey you're cute," hoping to strike up a conversation. The scammers send provocative photos, eventually followed by a link that leads to a webcam site. Only the site requires registration and the user is asked to hand over credit card information on this cam site. They may benefit from a few days of free access, but will eventually be charged at very high prices.

It's not just the specific social media sites to be concerned about. The growth in aggregate social media sites which allow users to quickly publish posts across multiple sites opened new avenues for attackers to take control of many points in a social profile at once. If these sites are hacked, as has already happened, they may not have gained direct access to users' various social media account details, but if they could send messages through the service it worked

Well-established markets, where phishers are able to sell such information on to other criminals, are in abundance. These markets provide an easier and less risky method to making money as they gather and sell personal details, in contrast to attempting to use the information directly.

just as well in helping them accomplish their mischievous goals.

Another lure we continued to see was enticing users to participate in scams by suggesting they could gain likes. For example, "Gain 100 followers by clicking this link and filling out a survey" or "Install this mobile app and gain 100 followers." In many cases, the app the user is directed to is legitimate, but the scammer made money from the download through affiliate programs. It's worth noting that the affiliate may not have been aware of the scam. In the end no followers or likes were given, but the scammer didn't care; they've achieved their objective.

In some cases, a scam did indeed increase followers. However, the followers may not have been the types of accounts that the user would have desired. The scammers generally had a large group of compromised or fake accounts which they used to like or follow the user's account. The InstLike app, that was removed from popular app marketplaces near the end of 2013, was one such example. The app allowed a user to purchase likes and followers and also requested the user's login details, which was then used to "auto-like" and "auto-follow" other InstLike users.[27]

This focus on identity theft increased in scams, though the underlying motive was still financially rooted, albeit more indirectly. Well-established markets where phishers were able to sell such information on to other criminals were in abundance. These markets provided an easier and less risky method to make money as they gathered and sold personal details, in contrast to having attempted to use the information directly.

This highlights why such scams were so popular and prevalent. The chief risk for a cybercriminal was capitalizing on their ill-gotten gains. This is often what exposed them to potential detection and capture. Selling information and details to others who have established networks for cashing out (i.e. money laundering) reduced the risk. This is why a credit card had a value on the black market that seemed lower than its potential value in real terms: The higher the value, the greater the risk.

In the overall threat landscape, social networking scammers were low on the food chain. Their margins were much less, but so was their risk. They made money by doing what they do in large volumes: spam run through compromised accounts, URL comment scams, fake profiles with the same details, along with other methodologies.

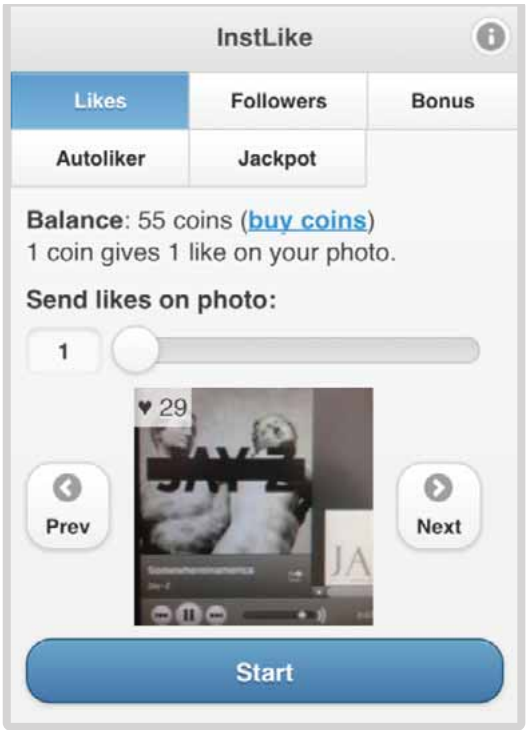


Fig. 4 The InstLike application

MOBILE

TRANSITION FROM DESKTOP

Mobile malware has been around for a number of years, and has multiplied with the widespread adoption of the Android platform. When Android gave smartphone users more freedom to install software from outside their official marketplace, it also opened the doors to malware authors, who have spent years honing their techniques. Much of the focus has been around stealing information from the device, although a variety of threats that have traditionally been found on desktop systems have begun to appear more regularly in the mobile landscape.

In the middle of 2013 remote access Trojan (RAT) toolkits began to appear for Android.[28] At first, attackers began to circulate Java-based RAT threats using email attachments, which were traced back to a toolkit designed to create threats that work across multiple platforms so long as a Java Runtime Machine is present.[29]

Fig. 5 Android.Fakedefender showing fake threats.

In 2012, Symantec's Norton Report showed that 44 percent of adults were unaware that security solutions existed for mobile devices, highlighting the lack of awareness of the mobile danger.

RAT toolkits began to be developed for the Android operating system shortly thereafter, such as in a threat called Android.Dandro.[30] This toolkit type, called a "binder," allowed an attacker to take a Trojan and package it with a legitimate app. The idea was simple; to take the Trojan and the legitimate app, put them together and attempt to get them onto as many mobile devices as possible while hoping users do not notice the extended permissions requested by the Trojanized app.

In 2012, Symantec's Norton Report[31] showed that 44 percent of adults were unaware that security solutions existed for mobile devices, highlighting the lack of awareness of the mobile danger. The 2013 Norton Report[32] showed this number rising to 57 percent. How did this awareness of security software decline? It seems that a lack of education among mobile users has contributed at least in part to this, or that people who had previously had feature phones (and therefore limited need for security software) were becoming smartphone users – but hadn't been made aware of the need to install a security app. The pool of people using mobile devices grew in 2013 as well, and many of these users were later adopters, who tend to be less digitally literate and less aware of the risks.

It appears that most mobile device users are just not aware of mobile threats, and as if to play into this lack of knowledge, rogue security software has been discovered on these devices; the first of which was identified in June. Android.Fakedefender did everything expected from fake security software: it ran a scan, warned the user of

non-existent threats that the software found on the device, then attempted to coerce the user into paying for the fake app in order to remove them.[33] Moreover, while desktop fake security software is annoying, it generally doesn't prevent someone from using the computer. Fakedefender[34] took it one stage further, preventing the user from using the device altogether. This is reminiscent of the ransomware frequently found on desktops, though it's difficult to determine whether this was truly intentional. The code behind Fakedefender was buggy and caused the device to crash. On the one hand, it might have been a trick to make the user think the phone was infected; on the other it may simply have been shoddy programing on the attacker's part. Regardless, it appears there may be more threats like this on the horizon, potentially having greater impact on mobile users as attackers improve them.

Phishing pages were also developed for mobile devices. These campaigns were hosted on standard websites, and simply designed in such a manner to lend themselves to mobile devices - smaller images, less text, and so on.

Mobile users are already very familiar with the idea of downloading applications (or apps) onto their smartphones for the convenience and added functionality they provide. Consequently, cybercriminals have sought new ways to hide their malicious code inside mobile apps and make them attractive to potential users; sometimes they will repackage malicious code within legitimate apps, or simply create new malicious apps that pretend to contain some

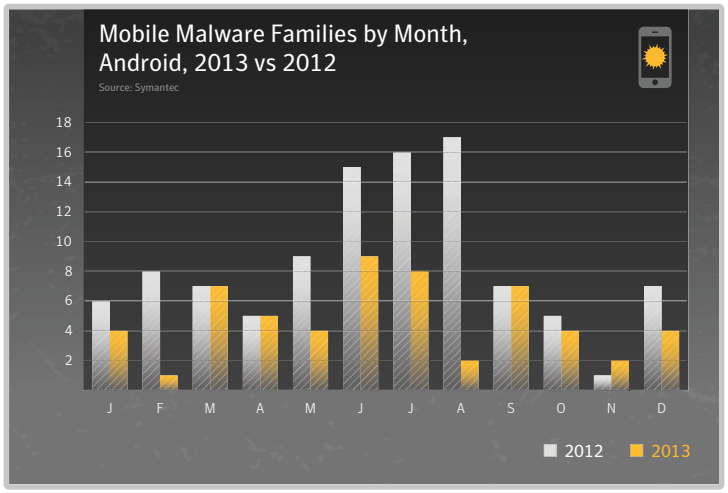


Fig. 6

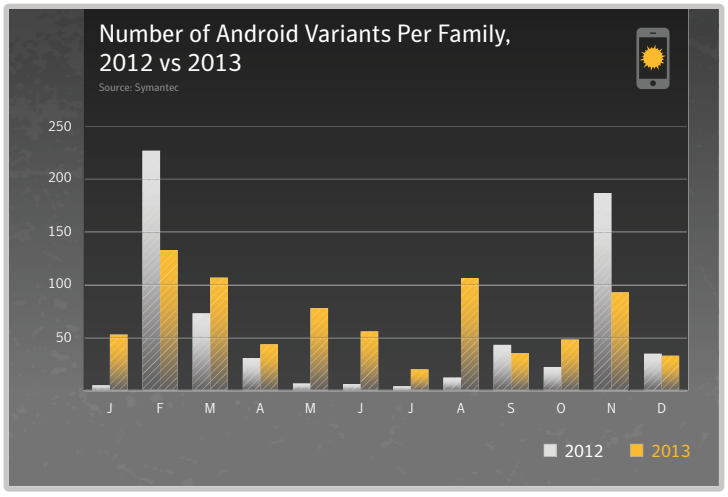


Fig. 7

- The average number of mobile malware families discovered per month in 2013 was 5, compared with 9 in 2012.
- June and July were the most active months in 2013, when 9 and 8 families were identified each month. The average number of variants within each family has increased since 2012.
- The average number of variants per family in 2012 was 1:38, increasing to 1:57 in 2013.
- March and June were the most active months for identifying new variants, with 748 and 504 variants being discovered, respectively. Fig. 7

The draw of mobile to attackers is clearly based on the size of the user base today. Yet it's also based on the amount of personal information that's easily attainable, once an attacker is on the device.

useful functionality while carefully masking their malicious purpose.

This highlights a key factor of the mobile landscape: App marketplaces are a quick way to get an application out to a large audience. Mobile users have become familiar with these marketplaces and the process of finding, downloading and installing new apps is a fast and painless process, whilst the cost is often small or even free. During the height of the desktop operating system's dominance, there was never such a simplified software marketplace quite like the app markets of today. In the past a developer would have to sign on with a software distributor, or would have to generate traffic to their own website for their customers to download applications.

This shift to app marketplaces was also helpful for cyber criminals. Attackers were likely to spend the time trawling through app marketplaces to find out what is popular, and then attempt to repackage malicious code with such apps. For instance, the release of an instant messaging application by a well-known smartphone vendor on the Android platform was greeted with much fanfare, and it quickly climbed to the top of the download charts. Attackers in turn took advantage of the popularity of the new app and released a variety of counterfeit versions bundled with adware. These apps were quickly removed from the Android marketplace, but not before accumulating a large number of downloads.

This trend appeared in our stats when we compared new mobile malware families to variants. The number of new families per month dropped from an average of 8.5 per month in 2012 to 4.8 in 2013.

In comparison, while a huge number of variants was discovered in February of 2012, the median number of variants discovered per month increased 25 percent in 2012, from 170.5 per month to 213.

Also of note in 2013 is that mobile malware seemed almost exclusively focused on the

Fig. 8

- The number of threats that track users has increased in 2013, from 15 to 30 percent, effectively doubling since 2012. This is perhaps an indication that this type of data is of more commercial value to the cybercriminals.
- In contrast, the largest type of mobile threat in 2012, those that steal information off the device, has actually decreased nine percentage points from 32 percent to 23 percent.

Fig. 9 A Japanese mobile spam message, used to spread Android.Exprespam.[35]

Fig. 10 A fake Russian app market, offering threats masked as popular apps.

Android platform. In fact only one new family was discovered outside this operating system—an information stealing Trojan for the Windows mobile platform.

REGIONAL LANDSCAPES

The type of attacks and the material attackers are pursuing often depends on the geographic region they're targeting. For example, there was a cluster of malicious mobile activity in Japan, which could be based on the presence of an advanced mobile infrastructure in the country. There are mobile services prevalent in Japan that are less common in other countries, as well as leading-edge, mobile-based purchasing methods.

One popular method for spreading malicious apps was through a mobile email account.[36] The emails provided a link and asked the user to download and install an app. If installed, information like contact details was gathered from the phone and the invitation messages were spammed out to other users in the recipient's address book. Similar attacks were carried out in South Korea as well, though these used SMS instead.

Another type of attack also surfaced this year in South Korea. A legitimate Korean app developer was compromised by attackers, which resulted in their app being replaced with a variant of Android.Fakeguard.[37] Users of the app were notified of an update to the app through normal means, and downloaded the revised, malicious code thinking it was a standard update. China is also another area where malicious versions of software are prevalent. However, this malicious activity has been driven due to a less robust version of official app marketplaces being available in the country. As a result, users have become inclined to install apps from unknown sources that have the functionality they desire,

putting themselves at risk in less-stringent marketplaces, where threats may not be identified as readily.

A similar problem was present in Russia, where the presence of counterfeit app marketplaces, designed to look like official ones, hosting malicious apps was commonplace. Many sites offered a variety of malware-laden apps, though in some cases they went a simpler route and created an app install page hosting only one app.

VULNERABILITIES

It still appears that the mobile threat landscape is under development. Attackers are researching what they can do on Android, and their attacks are becoming more sophisticated. For instance, we've seen threats like Android.Obad,[38] which used exploits to elevate its privileges, and then once installed, hid all traces of itself on the device.

The discovery of a vulnerability that allowed attackers to inject malicious code into apps without invalidating the digital signature is one example. This "Master Key" vulnerability allowed an attacker to modify apps to include malicious code, yet looked identical to legitimate apps in terms of their signature. In essence, the operating system had no way to tell the modified app from the original.

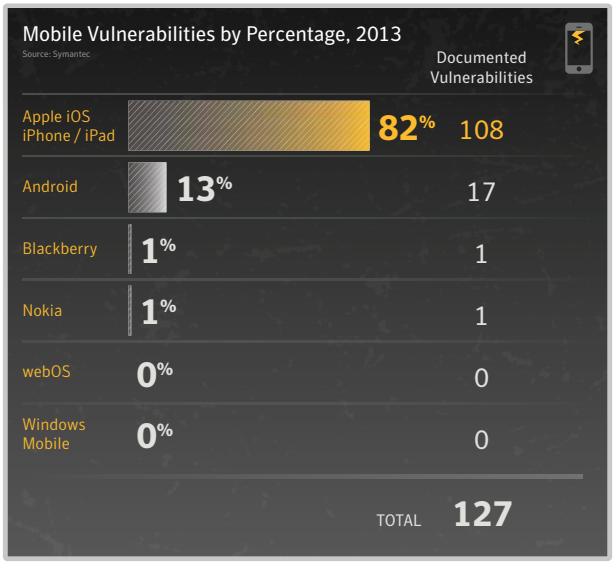


Fig. 11

- As we have seen in previous years, a high number of vulnerabilities for a mobile operating system does not necessarily lead to malware that exploits those vulnerabilities. Overall, there were 127 mobile vulnerabilities published in 2013, compared with 416 in 2012, a decrease of 69 percent.

Disclosed vulnerability numbers are lower in 2013 than the previous year, down almost 68 percent. September saw the largest number of disclosed vulnerabilities. This increase coincided with the release of Apple's iOS7, which included a number of patches for vulnerabilities discovered in iOS6. Similarly, the Android platform saw the release of version 4.3 in July and 4.4 in November.

MOBILE ADWARE ("MADWARE")

There's another risk to the mobile landscape that grew in 2013. Advertising is a core part of the free app business model; however, some developers aren't content with keeping their advertisements held within the bounds of their application. Some developers have taken to displaying ads in the notification bar, or suggest the user install other apps. This type of risk is called mobile adware – or "madware."

The problem is that madware is common on app stores and appears to be growing. In October of 2013, 65 ad libraries were identified.[39] This number increased to 88 ad libraries by the end of 2013. That's not to say the market owners aren't quick to pull apps that exhibit some of the more aggressive madware traits. However, an app like this can rack up a modest number of installs before it's discovered and removed.

HYBRID THREATS

Another new development we've seen is malware threats and campaigns targeted at both Android and Windows. In the case of the Android.Stels Trojan,[40] which was distributed via a malicious email campaign, the payload varied depending on the device type. If the malicious URL in the email was opened on a PC,

then a PC version of the malware was installed. If it was opened on a mobile device, a mobile version was served up. Other threats contained payloads for both device types in one package. If an Android device was connected to a compromised PC, it spread to the device.[41]

MOTIVATIONS

The attraction of the mobile environment to attackers is clearly based on the size and growth rate of the user base today. Yet it's also based on the amount of personal information that's easily attainable once an attacker is on the device. With the right permissions the device's phone number, GPS coordinates, camera, and other information become readily available.

Access to various features and data on a device is the key here. Mobile devices offer attackers a much wider attack surface: Cameras, near field communication (NFC), GPS and other location services, Bluetooth, and wireless are all common features present in most smartphones. All apps have to ask for access permissions to access these features on the device. Fortunately mobile operating systems are usually quite verbose in detailing which permissions are requested when installing an app. Still, most users don't examine these permissions carefully, opting to just accept the request rather than reading through the details, in much the same way many users approach EULAs. Given this behavior, malicious app developers find it simple to persuade users that they should grant unnecessary permissions to a malicious app.

The attraction of the mobile environment to attackers is clearly based on the size and growth rate of the user base today. Yet it's also based on the amount of personal information that's easily attainable once an attacker is on the device.

Fig. 12 Example madware pop-up advertisement.

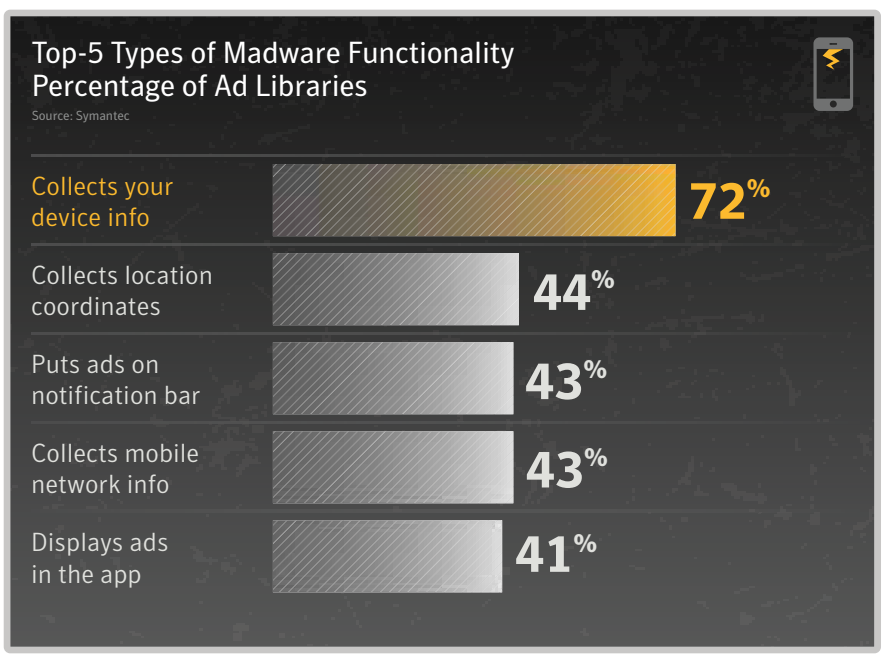


Fig. 13

SPAM AND PHISHING

AT A GLANCE

- The phishing rate has increased in 2013, from 1 in 414 for 2012 to 1 in 392 in 2013.
- Login credentials for various accounts are the primary type of information sought by phishers.
- Spam rates are down 3 percentage points in 2013, making up 66 percent of email traffic.
- Scammers are working to compromise websites in order to help spread their scams.

In the mid-to-late 2000s, most phishing attempts were carried out through email for financial gain. Over time, phishing attacks have expanded in the scope of their targets from not only banks, credit unions and other financial institutions, to a variety of other organizations. The social engineering involved has also grown more sophisticated in recent years and recent examples include phishing for online accounts of customers of domestic energy companies and loyalty card programs. More energy utility companies are encouraging their customers to move to paperless billing, enabling an attacker to retrieve utility bills. They can potentially use these bills in the money laundering process such as in creating a bank account in someone else's name and using the online bill as proof of identity.

The phishing rate for the year has increased, from 1 in 414.3 emails per day, to 1 in 392.4. The busiest month of the year was February, where the rate rose to 1 in 193.0 emails. Many of these phishing attempts consist of fake login pages for popular social networks. In addition to just spoofing login pages of legitimate sites, phishers began introducing baits relevant to current events to add flavor to the phishing pages. Celebrity promotions, popular community pages, social networking applications, and other related material were introduced into phishing sites as bait.

Phishers also began exploring new up-and-coming social networks. During the past five years, the number of social media sites that phishers have used in their attempts to gather sensitive information has increased to roughly three times its earlier figure.

Social networking is bringing down the overall impact of email phishing attempts as scammers post their messages and campaigns through social media instead. For instance, in October 2013 Symantec noted one such phishing campaign being propagated using social media messages. This phishing attack in particular used URLs with the .pw top-level domain (TLD), a TLD frequently utilized by

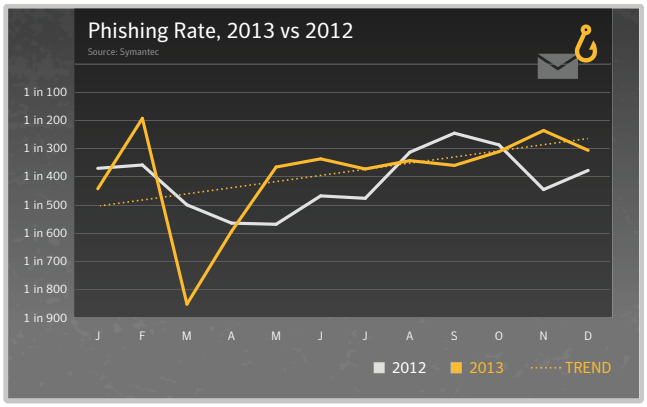


Fig. 1

- The global average phishing rate has increased from 2012 from 1 in 414 to 1 in 392.

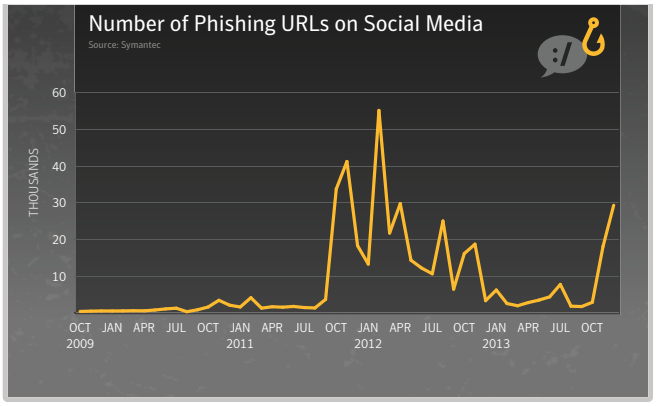


Fig. 2

- This chart represents number of URLs detected on social media websites per month.

scammers in 2013. The number of phishing URLs originating from social media sources increased six-fold in November 2013 as compared to the previous month. Out of these links, 84 percent of URLs had the .pw TLD.

That's not to say that attackers have abandoned email for spam and phishing attempts; these still make up a large percentage of email traffic. Spammers still hawk their wares and phishers still try to steal information.

Login credentials for accounts seem to be the main information phishers are looking for. Email campaigns often include socially-engineered text and links to web pages that are designed to impersonate popular social networking sites, while others may look almost identical to a bank's website. The email text might hint at a problem with a user's account or a special limited-time offer, the goal being to convince users that the web page is legitimate so that they will enter their credentials. Once entered, compromised social media accounts can be used to spread phishing and spam campaigns, or banking information can be used to access an individual's finances. In total, the 2013 Norton Report demonstrated that 12 percent of those surveyed said that someone has hacked their social media account.[42]

Social networking is bringing down the overall impact of email phishing attempts as scammers post their messages and campaigns through social media instead.

Phishers also continued to spoof webmail accounts during 2013. One popular attack method played off the idea that a mailbox has exceeded its quota. A victim is directed to a site where they are asked to "confirm" email, user name and password. However, no further information is provided about the quota issue and the account is compromised, leaving it open to be used to send spam.

One of the latest findings from analysis of phishing activity in 2013 was the emergence of campaigns targeting information not usually associated with more traditional phishing activities. These include attempts to steal frequent flyer and loyalty card accounts, online credentials for utility accounts, and cloud-based storage account details. More concerning perhaps was that some of these may be used in identity fraud. For instance, a utility bill is often a requirement as a proof of address. Many people today use paperless billing, so if phishers gained access to a utility account they could have feasibly changed the

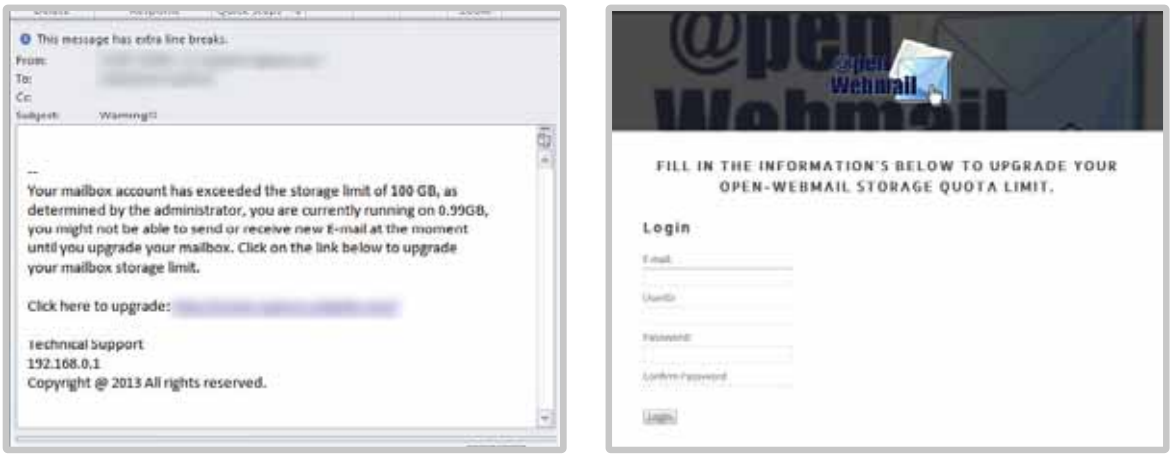


Fig. 3 Example quota phishing email and website.

account address and used it to fraudulently obtain goods and services in the victim's name.

In other cases, scammers preyed upon people's dreams of living in another country. Someone looking to travel or emigrate, particularly to countries with tight visa restrictions may have been willing to reveal sensitive information if they thought that it would help them to gain entry to the country in question.

With all the new phishing scams, the more traditional financial phishing has not declined. There were a number of new angles that became popular in 2013. Bitcoin wallet account details, tax information, welfare and benefit details, and payday loan accounts were all examples of campaigns targeting a victim's finances.

In terms of spam campaign strategies, some were quite blatant, clearly selling pills, whilst in other cases the message entirely unrelated topics - such as subject lines referencing replica watches, while the email body linked to pornographic sites.

The overall spam rate appeared to be down by 3 percentage points for the year, from 69 percent in 2012 to 66 percent in 2013. There was a period of time during 2013 where the spam rate did surpass rates for similar time periods during 2012. For approximately six months of the year, the global spam rate

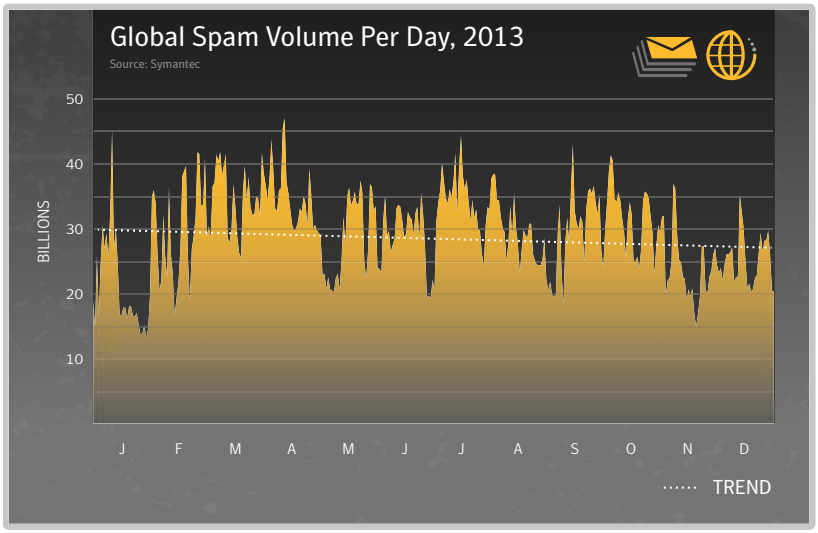


Fig. 4

- The estimated projection of global spam volumes for spam in business email traffic decreased marginally by 3 percent, from 30 billion spam emails per day in 2012, to 29 billion in 2013.
- Spam volumes were highest in March and April, with approximately 34.3 billion and 35.3 billion spam emails per day.

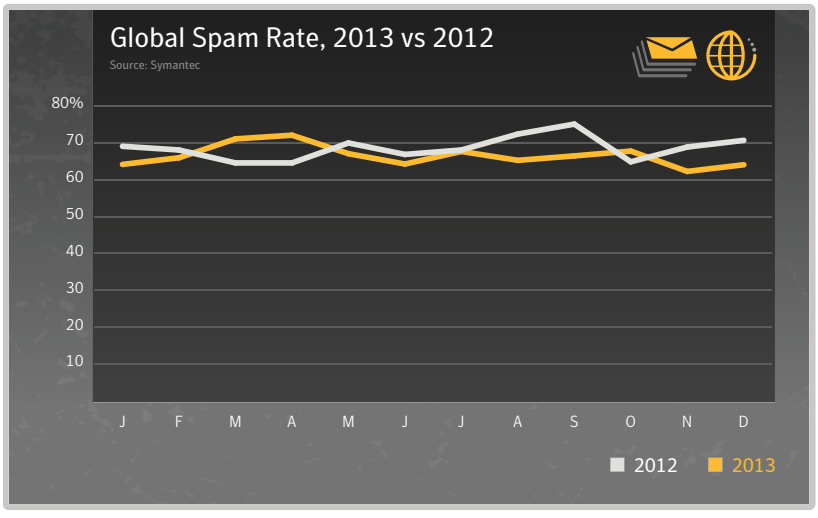


Fig. 5

- The global average spam rate for 2013 was 66 percent, compared with 69 percent in 2012; a decrease of 3 percentage points.
- Pharmaceutical spam accounts for 18 percent of all spam, but the Adult/ Dating category accounts for approximately 70 percent of spam. Pharmaceutical spam in 2013 declined by approximately 3 percentage points compared with 2012.
- Adult/Dating spam in 2013 increased by approximately 15 percentage points compared with 2012.

exceeded the equivalent rate for the same month in the previous year, despite the fact that the annual average was actually lower.

Lots of spam and phishing attacks use URL shortening, a method where a longer URL is shortened to save space, but still resolves to the original page. However, the use of shortened URLs also masks the original URL, allowing attackers to hide malicious links behind them. This technique was still popular and for much of 2013 its use remained fairly stable.

The use of shortened URLs also masks the original URL, allowing attackers to hide malicious links behind them. This technique was still popular and for much of 2013 its use remained fairly stable.

COMPROMISED SITES

Many ordinary users and small businesses are comfortable managing their own web servers, whether internally or externally hosted, since it's now easier to do and relatively inexpensive. However, while the ease of installation and cost of maintenance may have decreased, many new administrators are perhaps not familiar with how to secure their servers against attacks from the latest web attack toolkits. Nor are they diligent about keeping their sites secure and patched with the latest software updates. Updating popular applications such as content management systems or blogging software on the web server is a necessity. These services have become major targets for abuse by hackers, and a single vulnerability may be used across thousands of sites.

Scammers are also attacking web hosting sites that provide hosting platforms as a service. If an attacker can figure out a way to successfully breach a company that provides such services, they can gain access to multiple sites hosted by the compromised company. It's possible for thousands of sites to be impacted in such breaches. Hackers can also use popular search engines to quickly discover potentially vulnerable websites that they may be able to compromise. In this way, a website may be easily hijacked if any software vulnerabilities can be exploited by the attackers.

Beyond hijacking websites in order to spread spam, scammers continue to attack Autonomous Systems (ASes) using the Border Gateway Protocol (BGP), as first discussed in last year's ISTR. In these situations, attackers hijack entire blocks or ranges of IP addresses that may belong to a business and re-route them to a new destination URL of their choosing. The spammers then use those IP addresses to send spam for a brief period, where the spam appears to come from the legitimate business. This topic is covered in detail in Appendix C of this report, New Spam Tread: BGP Hijacking.

• *For more information on spam and phishing trends, see the Spam and Phishing appendix.*

LOOKING AHEAD

PRIVACY AND TRUST

Many factors helped to shape the threat landscape during 2013, and some will have an enduring impact by altering our thinking about how we behave and conduct ourselves online. For some, the attitude regarding online privacy may be a factor of our age and perhaps to some extent how long we have been online; however, the general attitudes regarding online trust and privacy changed more during 2013 than in any other time.

In one sense, anything published online may be there forever; our proudest moments may sit alongside our most embarrassing mistakes. It is when the personal information we casually share falls into what we call "the wrong hands" that we are most concerned. We are increasingly sharing more data about ourselves that we may not even think about; for example, if it will lower our insurance premiums, we are willing to share GPS tracking information with an insurance provider to prove that we don't drive recklessly. So much of what we do is online and linked across many different environments, social media applications, and devices. What we do in one area is quickly shared with another.

One of the key drivers for the adoption of cloud-based technology has been the widespread use of social media; social networking sites, applications and mobile apps all use the cloud. Without Internet access, a smartphone is just a phone. Widespread cloud adoption has essentially enabled rapid growth to occur on an enormous scale, and as a result of some of the headlines in 2013 some people are already asking questions: "Do we still trust the cloud?" "Who should we trust to look after our personal data?" We have seen limited impact, but it remains to be seen whether this will influence the social media and mobile app revolution in any meaningful way over the coming months. In 2014 and beyond we can expect social networking organizations and other online service providers to seek to win back the hearts and minds of their users by making online privacy and data security core to their offerings. The worst case scenario is that people will become even more lackadaisical about online privacy to the detriment of their own personal security.

The adoption of encryption technology is expected to grow in 2014 and beyond, not only for securing data on personal devices but for online transactions including emails. The use of personal VPNs is also likely to increase as concerned users become wary about the traffic that may be exposed through their Wi-Fi hotspot, or simply to prevent their ISP from being able to track their activity. More up-to-date, faster encryption protocols will be in demand to secure these devices, so even if data is exposed or a device falls into the wrong hands, users can be assured that it cannot be exploited by the criminals.

TARGETED ATTACKS AND DATA BREACHES

The huge scale of breaches dominated the headlines during 2013, and has forced both businesses and home users to seriously consider how they secure their confidential information to keep it both private and secure. The sheer number of data breaches and even larger volume of identities being leaked was alarming, and the majority of these were caused by hacking. As the pressure mounts not to become the next victim, businesses are looking more towards trusted security vendors as a one-stop solution provider to take care of all their data protection needs. Not only will the focus be on safeguarding against an attack by hardening the perimeter, but also

on minimizing the potential impact of any breach should one occur. The wider adoption of encryption technology will be at the core of securing personal data, intellectual property, and company secrets. It has often been considered difficult to implement a robust and comprehensive encryption policy within an organization, hence the growing demand for such technology to become a seamless part of the underlying infrastructure rather than an add-on only used by a few.

As more personal information is stored in the cloud and accessible online, we routinely share more data with each other. Businesses and governments need to routinely handle massive quantities of personal information securely. Important questions are now being asked by the owners of this data, such as whether the caretakers are taking sufficient protective measures to safeguard it, irrespective of whether information is on their own computers and devices or in the cloud?

E-CRIME AND MALWARE DELIVERY

In the short term, e-crime will continue to grow. This will lead to greater cooperation between law enforcement and industry, and make it increasingly difficult for cybercriminals to operate. Rather than disappearing, e-crime is likely to move towards a new, more professional business model.

At the end of 2013 there are still many users on Windows XP using older, more vulnerable web browsers and plug-ins; in many ways this combination can be the Achilles heel of security. Microsoft is sun-setting their support for Windows XP in 2014 and it will be interesting to see how this affects people's attitudes towards online security. On the one hand, those that continue to use the retired operating system will no longer get patches directly from Microsoft. On the other, it may precipitate a large move to newer and more secure operating systems.

The next two or three years may bear witness to a divergence in the threat landscape; as people move to newer, more secure operating systems and modern web browsers, it will naturally become more easy to avoid falling victim to a casual malware attack. The success or failure of these attacks will be increasingly determined by the level of social engineering involved, which in turn may drastically affect the overall shape of the online security landscape.

Finally, as the "Internet of Things" becomes more an everyday reality, items like TVs, telephones, security cameras, and baby monitors as well as wearable technology and even motor cars will become woven into the fabric of the Internet. This in turn increases the attack surface, presenting new opportunities for researchers and attackers alike. The Internet of Things could soon become the next battleground in the threat landscape.

SOCIAL MEDIA AND MOBILE

So much of what we now do in our daily lives is being tracked and recorded online. The public has a seemingly insatiable appetite for personal lifestyle apps that help do things better than before and help achieve our goals faster than we could imagine. This may open more avenues for cybercriminals to exploit and allow them to take advantage of potential victims. While there may still be a number of activities in our lives that aren't currently shared online, this is likely to diminish in the near future. Wearable technology such as interactive wristwatches and other accessories will make interacting with these apps less like being online and simply a part of everyday life. Users who are less aware of the potential risks and dangers may soon find themselves victims. The importance of online security education

and awareness-raising for these users will be greater than ever.

In the future, expect more traditional malware threats being "ported" to mobile devices. Fake security software has already appeared in this environment, and ransomware could soon be developed for the mobile platform too, given how lucrative it has proved on desktop and laptop computers. The latest mobile devices also contain a large number of entry points, including Wi-Fi, Bluetooth, and near field communication (NFC), as well as USB. There may be plenty of opportunities to compromise these devices through new methods not fully explored at this stage. So far, mobile threats are still mainly aimed at consumers rather than enterprises. Only a few cases have been discovered where a mobile threat has targeted corporate users. Targeted attacks can be expected to take advantage of the mobile landscape in the near future, especially since the potential for surveillance or counter surveillance measures are even higher on devices that include in-built cameras and microphones that may be switched on and off with ease.

BEST PRACTICE GUIDELINES FOR BUSINESSES

01

EMPLOY DEFENSE-IN-DEPTH STRATEGIES

Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls as well as gateway antivirus, intrusion detection or protection systems (IPS), website vulnerability with malware protection, and web security gateway solutions throughout the network.

02

MONITOR FOR NETWORK INCURSION ATTEMPTS, VULNERABILITIES, AND BRAND ABUSE

Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious website reporting.

03

ANTIVIRUS ON ENDPOINTS IS NOT ENOUGH

On endpoints, it is important to have the latest versions of antivirus software installed. Deploy and use a comprehensive endpoint security product that includes additional layers of protection including:

- Endpoint intrusion prevention that protects unpatched vulnerabilities from being exploited, protects against social engineering attacks, and stops malware from reaching endpoints;
- Browser protection for avoiding obfuscated web-based attacks;
- File and web-based reputation solutions that provide a riskand- reputation rating of any application and website to prevent rapidly mutating and polymorphic malware;
- Behavioral prevention capabilities that look at the behavior of applications and prevent malware;
- Application control settings that can prevent applications and browser plug-ins from downloading unauthorized malicious content;
- Device control settings that prevent and limit the types of USB devices to be used.

04

SECURE YOUR WEBSITES AGAINST MITM ATTACKS AND MALWARE INFECTION

Avoid compromising your trusted relationship with your customers by:

- Implementing Always On SSL (SSL protection on your website from logon to logoff);
- Scanning your website daily for malware;

- Setting the secure flag for all session cookies;
- Regularly assessing your website for any vulnerabilities (in 2013 1 in 8 websites scanned by Symantec was found to have vulnerabilities);
- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users;
- Displaying recognized trust marks in highly visible locations on your website to show customers your commitment to their security.

05

PROTECT YOUR PRIVATE KEYS

Make sure to get your digital certificates from an established, trustworthy certificate authority that demonstrates excellent security practices. Symantec recommends that organizations:

- Use separate Test Signing and Release Signing infrastructures;
- Secure keys in secure, tamper-proof, cryptographic hardware devices;
- Implement physical security to protect your assets from theft.

06

USE ENCRYPTION TO PROTECT SENSITIVE DATA

Implement and enforce a security policy whereby any sensitive data is encrypted. Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution. Ensure that customer data is encrypted as well. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization. Use Data Loss Prevention to help prevent data breaches: Implement a DLP solution that can discover where sensitive data resides, monitor its use, and protect it from loss. Data loss prevention should be implemented to monitor the flow of information as it leaves the organization over the network, and monitor traffic to external devices or websites.

- DLP should be configured to identify and block suspicious copying or downloading of sensitive data;
- DLP should also be used to identify confidential or sensitive data assets on network file systems and computers.

07

ENSURE ALL DEVICES ALLOWED ON COMPANY NETWORKS HAVE ADEQUATE SECURITY PROTECTIONS

If a bring your own device (BYOD) policy is in place, ensure a minimal security profile is established for any devices that are allowed access to the network.

08

IMPLEMENT A REMOVABLE MEDIA POLICY

Where practical, restrict unauthorized devices such as external portable hard-drives and other removable media. Such devices can both introduce malware and facilitate intellectual property breaches, whether intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

09

BE AGGRESSIVE IN YOUR UPDATING AND PATCHING

Update, patch, and migrate from outdated and insecure browsers, applications, and browser plug-ins. Keep virus and intrusion prevention definitions at the latest available versions using vendors' automatic update mechanisms. Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

10

ENFORCE AN EFFECTIVE PASSWORD POLICY

Ensure passwords are strong; at least 8-10 characters long and include a mixture of letters

and numbers. Encourage users to avoid re-using the same passwords on multiple websites and sharing of passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days.

11
ENSURE REGULAR BACKUPS ARE AVAILABLE

Create and maintain regular backups of critical systems, as well as endpoints. In the event of a security or data emergency, backups should be easily accessible to minimize downtime of services and employee productivity.

12
RESTRICT EMAIL ATTACHMENTS

Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments. Ensure that mail servers are adequately protected by security software and that email is thoroughly scanned.

13
ENSURE THAT YOU HAVE INFECTION AND INCIDENT RESPONSE PROCEDURES IN PLACE

- Keep your security vendor contact information handy, know who you will call, and what steps you will take if you have one or more infected systems;
- Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss;
- Make use of post-infection detection capabilities from web gateway, endpoint security solutions and firewalls to identify infected systems;
- Isolate infected computers to prevent the risk of further infection within the organization, and restore using trusted backup media;
- If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied.

14
EDUCATE USERS ON BASIC SECURITY PROTOCOLS

- Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless the download has been scanned for viruses;
- Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;
- Deploy web browser URL reputation plug-in solutions that display the reputation of websites from searches;
- Only download software (if allowed) from corporate shares or directly from the vendor website;
- If Windows users see a warning indicating that they are "infected" after clicking on a URL or using a search engine (fake antivirus infections), educate users to close or quit the browser using Alt-F4, CTRL+W or the task manager.

BEST PRACTICE GUIDELINES FOR CONSUMERS

01
PROTECT YOURSELF

Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:

- Antivirus (file- and heuristic-based) and behavioral malware prevention can prevent unknown malicious threats from executing;
- Bi-directional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer;
- Browser protection to protect against obfuscated web-based attacks;

- Use reputation-based tools that check the reputation and trust of a file and website before downloading, and that check URL reputations and provide safety ratings for websites found through search engines;
- Consider options for implementing cross-platform parental controls, such as Norton Online Family.[43]

02
UPDATE REGULARLY
Keep your system, program, and virus definitions up-to-date – always accept updates requested by the vendor. Running out-of-date versions can put you at risk from being exploited by web-based attacks. Only download updates from vendor sites directly. Select automatic updates wherever possible.

03
BE WARY OF SCAREWARE TACTICS
Versions of software that claim to be free, cracked or pirated can expose you to malware, or social engineering attacks that attempt to trick you into thinking your computer is infected and getting you to pay money to have it removed.

04
USE AN EFFECTIVE PASSWORD POLICY
Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary. Do not use the same password for multiple applications or websites. Use complex passwords (upper/lowercase and punctuation) or passphrases.

05
THINK BEFORE YOU CLICK Never view, open, or copy email attachments to your desktop or execute any email attachment unless you expect it and trust the sender. Even when receiving email attachments from trusted users, be suspicious.

- Be cautious when clicking on URLs in emails or social media communications, even when coming from trusted sources and friends. Do not blindly click on shortened URLs without expanding them first using a preview tool or plug-in.
- Use a web browser plug-in or URL reputation site that shows the reputation and safety rating of websites before visiting. Be suspicious of search engine results; only click through to trusted sources when conducting searches, especially on topics that are hot in the media.
- Be suspicious of warnings that pop up asking you to install media players, document viewers and security updates. Only download software directly from the vendor's website.
- Be aware of files you make available for sharing on public sites, including gaming, bitTorrent, and any other peer-to-peer (P2P) exchanges. Keep Dropbox, Evernote, and other usages to a minimum for pertinent information only.

06
GUARD YOUR PERSONAL DATA
Limit the amount of personal information you make publicly available on the Internet (in particular via social networks). This includes personal and financial information, such as bank logins or birth dates.

- • Review your bank, credit card, and credit information frequently for irregular activity. Avoid banking or shopping online from public computers (such as libraries, Internet cafes, and similar establishments) or from unencrypted Wi-Fi connections.
- Use HTTPS when connecting via Wi-Fi networks to your email, social media and sharing websites. Check the settings and preferences of the applications and websites you are using.
- Look for the green browser address bar, HTTPS, and recognizable trust marks when you visit websites where you log in or share any personal information.
- Configure your home Wi-Fi network for strong authentication and always require a unique password for access to it.

SANS CRITICAL SECURITY CONTROLS:

HOW TO PROTECT YOUR ORGANIZATION FROM CYBER ATTACK

INTRODUCTION

The goal of the annual Symantec Internet Security Threat Report (ISTR) is not only to raise awareness of cyber threats and educate business users and consumers about the changing nature of the cyber security threat landscape, but also to provide guidance and advice about how to secure your critical assets, including your personal data to help reduce the impact of any potentially harmful incidents.

There are a number of good best practice guidelines that, if followed, can help to reduce the risk from cyber threats – many of these have been outlined in this report. However, for businesses and organizations especially, the implementation of a more methodological approach to hardening their security profile can bring additional benefits as well. There are a variety of frameworks that can help, and each one may suit different organizations in different ways. Generally a standard framework will need to be continually maintained, and adapted to new threats and challenges. Moreover, your business will benefit from the wealth of experience and lessons learned by other organizations that are also using these standards and frameworks, and building on them in turn. This approach will help you to prioritize the areas that you need to focus on first, and also to harden your existing defenses and develop the right security posture to help prevent the most common and potentially most harmful types of attack from damaging your business.

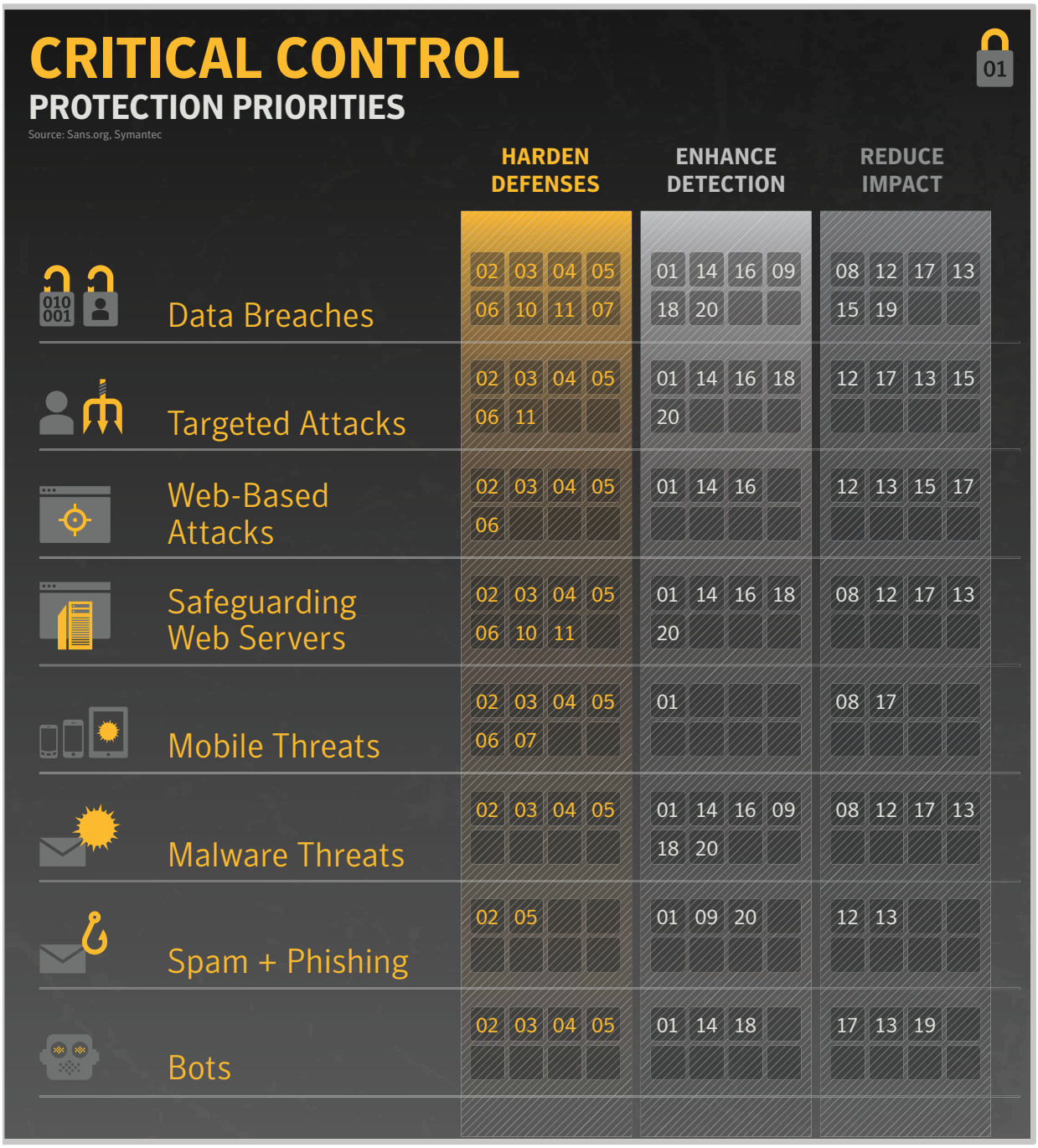
In the United States, the National Institute of Standards and Technology (NIST) recently published the "Framework for Improving Critical Infrastructure Cybersecurity," and Symantec has played a central role in shaping it. The NIST framework is not designed to be a standard or set of controls, nor is it a checklist; instead, it is a tool to help organizations assess and improve their cybersecurity programs, or to help develop such a program if they don't already have one in place. Symantec also works with the SANS Institute44, one of the largest sources for information security training and certification, which operates the SANS Top 20 Critical Security Controls. The SANS CSC is comprised of a detailed list of controls that any organization can implement and adapt quickly, and each one is specifically designed to address particular areas of concern. For more information on the SANS CSC, please visit www.sans.org/critical-security-controls/guidelines. Additional details about the new NIST framework can also be found here: www.nist.gov/cyberframework.

HOW TO APPLY THE SANS CRITICAL SECURITY CONTROLS

In order to apply the controls effectively, it's not always necessary to try to implement everything at once. By identifying some "quick wins," you should be able to quickly implement the relevant controls that will have the greatest impact and reduce the exposure of your organization to the greatest threats more quickly.

For example, in order to tighten the controls that will help reduce the likelihood of a website being breached; you may wish to consider the following controls: 3, 4 and 5 to begin with and then 6 and 11 when that is fully operational. Additional controls may then be introduced later, once you have the basics in place and operating effectively.

Following is a list of potential controls that could be implemented to safeguard against some of the most important types of threats discussed in the Symantec ISTR.



01

INVENTORY OF AUTHORIZED AND UNAUTHORIZED DEVICES

Reduce the ability of attackers to find and exploit unauthorized and unprotected systems: Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.

02

INVENTORY OF AUTHORIZED AND UNAUTHORIZED SOFTWARE

Identify vulnerable or malicious software to mitigate or root out attacks: Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.

03
SECURE CONFIGURATIONS FOR HARDWARE & SOFTWARE ON LAPTOPS, WORKSTATIONS, AND SERVERS
Prevent attackers from exploiting services and settings that allow easy access through networks and browsers: Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.

04
CONTINUOUS VULNERABILITY ASSESSMENT AND REMEDIATION
Proactively identify and repair software vulnerabilities reported by security researchers or vendors: Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.

05
MALWARE DEFENSE
Block malicious code from tampering with system settings or content, capturing sensitive data, or from spreading: Use automated antivirus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using autorun programs to access removable media.

06
APPLICATION SOFTWARE SECURITY
Neutralize vulnerabilities in web-based and other application software: Carefully test internally-developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic, and explicitly check for errors in all user input (including by size and data type).

07
WIRELESS DEVICE CONTROL
Protect the security perimeter against unauthorized wireless access: Allow wireless devices to connect to the network only if they match an authorized configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.

08
DATA RECOVERY CAPABILITY
Minimize the damage from an attack: Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more frequently. Regularly test the restoration process.

09
SECURITY SKILLS ASSESSMENT AND APPROPRIATE TRAINING TO FILL GAPS
Find knowledge gaps, and eradicate them with exercises and training: Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.

10
SECURE CONFIGURATIONS FOR NETWORK DEVICES SUCH AS FIREWALLS, ROUTERS, AND SWITCHES
Preclude electronic holes from forming at connection points with the Internet, other organizations, and internal network segments: Compare firewall, router, and switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates.

11
LIMITATION AND CONTROL OF NETWORK PORTS, PROTOCOLS, AND SERVICES
Allow remote access only to legitimate users and services: Apply host-based firewalls, port-filtering, and scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.

12
CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES
Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open a malicious email, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.

13
BOUNDARY DEFENSE
Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines: Establish a multi-layered boundary defense by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks ("extranets").

14
MAINTENANCE, MONITORING, AND ANALYSIS OF SECURITY AUDIT LOGS
Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines: Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.

15
CONTROLLED ACCESS BASED ON THE NEED TO KNOW
Prevent attackers from gaining access to highly sensitive data: Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.

16
ACCOUNT MONITORING AND CONTROL
Keep attackers from impersonating legitimate users: Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.

17
DATA LOSS PREVENTION
Stop unauthorized transfer of sensitive data through network attacks and physical theft: Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.

18
INCIDENT RESPONSE MANAGEMENT
Protect the organization's reputation, as well as its information: Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering

an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

19

SECURE NETWORK ENGINEERING

Keep poor network design from enabling attackers: Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers: DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.

20

PENETRATION TESTS AND RED TEAM EXERCISES

Use simulated attacks to improve organizational readiness: Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises— all-out attempts to gain access to critical data and systems to test existing defense and response capabilities.

FOOTNOTES

TARGETED ATTACKS + DATA BREACHES

1. An attack campaign is defined as a series of emails that:
   A.) Show clear evidence that the subject and target has beendeliberately selected.
   B.) Contain at least 3 or 4 strong correlations to other emails
   such as the topic, sender address, recipient domain, source IP address, etc.
   C.) Are sent on the same day or across multiple days.
2. http://www.symantec.com/connect/blogs/francophonedsophisticated-social-engineering-attack
3. In previous years, this category was labeled as Government.
4. The Professional category includes Engineering, Accounting, Legal, and Heath-related services. The Non-Traditional category includes Business, Amusement, and Repair-related services.
5. Fires in workplace premises: risk data. Holborn et. al.(2002) Fire Safety Journal 37 303-327. The full range is from 1:161 and 1:588.
6. These are frequently referred to as case-control studies, which compare a group of subjects with a disease (cases) to a similar group without the disease (the controls). The resulting ratio shows the risk of contracting the disease. In the case of spear phishing, we simply substitute "afflicted with a disease" for "received at least one spear-phishing email in 2013."
7. This represents the proportions of organizations within the same sector that were subjected to one or more targeted attacks within the year.
8. http://www.symantec.com/content/en/us/enterprise/media/ security_response/whitepapers/the-elderwood-project.pdf
9. http://www.symantec.com/content/en/us/enterprise/media/ security_response/whitepapers/hidden_lynx.pdf
10. http://www.symantec.com/en/aa/theme.jsp?themeid=sslresources
11. http://www.symantec.com/about/news/release/article. jsp?prid=20130206_01
12. http://www.symantec.com/about/news/resources/press_kits/ detail.jsp?pkid=ponemon-2013

ECRIME, MALWARE + MALWARE DELIVERY TACTICS

13. http://www.symantec.com/content/en/us/enterprise/media/ security_response/whitepapers/trojan_bamital.pdf
14. http://internetworldstats.com/
15. http://www.symantec.com/connect/blogs/grapplingzeroaccess- botnet
16. http://krebsonsecurity.com/2012/08/inside-a-revetonransomware-operation/
17. http://www.symantec.com/connect/blogs/massivemalvertising- campaign-leads-browser-locking-ransomware
18. http://www.symantec.com/security_response/writeup.jsp?docid=2012-111612-5925-99
19. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_state_of_financial_trojans_2013.pdf
20. http://www.secureworks.com/resources/blog/research/cutwailspam-swapping-blackhole-for-magnitude-exploit-kit/
21. http://www.threattracksecurity.com/it-blog/shylock-caphawdrops-blackhole-for-styx-and-nuclear/
22. http://www.scmagazine.com/criminals-move-quickly-to-otherexploit-kits-after-arrest-of-blackhole-author/article/315629/
23. For more details about Symantec Rulespace, please visit http://www.symantec.com/theme.jsp?themeid=rulespace
24. http://www.symantec.com/connect/blogs/massivemalvertising-campaign-leads-browser-locking-ransomware
25. https://otalliance.org/resources/malvertising.html
26. http://www.symantec.com/connect/blogs/creepware-who-swatching-you

SOCIAL MEDIA + MOBILE THREATS

27. http://www.symantec.com/connect/blogs/instagram-userscompromise-their-own-accounts-likes
28. http://www.symantec.com/connect/blogs/remote-access-tooltakes-aim-android-apk-binder
29. http://www.symantec.com/connect/blogs/rise-java-remoteaccess-tools
30. http://www.symantec.com/security_response/writeup.jsp?docid=2013-012916-2128-99
31. http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf
32. http://www.symantec.com/about/news/release/article.jsp?prid=20131001_01
33. http://www.symantec.com/connect/blogs/fakeav-holdsandroid-phones-ransom
34. http://www.symantec.com/security_response/writeup.jsp?docid=2013-060301-4418-99
35. http://www.symantec.com/connect/blogs/androidexprespamauthors-revamp-gcogle-play-android-express-s-play
36. In Japan email is often used instead of SMS, through special email addresses provided by mobile carriers. While primarily accessed and used through mobile devices, these email addresses can send and receive email from standard email addresses.
37. http://www.symantec.com/security_response/writeup.jsp?docid=2012-102908-3526-99
38. http://www.symantec.com/security_response/writeup.jsp?docid=2013-060411-4146-99

39. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/madware_and_malware_analysis.pdf
40. http://www.symantec.com/security_response/writeup.jsp?docid=2013-032910-0254-99
41. http://www.symantec.com/connect/blogs/windows-malwareattempts-infect-android-devices

PHISHING + SPAM

42. http://www.symantec.com/about/news/release/article.jsp?prid=20131001_01

BEST PRACTICE GUIDELINES

43. For more information about Norton Online Family, please visit https://onlinefamily.norton.com/

SANS CRITICAL CONTROLS

44. www.sans.org

CHAPTER 8

CAPABILITY OF THE INFORMATION AND COMMUNICATIONS TECHNOLOGY SERVICES USER SECTOR IN MALAYSIA: AN INDUSTRY PERSPECTIVE

SHAIFUBAHRIM SALLEH
Immediate Past President
shaifu@mspc.my

Malaysian Services Provider Confederation (MSPC)

MSPC
Malaysian Service Providers Confederation

INTRODUCTION

Convergence and reinforcement of information, cloud, mobile and social elements (Carlton, 2012) well supported with speed, seamless communications, multi-facet technological capabilities and diverse devices are poised to register a continuous plethora of new business opportunities and technological innovations. Over the past decade, many disruptive technological innovations have emerged in the Information and Communications Technology (ICT) sector, changing entire business landscapes and market structures as well as consumer behaviour and lifestyles (Christensen, 2011; Drucker, 2008). Currently, 'consumerization' of the Information Technology (IT) phenomena as well as the advent of social businesses, cloud computing, mobile social commerce, big data analytics, platform as a service (PaaS) and content as a service (CaaS) are increasingly impacting businesses and economic development (IBM, 2012, Saleh, 2012).

Specifically, 'consumerization' of IT connoting the usage of consumer devices and services in the workplace are giving rise to new work practices and business cultures (Mansor, 2012). Similarly, with the support of seamless broadband connectivity, e-mail communication, data security and authentication systems in place, many companies are already experimenting or reinventing themselves with new work cultures such as Bring Your Own Device (BYOD) and working remotely from anywhere at anytime. Indeed, the technology savvy Y & Z generations prefer such work practices as opposed to typical rigid working hours. Social technology platforms are also increasingly being used for generating new networks of customers, partners and employees, thus expanding the business coverage and innovation scope (Mansor, 2012; IBM, 2012). Some companies gauge customer mood and employee sentiments using social networks platforms. These are only the tip of the iceberg, with many other things to come. Such changes are not only evolutionary but sometimes revolutionary, impacting not only the technology providers but also the users of ICT services (ICTS).

Today, ICT businesses and communities are confronted with countless technological features and applications. These include pervasive and ubiquity computing, smart-infrastructure, preventive healthcare, green technology entailing low power servers, green data centres and tele-presence, cyber warfare, flexibility in mass customization, rise of the machines, pay as you use models, real time and all-time communications, networking and interactions (Abdul Wahab, 2012). All companies pay great attention to technology and its innumerable applications such as cloud computing, bug data analysis, security platforms. e-services, wireless intelligence and all things Internet-based. Therefore, the ICT capabilities of companies is crucial to business growth, not only in reaching out to consumers and clients but also within the internal working of the companies themselves, encompassing administration and management procedures across the board.

Additionally, ICT also plays an important role in creativity and innovation as well as communication, effectively embracing the each and every part of today's business.

POLICY AND INDUSTRY IMPERATIVES

Since the advent of the Internet in the early nineties, the Government of Malaysia has continuously promulgated the deployment of ICT as a major development thrust in achieving a knowledge-based economy (EPU, 2001; Abdulai, 2001; Nair, 2007; Abdul Wahab and Ramachandran, 2011;) and an innovation-based economy (EPU, 2006 ; Abdul Wahab, 2012). The New Economic Model (NEM) released in March 2010, among many others,

had identified ICT as a strategy to alleviate the country from the middle income trap (NEAC, 2010; PEMANDU, 2010).

It has been more than two decades of concerted effort to usher the nation incrementally into an endogenous growth path vide an ICT promulgation strategy but it has yet to reach the global standards like what the Koreans and Japanese have achieved. In the industrial age, Japan has created numerous global brands with global standards and quality (e.g. Honda, Toyota, Panasonic and Sony), and in many instances, they have overtaken the Western market which had been dominating the industrial market for many ages since the Renaissance started five centuries ago (Yu, 2012).

In the same vein, the Koreans are making an indelible mark by innovating world class ICT products and services (e.g. Samsung, Hyundai and LG), which have successfully captured a substantial share in the global market (Hollis, 2008). The Chinese are joining the global brands rank, even at a faster rate (Hollis, 2008). Despite poor command in the English language, which is considered the lingua franca of business and the Internet world (Wolk, 2004; Bhatnagar, 2006), companies in Japan and Korea have registered meteoric rise in entrepreneurial development.

This may be conjectured to many factors including cultural, societal, educational, legal, financial and political will as well as an ingrained societal value system. However, such factors alone would not suffice unless companies enhance their organizational capabilities, which is fundamentally critical for research, development, innovation, patenting intellectual properties, registering trademarks and branding as well as for having a successful commercialization track record.

Organizational capabilities have been always a major concern for any company for its existence, relevance, and business continuity (Schienstock, 2009; Dosi, Nelson and Winter 2000; Grant, 1996). The only difference is what was apt for an agricultural or industrial age may not be appropriate for the current information era (OECD, 1997), which comes with ubiquitous and pervasive impact of contemporary ICT on all spheres of life, unprecedented in the human history (Castells, 1996; Tapscott, 1997; Azzman, 2000; Castells, 2000; Ramachandran, 2008). It is continuously changing the way one works, plays and performs transactions, including institutional structures, roles, rights, rules and regulations as well as relationships and networking (Graham, 2008; Shapiro & Hal Varian, 1999; Dertouzos, 1997; Cairncross, 1997).

ICT investments in Malaysia are targeted at sources of new growth areas such as hybrid of wired and wireless telecommunications, multimedia content development, packaged software, software and hardware consultancy as a service, exports and imports of ICT services, e-commerce, mobile and online banking, e-government and outsourcing. Similarly, on the technology front, the country has also been experiencing significant strides in technological advancements pertaining to Nanotechnology, Micro-Electro- Mechanical Systems (MEMS), Semantic Technology, Wireless Communication, Grid-Computing, Biometrics and Biotechnology, which are aimed at revitalizing the ailing micro-electronics sector (Abdul Wahab, 2012).

In tandem, the Government has also been promoting research and development in the ICT Services segments through six technology focus areas (TFAs) under ICT Roadmap 2012, namely e-Services, Wireless Intelligence, Ubiquitous Connectivity, Big Data Analytics, Security & Platforms and Cloud Computing (Abdul Wahab, 2012). The TFAs were identified after taking into consideration global ICT trends such as pervasive and ubiquitous computing, pay as you use models, smart infrastructure,

preventive health care, rise of the machines, real time and all the time, mass customization and cyber warfare as well as capabilities pertaining to human capital, patenting and commercialization culture (Abdul Wahab, 2012). The earlier ICT Roadmap 2008 focused on only three key TFAs, namely Wireless Sensor Networks, 3DInternet and Predictive Analytics. The industry membership, specifically the composition of The National ICT Association of Malaysia, popularly known as PIKOM, has also diversified over the years. When it started in 1986, it solely consisted of members from the computer hardware and software vendor industry (Saleh, 2011).

Today, its membership covers the entire ICT landscape, namely bio technology, business process outsourcing, communication / networking, consultancy / professional services, creative content, data centre / web hosting providers, education / training, hardware design, Internet-based business, information technology Outsourcing (ITO), business process outsourcing (BPO), shared services outsourcing (SSO), maintenance, repairs and services, mobile and wireless, network security, software development, system integrators / value added resellers, telecommunications and principal for manufacturers. The country has been always at the point of inflexion, pursuing new frontiers and heights in the ICT evolution (Rasiah, 2009) beginning with main-frame introduction in the Sixties (Alhabshi, 2002) followed by setting up of microelectronics production factories in the Seventies (Vijayakumari, 1994; Jomo and Edwards, 1993). In this evolutionary process, the role of the ICT sector, more so the ICT services segment, is undeniably seen as a mover and shaker of not only ICT products and services producing companies but also the ICT user industries like banking, insurance, medical, education, transport, logistics, et cetera. Indeed, the era of the Internet saw emergence of many modern lifestyle applications pertaining to online banking, distance learning, tele-working, tele-medicine, e-commerce, online shopping, cloud computing, big data analytics, provision of e-government services and e-democracy et cetera (Tapscot, 1997; Castells, 2000; Saleh, 2011). Similarly, with an eye towards creating an eco-friendly environment, new and innovative green ICT products and services are being added into the market more often now than in the past.

For the same objective, creation of green ICT jobs is also on the rise (Rajendra, 2012). In tandem with technology evolution, industries are also compelled to beef up their organizational capabilities in coping with structural reforms and institutional changes pertaining to online publishing (CIJ, 2012), Internet freedom (CIJ, 2012; RWB, 2011), data protection (Khera, 2012), cyber threats and security (Ong and Tan, 2012), intellectual property rights (IPR) and branding (Kwang, 2010). In other words, today the ICT sector in its contemporary form has evolved to be more than a mere collection of technological tools (Azzman, 2000). Knowledge-based organizations (Grant, 1996) and skilled biased techno-organizational change (Breshhnaham, Brynjolfsson and Hitt, 1999) imperative for not only for spearheading the nations into more advanced developed status but also for accelerating the phase, pace and speed of knowledge-based innovation society and economy. As highlighted earlier, the reinforcement of information, cloud, mobile and social elements in the days ahead are likely to register a plethora of new applications (Carlton, 2012) that have never been seen before. Therefore, the level of preparedness and, more so, the ability to cope with contemporary demands have become imperative not only for ICT services providers but also for ICT users in the Government and businesses as well as societies at large.

CAPABILITY AT SECTOR LEVEL

Sectors are seen as complex systems of organizations, which also involve a wide range

of stakeholders in the public sector, as well as across the civil society and the private sector – at the international, national, sub-national and local levels (OECD,2010). All these players are likely to shape and condition the dynamics of a sector (Van Esch et al., 2010).

Typically, sector dynamics are influenced by political decisions, policy directions, socio-cultural elements, power relations, incentive systems and inter-linkages with other sectors (Boesen, 2008). The ICTS sector is not an exception to such complexity, multidimensionality and interdependence as well as multi-stakeholder partnership involvement. However, the paper did not assess all the dimensions of the sector's dynamics, which would have been a formidable task, but rather only confined observations to the firms' usage of ICT.

SIGNIFICANCE OF ORGANIZATIONAL CAPABILITY

Businesses consider organizational capability as the overall ability of a company in managing its resources efficiently and effectively in meeting its business goals and aspirations (Gusberti and Echeveste, 2012; Kelchner, 2012) as well as ensuring their business relevance, continuity and growth (Prahalad and Hamel, 1990). This can be seen from two aspects: managing business efficacy and managing internal dynamics. As surmised by Kelcher (2012), organizational capability in managing business efficacy includes: (i) ability to administer, manage and appropriately direct the experiential knowledge and skills endowed in the workforce towards achieving the company's business objectives (Drucker, 2008; Helfat and Lieberman, 2002); (ii) ability to create new knowledge, innovating new products, services and processes as well as undertake commercialization of patents and licenses (Knight and Cavusgil, 2004; Christensen, 2011); and (iii) ability to uphold good customer relationship including learning from customers (George, 2003; De Feo and Bernard, 2005).

In managing the internal dynamics, the organization capability is reflected on: (i) its ability in balancing customer demands and organization resources especially in managing quality and process improvement dynamics (Keller and Keller, 2010; George, 2003; Pyzdek, 2002); (ii) creating a conducive working environment and motivational elements for its employees (Helfat and Peteraf, 2003) and (iii) how flexible, versatile, and responsive it is towards changing work culture and practices, business dynamics and sustainable growth (Drucker, 2008; Lawson and Samson, 2001). Succinctly put, organizational capability does not only involve business factors but also institutional and people elements that support business growth. As such, when firm level strengths and weaknesses are aggregated across the industry, it will provide a cumulative reflection on sector level business capability.

However, in practice, organizational capability vary greatly among companies depending on their size, financial strength, core competencies, human resource practices, technology adoption, work culture and practices, institutional support system, R&D and innovation capability as well as organizational values (Knight and Cavusgil, 2004; Schienstock, 2009). Typically, the multi-nationals and the big corporations who aspire to remain relevant and sustainable in a fast changing business and technological world are likely to have a greater tendency, as well as the capacity, to put capability models in place. When processes, procedures, methods, rules, roles and regulations are in place, it will be a lot easier for organizations to constantly identify gaps, business risks and market potentials and also undertake competitor analysis, and comprehend product and service development nuances (Lawson and Samson, 2001; De Feo, Joseph and Barnard, 2005; George, 2003).

Due to various constraints, it is difficult for small and medium businesses to pursue globally recognized certifications as these usually require that high standards and quality be met. The cost factor is also a deterrent. Such organizations are likely to depend upon Government support in improving their organization capabilities and workforce competencies. Therefore, assessing sector level capability is not only in the interest of business development but is also a matter of public policy and macro-economics, especially when it comes to resource appropriation and allocation by mainstream government agencies.

SHADES OF CAPABILITY MODELS IN ICT

There are many types of models and levels of capability assessment targeted at the organizational, team and even individual level (Bakhru and Grant, 2010). Prahalad and Hamel (1990) viewed core competence of a firm as a tree – roots constitute competencies, trunk and limbs as core products and flowers representing end products. Similarly, Chandler (1992) conceived firm level capabilities as a vertical chain consisting of R&D, raw materials sourcing to marketing and up to sales and distribution.

However, the predominant view about organizational capabilities is integration of knowledge hierarchy entailing various functional and cross-functional capabilities (Bakhru and Grant, 2010) at strategic, tactical and operational levels (Zollo and Winter, 2002). As mentioned earlier, any organizational capability model is simply aimed at measuring what organizations are able to do, or more precisely, deploying resources towards achieving a desired end result (Helfat and Peteraf, 2003). It is the question of how organizations build or create their capabilities, which may entail cognitive search through one or more of the following: covert or overt learning via concepts and models (Gavetti, 2005), sourcing from outside or transfer of capabilities from existing to new businesses (Buenstorf and Klepper, 2005), prior employment of the founders (Philips, 2002), knowledge conversion from tacit to explicit modes between individual and organizational levels (Nonaka, 1994) or, simply learning by doing (Prencipe & Tell, 2001).

CAPABILITY MODELS IN ICT

In the ICT sector, models such as Capability Maturity Model Integration (CMMI) from the Software Engineering Institute (SEI), used for gauging software development maturity (SEI, 2013; Nandayal and Ramasamy, 2011) and Information Technology Infrastructure Library for gauging IT management practices (ITIL, 2013) are widely used in assessing organizational capabilities and competencies. Some organizations that pursue CMMI also, in tandem, implement People Capability Maturity Model (PCMM) from SEI, which is used for gauging workforce competency at organization wide level (Nandyal, 2003; Nandyal and Ramasamy, 2011).

Similarly, agencies like the Green Computing Initiative (GCI) provide dedicated certifications for organizations and individuals in the area of Green Computing that aligns all IT processes and practices with the core principles of environment sustainability, which are to reduce, reuse, and recycle wastes (IAOP, 2013; Curry, Guyon, Sheridan, and Donnellan, 2012; Rajendra, 2012). In the contemporary outsourcing sector where ICTS usage is the core, capability models like e-Sourcing Capability Model for Service Providers (eSCM-SP) and the e-Sourcing Capability Model for Client Organizations (eSCM-CL) from International Association of Outsourcing Professionals (IAOP) are deployed in assessing organizational competencies. Some capability models are organization specific like IBM Process Reference Model for IT (PRM-IT), which assesses IT management processes within IBM,

mainly by providing a checklist on adherence to process and quality (Finden-Browne, 2007).

SUBJECT MATTER SPECIFIC CAPABILITY MODELS: ALSO APPLICABLE TO ICT SECTOR

Besides sector specific organizational models, some models are subject matter specific but applicable to any sector including ICT. To name a few, these include new product development (Ethiraj et al, 2005), project management (Ethiraj et al, 2005), R&D capability (Nerkar and Prachuri, 2005), acquisition capability (Arikan and McGahan, 2010), customer relations capability (Ethiraj et al, 2005), engineering capability (Kazanjian and Rao, 1999) and quality and process improvements capability using Six Sigma methodology (DE Feo and Joseph, 2005; Pyzdek, 2003).

A close scrutiny reveals that these models are supported with well-defined methods, processes, procedures, rules, regulations and operational templates as well as certification and accreditation mechanisms for assessing organizational competencies, but focused on organizational needs (Bakhru and Grant, 2010).

MIXED MODELS

In this progression, it is not uncommon nowadays to discover deployment of mixed models especially software companies pursuing CMMI, PCMM and Six Sigma practices as these models complement each other well. Specifically, CMMI provides the framework for developing maturity levels in organizational processes, PCMM provides framework for attaining maturity in workforce competency and Six Sigma practices come in handy as a data supported problem solving methodology (Nandayal and Ramachandran, 2011). Whichever model an organization may use, they all have one common objective of getting certified based on their use of and adherence to the best practices and processes as well as quality. Indeed, certifications help greatly in branding organizations and their products and services, which is critical for market access and entry; for example, CMMI certification is one of the requirements for any company (including foreign companies) to procure software development businesses that come under the Government contract (Carmel, 2003).

CAPABILITY CERTIFICATION

Most of these organizational or individual capability models come with certifications, which determine competency, authority, or credibility. Capability certifications are issued either by a global institution or an individual organizational. A certificate is issued once the applying organization attains the prescribed standards in product development or service delivery or process maturity or workforce competency as per the criteria and guidelines laid out by the certification issuing agency. Certification agencies can be divided into two types, one operating at the global level and the other at an organization level. For instance, SEI of Carnegie Mellon University holds the authority in issuing CMMI certification for software development maturity and PCMM for attaining work force competency. Similarly, ITIL Certification Management Board (ICMB) of United Kingdom certifies IT Management practices; GCI on green computing practices and IAOP on outsourcing practices.

Organizations like General Electric and Motorola, early adopters of Six Sigma for process and quality improvement activities, have developed their own certification programmes as part of their Six Sigma implementation, verifying individuals' command of the Six Sigma methods at the relevant skill levels, namely White Belt, Green Belt, Black Belt, etc. Though started in manufacturing plants, today the Six Sigma practice has spread to transactional and services-based organizations (Keller and Keller, 2010; De Feo and Bernard, 2005). Unlike global institutions, criteria for Six

Sigma certifications vary across organizations as there is no standard certification body (Coryea, Leroy, 2006).

KEY CHALLENGES

Not all organizations are at the same level in pursuit of organizational capabilities (Knight and Cavusgil, 2004). Typically, the multi-nationals and the big corporations who aspire to remain relevant and sustainable in a fast changing business and technological world have a greater tendency to put capability models in terms of processes, procedures, methods and approaches as well as administrative and institutional support systems in place. Such institutional best practices facilitate organizations to constantly identify gaps, distinguish business risks, conduct competitor analysis, understand market potentials and comprehend product and service development nuances (Lawson and Samson, 2001).

Lacking such agility, maturity and competency may affect an organization's performance in terms of decision making and undertaking timely corrective actions, which in turn becomes detrimental to revenue, growth, profitability, corporate governance, market positions and industry leadership (De Feo, Joseph and Barnard, 2005; George, 2003). Smaller organizations may lack adequate resources in pursuit of globally recognized certifications, which typically come with high expectations in terms of standards and quality and is quite costly. Such organizations are likely to depend upon Government support in building their organization's capabilities and workforce competencies. The other challenge is that levels of capabilities vary across organizations and among individuals (Schienstock, 2009). Individuals enhance their capabilities either on their own, if it is affordable, or with their organization's support (Rajendra, 2012, Nandyal and Ramasamy, 2011). Failing which, they also may become irrelevant due to lack of up to-date knowledge and competency at work.

GENERIC CAPABILITY MODELS

Some models are generic but applicable to specific situations like Carmel's (2003) Oval Model for gauging success factors for software exports. Similarly, Lawson and Samson (2001) reviewed Kanters' (1989) Innovation Capability model by incorporating new business streams, products and process systems, knowledge factors, end customer and market demands. In the same vein, this paper also proposed a H-Model Framework to gauge the capabilities of the ICTS User sector.

H-MODEL FRAMEWORK FOR ASSESSING SECTOR LEVEL CAPABILITY

Recognizing the gaps as well as the business and policy relevance, the paper proposed a generic H-Model Framework (HMF) to investigate the collective capability of the ICTS User sector, as shown in Figure 1. The H-Model Framework represents eight broad based factors under three dimensions, namely Institutional Dimension, People Dimension and Business Dimension. The institutional dimension entails four factors, namely visionary leadership, government relations, organizational elements and security & risk; the business dimension covers quality and standards, business intelligence, innovation and process, and market & globalization; and the people dimension, that is central to both the institution and business dimensions, consists of human capital and motivational elements.

Essentially, the H-Model Framework provided the conceptual framework for designing survey instruments, particularly survey questionnaires and analytics frameworks. Since, from the onset itself the survey covered large corporations, no efforts have been made to gather any demographic characteristics and features of

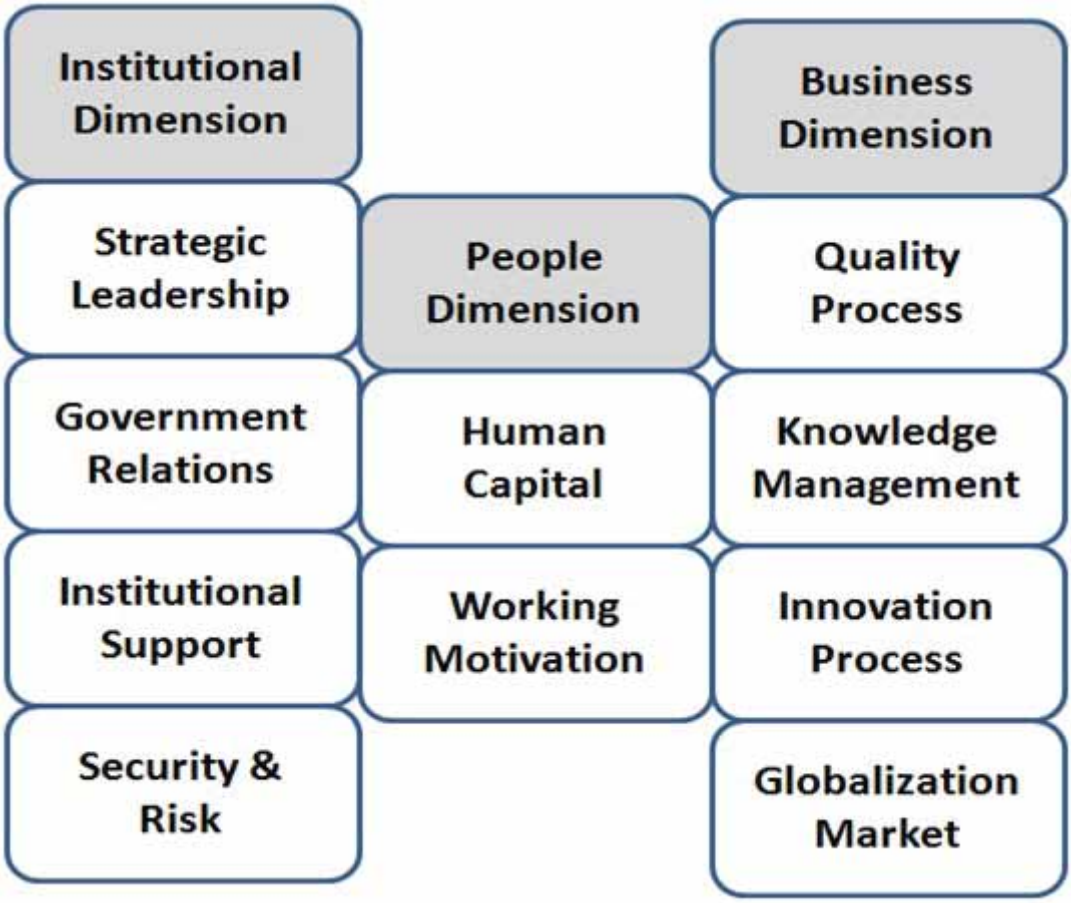


Figure 1: H-Model Framework for Assessing Capabilities of ICTS Companies

firms. The questionnaire probed a total of 30 variables of ICTS User firm's capability level, raising three questions under each broad based factor. Due references are also made to experiences of past studies so that the relationship between the 30 variables and the observed patterns have relevance, validity and that it remains appropriate to the study.

MALAYSIA AS A CASE STUDY

For illustrating the proposed sector level capability, the study attempted to assess the collective organizational capabilities of ICTS users in Malaysia. Malaysia has a long ICT history, not only as ICT producers but also as ICT users. Since the early 1960s, when mainframe computers were introduced in the country followed by the establishment of the micro-electronics industry in the early 1970s, all national development plans have highlighted ICT as one of the key thrusts. Specifically, over the past two decades, the Internet driven sector is considered a key enabler and driver in the development of a knowledge-based economy and society.

Currently, the country is in pursuit of attaining a high income status by 2020. Besides depending upon foreign direct investment (FDI) as in the past, in tandem the country also promulgates an endogenous growth strategy. With this strategy, the country is poised to embark upon indigenous inventions and innovations of globally recognized stature. Again, contemporary ICT and its services component are poised to play a significant role in this endeavor. Unequivocally, this aspiration can only be realised if both the ICT producer and user sectors are equipped with a competent workforce. They must also be responsive to technology adoption, be active in R&D, be innovative and also strive towards commercialization and patenting of inventions.

SURVEY METHODOLOGY

A total of 108 ICTS user companies were targeted for data collection. The selected respondents were members of the Chief Information Officer (CIO) Chapter of The National ICT Association of Malaysia (popularly known as PIKOM) and constituted only a sub segment of PIKOM's membership database. The CIO Chapter was formed in 2009. The main objective of this Chapter is to raise the level of professionalism and standards through the sharing and exchange of information, knowledge and experience related to ICT; creating a platform for building networks; nurturing leaders to deploying leading edge technology; and employing best practices in ICT management.

The ICT user sector is wide and diversified, including both small and medium enterprises as well as large corporations and multinationals. However, the PIKOM CIO Chapter members constitute only those companies with an average annual budget of more than RM 10 million and employ at least 1,000 personnel. In other words the sampling frame constituted only large firms, precluding ICT users in the SME segments. Using these criteria, the targeted CIO members in the PIKOM membership database represented the following industries:-

- Business & Professional;
- Logistics;
- ICT;
- Distributive Trade;
- Construction;
- Education & Training;
- Environmental;
- Healthcare;
- Advertising Services; Tourism; and
- Oil & Gas

Large corporations and multinational companies typically lead in adopting new technology and best practices, often setting the trend for the smaller organisations which follow suit when said technology becomes more affordable. Some of the key contemporary technology areas that were probed in the study include the following:-

- Security platforms
- Cloud computing
- Big data analytics
- E-Services
- Ubiquitous connectivity
- The Internet
- Media tablets and beyond
- Mobile centric applications
- Wireless communications
- Buy your own device (BYOD)
- Green / Innovating to zero

With the focus being on the higher end of the ICT user community, the study also probed disciplines pertaining to the management of projects, security, network, quality and IT services (ITSM) as well as Software process improvement Network (SPIN).

The study was conducted mainly in the Klang Valley where most of the PIKOM CIO members are located. The telephone and e-mail were used to collect responses, followed by field visits and face-to-face interviews wherever necessary. The study successfully netted 96 responses, translating to a 88.9% response rate.

MODEL ASSUMPTIONS

The study used both exploratory and factor analysis. Factor analysis was used mainly to condense the 30 variables into a few meaningful latent constructs. Prior to that, the following conceptual and statistical assumptions of the model were validated:-

i. ***Reliability measure:*** Cronbach's measures of reliability using Alpha and Split-Half method were carried out. This measure ensured internal consistency between multiple measurements of a variable and clarity of respondents in understanding

Methodology	Number of Items	Cronbach's Alpha	Remark
Alpha	30	0.962	
Split-half	15	0.936	The items are: Visionary Leadership, Responsive to ICT best practices, ICT Innovations, Mobilizing finance for ICT , Soliciting Voice of Customers (VOC), Branding & business networking, ICT Skills & Competencies, Inter-disciplinary skills, Knowledge seeking workforce, Rewards & recognition, Talent retention, Knowledge sharing, Innovation support, R&D and Commercialization, Branding & patenting.
	15	0.935	The items are: Quality and standards, Quality accreditations, Service level & customer satisfaction, Awareness security & risk management practices, Adoption security & risk management practices, Security threats mitigation, Integrated Knowledge Management System, Market & business intelligent, Information & knowledge dissemination, Awareness government incentives, Soliciting Government grants, Networking with Government, Managing global ICT threats, Pursuing global ICT opportunities, Coping ICT trade liberalization policies.

Table 1: SPSS Cronbach's Reliability Measure on Survey Reliability Pertaining to Questionnaire Consistency and

the constructs investigated, that is, organizational capability of each company (Hair et al., 1992; Hair et al, 2006; Timm, 2002; Liu, Onwuegbuzie and Meng, 2011). The results are shown in Table 1, which were well above the recommended measure of 0.7 as a threshold limit (Field, 2005; Hair et al, 1992);

ii. ***Adequacy of response rate:*** 96 responses netted in the survey fulfilled the condition that it should exceed the total number of study variables, which was 30 and the recommended sample size of 50 cases for undertaking meaningful factor analysis;

iii. ***Reducing error variance:*** Since the study is based on pre-determined conceptual framework, the selection of appropriate variables implicitly ensured that specific and error variances are smaller than common variance;

iv. ***Rotated factor loadings:*** Orthogonal rotation was used not only for assuming independence among the variables but also aimed at redistributing the variance among the latent roots, otherwise heavy loadings will be concentrated on the first component under un-rotated factor loadings;

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.904
Bartlett's Test of Sphericity	Approximate Chi-Square	2665.3
	Degrees of freedom	435
	Significance.	.000

Table 2: Kaiser-Meyer-Olkin (KMO) and Bartlett's Test

v. ***Significance of correlation measures:*** Statistically, all the correlations in the correlation matrix were found to be significant at the 0.01 level;

vi. ***Adequacy of sample size and normality assumption:*** As shown in Table 2, the Kaiser- Meyer-Olkin measure of sampling adequacy score of 0.904 is well above the recommended threshold level of 0.3 (Malhotra, 2008; Hair et al, 2006; Hair et al, 1992), indicating that the sample size is adequately large thus it validates the normality assumption;

vii. ***Suitability of factor analysis:*** The Bartlett's test of Sphericity, shown in Table 2, also provided a single measure to assess the statistical significance of the correlation

matrix at the 0.001 level of significance. Literature review has indicated that at least 30% of the variables investigated in the study should fulfill this statistical significance condition before factor analysis could be considered on data reduction activity (Hair et al, 2006; Timm, 2002; Hair et al, 1992). The results showed that all correlations were significant; see Table 2.

viii. ***Communalities measure:*** Table 3 shows the communalities measures for the 30 factors. The communalities indicate the amount of variance an original variable shares with all the other variables and, as such, technically speaking variables that record a correlation value below 0.5 to be removed from subsequent analysis. This analysis revealed that all correlations generated by the 30 variables exceeded the correlation measure of 0.3, which is one of the criteria set in the literature review for determining appropriateness of factor analysis (Hair et al, 2006; Timm, 2002; Hair et al, 1992).

ix. ***Variance analysis:*** Table 4 shows that the total variance is explained by the latent roots under initial eigenvalues (un-rotated) and Varimax Orthogonal Rotation factor loadings. By default, the SPSS system generated 6 loading latent factors, accounting for 77.0% of the total variations. Under the initial eigenvalues component, one alone accounted for 47.6% of the total variations and the rest of the components contributed only a small percentage of variations each (Table 4). However, the efficiency of variation distribution among the 7 latent

Communalities

Study Variables	Initial	Extraction	Study Variables	Initial	Extraction
Visionary Leadership	1.000	.631	Quality and standards	1.000	.743
Responsive to ICT best practices	1.000	.689	Quality and accreditations	1.000	.792
ICT Innovations	1.000	.664	Service level & customer satisfaction	1.000	.744
Mobilizing finance for ICT	1.000	.779	Awareness security & risk management	1.000	.821
Soliciting Voice of Customers (VOC)	1.000	.722	Adoption security & risk management practices	1.000	.861
Branding & business networking	1.000	.705	Security threats mitigation	1.000	.799
ICT Skills & Competencies	1.000	.738	Integrated Knowledge Management System	1.000	.896
Inter-disciplinary skills	1.000	.747	Market & business intelligent	1.000	.888
Knowledge seeking workforce	1.000	.801	Integrated Knowledge dissemination	1.000	.848
Rewards & recognition	1.000	.718	Awareness government incentives	1.000	.777
Talents retention	1.000	.674	Soliciting Government grants	1.000	.855
Knowledge sharing	1.000	.716	Networking with Government	1.000	.795
Innovation support	1.000	.782	Managing global ICT threats	1.000	.714
R&D and Commercialization	1.000	.817	Pursuing global ICT opportunities	1.000	.760
Branding & patenting	1.000	.809	Copying ICT trade liberalization policies	1.000	.815

Table 3: Communalities of Study Variables under Extraction Method: Principal Component Analysis

Component	Initial Eigen Values =1 Extraction Sums of Squared Loadings			Varimax Orthogonal Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	14.958	49.9	49.9	4.575	15.3	15.3
2	2.516	8.4	58.3	4.381	14.6	29.9
3	1.736	5.8	64.1	4.050	13.5	43.4
4	1.521	5.1	69.2	3.478	11.6	55.0
5	1.230	4.1	73.2	3.341	11.1	66.1
6	1.141	3.8	77.0	3.276	10.9	77.0

Table 4: Sums of Squared Loadings

Total Variance Explained			
Component	Varimax Orthogonal rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %
1	5.105	17.0	17.0
2	4.738	15.8	32.8
3	4.459	14.9	47.7
4	4.197	14.0	61.7
5	3.462	11.5	73.2

Table 5: Latent Roots Extraction Under 5-Factors Option

components improved greatly under the Varimax Method of orthogonal rotation. As shown in Table 4, it can be observed that the skew in the variation was reduced with component 1 accounting for 15.3 % of the total variation as opposed to 49.9% under an un-rotated situation. Similarly, component 2 and component 3 accounted for 14.6% and 13.3% respectively, which are much higher than those depicted under an un-rotated condition.

x. ***Number of latent factors:*** Deciding on the number of factors required a more discretionary approach rather than a rigid and objective stance. Two challenges warranted attention in deciding the initial six components. One was that the correlation value for some of the best represented variables under certain components had to be above 0.5, which was set as a minimum criterion for deciding on the representative variable (Hair, et al, 2006; Hair et al, 1992). Indeed, all variables depicted correlation above this criterion value. The other more critical challenge was that in some of the latent components, the number of variables fell below 5, which was set as a minimum criterion for understanding and examining intra-relationships among the constructs, before making any meaningful attempts in naming or interpreting the latent components (Hair, et al, 2006; Hair et al, 1992).

After taking into consideration these constraints, the study arbitrarily finalized five latent components for the final analysis and, accordingly, the sums of the squared loadings under the Varimax Orthogonal Rotation are shown in Table 5. The results showed an improved distribution of variance compared to the earlier six-factor loadings but at the expense of reduction in total variance from 77.0% to 73.2%, which registered only marginal reduction.

OVERALL ANALYSIS

As shown in Table 6, 86.5% or 83 out of 96 companies netted in the survey only provided one service. Another 6.3 % were providers of two services and the rest provided multiple-services. For example, companies like Hitachi Sunway Information System offered services encompassing ICT, distributive trade, construction, education & training, environmental, healthcare, advertising, tourism and property development.

Thus, taking into account the multiplicity of services the survey netted a total of 127 different applications. Table 7 below shows the distribution of technology by sector. It shows that security platforms ranked the highest with 114 applications followed by wireless communications and Internet of Things (IOT) indicating technology priority among the companies netted in the study.

Table 8 illustrates the distribution of technology application by type of ICT Services. Despite small number of incidences netted, the results provided some indication that security platforms are the major concern among the users of ICT. Indeed, an average 89.8%

Number of Services	Frequency	Percent
1	84	86.5
2	6	6.3
3	1	1.0
4	2	2.1
6	1	1.0
7	1	1.0
8	1	1.0
Total	96	100.0

Table 6 : Distribution of Number of Services Provision

Type of Technology	Technological Incidences Netted (Total = 127)	Percentage
Security & Platforms	114	89.8
Wireless Communications	88	69.3
Internet of Things	78	61.4
e-Services	62	48.8
Mobile Centric Applications	51	40.2
Media Tablets & Beyond	42	33.1
Cloud Computing	33	26.0
Big Data Analytics	28	22.0
Ubiquitous connectivity	23	18.1
Buy Your Own Device (BYOD)	23	18.1
Green Innovating to Zero	15	11.8
Other technology	13	10.2

Table 7 : Distribution of Technology Incidences Netted by Type of Technology

ICT Services User Companies	Total Responses Netted in the Survey (N-96 cases)	Security & Platforms		Cloud Computing		Big Data Analytics		e-Services		Ubiquitous connectivity		Internet of Things	
	Frequency	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Business & Professional Services	7	6	85.7	3	42.9	4	57.1	4	57.1	2	28.6	7	100.0
Logistic Services	8	6	75.0	1	12.5	4	50.0	4	50.0	3	37.5	5	42.0
ICT Services	16	14	87.5	7	43.8	3	18.8	7	43.8	4	25.0	8	50.0
Distributive Trade Services	4	3	75.0	0	0.0	2	50.0	1	25.0	1	25.0	1	25.0
Construction Services	10	9	90.0	2	20.0	1	10.0	6	60.0	3	30.0	6	60.0
Education & Training Services	4	3	75.0	1	25.0	0	0.0	2	50.0	1	25.0	2	50.0
Environmental Services	2	1	50.0	1	50.0	1	50.0	2	100.0	0	0.0	1	50.0
Healthcare Services	5	5	100.0	3	60.0	1	20.0	2	40.0	1	20.0	3	60.0
Advertising Services	2	2	100.0	1	50.0	0	0.0	1	50.0	0	0.0	1	50.0
Tourism Services	3	3	100.0	1	33.3	0	0.0	1	33.3	0	0.0	1	33.3
Oil & Gas Services	5	5	100.0	1	20.0	1	20.0	2	40.0	0	0.0	4	80.0
Other	61	57	93.4	12	19.7	11	18.0	30	49.2	8	13.1	38	62.3
Total	127	114	89.8	33	26.0	28	22.0	62	48.8	23	18.1	78	61.4

ICT Services User Companies	Total Responses Netted in the Survey (N-96 cases)	Media Tablets & Beyond		Mobile Centric Applications		Wireless Communications		Buy Your Own Device (BYOD)		Green Innovating to Zero		Other technology	
	Frequency	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Business & Professional Services	7	4	57.1	3	42.9	4	57.1	1	14.3	1	14.3	0	0.0
Logistic Services	8	3	37.5	2	25.0	5	62.5	1	12.5	0	0.0	0	0.0
ICT Services	16	8	50.0	9	56.3	11	68.8	5	31.3	3	18.8	4	25.0
Distributive Trade Services	4	2	50.0	2	50.0	3	75.0	1	25.0	1	25.0	0	0.0
Construction Services	10	3	30.0	4	40.0	7	75.0	1	10.0	2	20.0	1	10.0
Education & Training Services	4	2	50.0	1	25.0	2	50.0	1	25.0	1	25.0	1	25.0
Environmental Services	2	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	1	50.0
Healthcare Services	5	2	40.0	2	40.0	4	80.0	1	20.0	1	20.0	1	20.0
Advertising Services	2	1	50.0	2	100.0	2	100.0	1	50.0	1	50.0	0	0.0
Tourism Services	3	1	33.3	1	33.3	2	65.7	1	33.3	1	33.3	1	33.3
Oil & Gas Services	5	0	0.0	0	0.0	4	80.0	0	0.0	0	0.0	0	0.0
Other	61	16	26.2	25	41.0	44	75.1	10	16.4	4	6.6	4	6.6
Total	127	42	33.1	51	40.2	88	69.3	23	18.1	15	11.8	13	10.2

Table 8 : Distribution of ICT Services User Companies by Type of Technology

of ICTS users were equipped with security platforms, which understandably is critical for safeguarding data and operations. The next priority was wireless communications, which is significantly gaining footage in various types of applications and business operations, in particular with the advent of broadband technology.

OVERALL CAPABILITY

The survey used the Likert Scale for gauging the performance of each organizational capability variable by defining "1" for very weak and "5" for very strong. Against this backdrop, the analysis defined a binomial criterion for defining ICTS User Sector Capability Maturity, which are as follows:-

Mean Score Value	Sector Capability Maturity Status
≥ 3.5	"Attained Capability Maturity"
< 3.5	"Further Work Needed on Improving Sector Capability".

As shown in Figure 2, of the 10 broad-based factors investigated, five factors namely Security & Risk, Visionary Leadership, Human Capital, Institutional Support and work environment; secured a mean score of 3.5 and above. This shows that ICTS user companies pay a great deal of attention to these factors in comparison to quality process, knowledge management, market and globalization, Government relations and innovation processes. Indeed, Government relations and innovation processes secured only a mean score of 2.95 and 1.05 respectively. Understandably being an integral component of a large organization, building Government relations or undertaking innovation activities may not be under the purview of the CIO members who responded in the survey.

FACTOR ANALYSIS

To understand the inner dynamics of the broad-based factors, factor analysis was used in reducing the original 30 study variables into five meaningful components, as explained

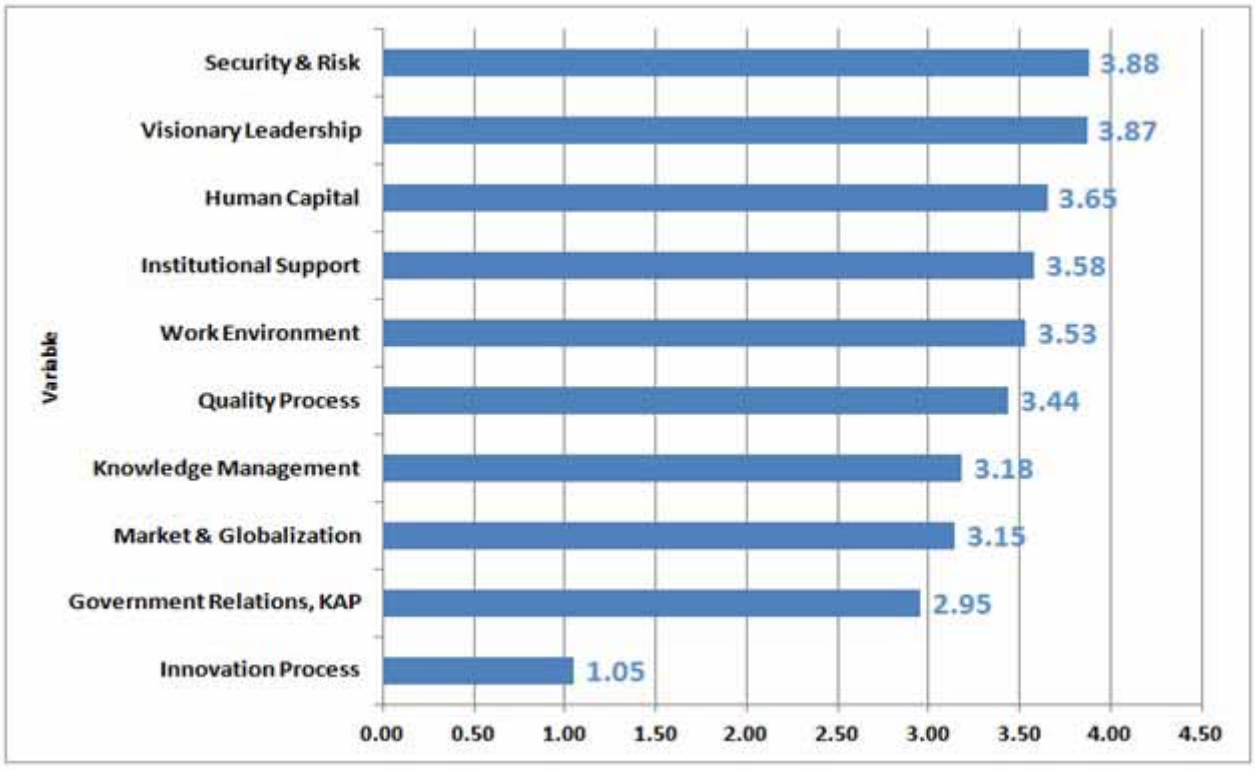


Figure 2: Capability Mean Score Value Secured by ICTS User Companies by of Ten Broad based Factors

earlier. The Rotated Component Matrix values that showed the correlation between the variables probed in the survey and the five latent constructs in Table 9 was used to pick those variables with a correlation value of 0.5 above attributed to each latent constructs. As highlighted in the earlier assumption, at least 5 variables are needed under each latent component for making a meaningful nomenclature.

Rotated Component Matrix

	Component				
	1	2	3	4	5
Visionary Leadership	.622	.211	.115	-.070	.416
Responsive to ICT best practices	.646	.114	.191	-0.24	.471
ICT Innovations	.445	.200	.282	.073	.541
Mobilising financing for ICT	.278	.105	.187	.071	.805
Soliciting Voice of Customers (VOC)	.182	.273	.323	.248	.640
Branding & business networking	.264	.191	.344	.203	.646
ICT Skills & Competencies	.351	.153	.665	.178	.244
Inter-disciplinary skills	.440	.259	.628	.115	.202
Knowledge seeking workforce	.474	.212	.606	.141	.192
Rewards & recognition	.411	.326	.191	.423	.456
Talent retention	.548	.302	.153	.446	.208
Knowledge sharing	.520	.195	.159	.373	.338
Innovation support	.133	.719	.266	.248	.333
R&D and Commercialization	.098	.768	.225	.312	.252
Branding & patenting	.081	.736	.161	.398	.272
Quality and standards	.362	.719	.242	.157	.096
Quality accreditations	.097	.747	.192	.221	-.025
Service level & customer satisfaction	.349	.700	.176	-0.72	.286
Awareness security & risk management practices	.776	.066	.243	.179	.184
Adoption security & risk management practices	.797	.139	.138	.304	.078
Security threats mitigation	.699	.190	.137	.252	.222
Integrated Knowledge Management System	.060	.307	.776	.254	.317
Market & business intelligent	.110	.304	.735	.349	.223
Information & knowledge dissemination	.132	.210	.798	.230	.276
Awareness government incentives	.276	.065	.301	.751	.206
Soliciting Government grants	.109	.297	.171	.838	.152
Networking with Government	.121	.238	.175	.818	.148
Managing global ICT threats	.487	.435	.432	.306	-.083
Pursuing global ICT opportunities	.379	.345	.372	.548	-.195
Coping ICT trade liberalization policies	.322	.430	.399	.587	-0.85

Table 9: Rotated Component Matrix Under Five Factor Loadings

After closely examining the variables, the five components were assigned as follows: Component I – ICT Security; Component II – Branding; Component III – Business Intelligence; IV – Business Efficacy; Component V - Government Relations; see Table 10. Table 10 also shows the variables that are associated with each component, the correlation value between the study variables and the latent constructs as well as the mean score value for each variable and latent component. The results revealed all variables have positive correlations, significantly well above 0.5, indicating strong relationships between the study variables and the latent constructs. For a more meaningful interpretation, the analysis ensured that each latent construct was adequately represented by at least 5 variables.

Latent Constructs	Variables	Component Mean	Correlation
ICT Security	Adoption security & risk management practices	**3.72**	.797
	Awareness security & risk management practices		.776
	Security threats mitigation		.699
	Responsive to ICT best practices		.646
	Visionary Leadership		.622
	Talent retention		.548
	Managing global ICT threats		.487
Business Efficacy	R&D and Commercialization	**3.29**	.798
	Quality accreditations		.747
	Branding & patenting		.736
	Quality and standards		.719
	Innovation support		.719
	Service level & customer satisfaction		.700
Business Intelligent	Information & knowledge dissemination	**3.42**	.798
	Integrated Knowledge Management System		.776
	Market & business intelligent		.735
	ICT Skills & Competencies		.665
	Inter-disciplinary skills		.628
	Knowledge seeking workforce		.606
Government Relations	Soliciting Government grants	**2.99**	.838
	Networking with Government		.818
	Awareness government incentives		.751
	Coping ICT trade liberalization policies		.587
	Pursuing global ICT opportunities		.548
Branding	Mobilising financing for ICT	**3.64**	.805
	Branding & business networking		.646
	Practices for Soliciting Voice of Customers (VOC)		.640
	Administrative Support for ICT Innovations		.541
	Rewards & recognition schems for innovation		.456

Table 10 : Nomenclature and Mean Score Value by Five Latent Constructs,

ICT SECURITY

Ubiquitous and pervasive digital technology has created new demand for ICT security in order to protect the ICT infrastructure and information system services that are produced and used by companies. Globally, acts of aggression and hostile activities such as cyber espionage, malicious software infection, system intrusion, technically complex and sophisticated high scale attacks targeting critical systems have also been on the rise in recent years. Some of these activities are complex and are believed to be state-sponsored. Malware threats are now becoming more devastating and some of them are aimed at critical systems and to steal sensitive data. ICT security threats are not only technical in nature as risks are also in the form of content posted on cyber media such as seditious and defamatory statements that can be detrimental to national security, business development and social harmony as well as the privacy of individual.

The Symantec Internet Security Threat Report: Trends 2012, reported five major areas of concern affecting business security:

i. The report indicates that 50% of all attacks are targeted at small businesses which are easier to infiltrate compared to large businesses. Small businesses mistakenly assume that they have nothing much of value, forgetting that they hold valuable customer information, own intellectual property, and have money in the bank. Moreover, small businesses also tend to lack cyber defense strategies.The white paper reveals that cyber espionage gangs hijack websites of small businesses and lie in wait for their targets, especially big businesses, to visit so that they can infect them.
ii. Malware authors act like a big brother by spying, tracking movements and stealing personal information such as banking particulars, phone numbers, email addresses and other pertinent information with an ultimate goal of making fast money.
iii. Vulnerabilities reported in the mobile operating system have increased by 58% within a year because of the openness of the platform and multiple distribution methods available to applications that can be embedded with malware.
iv. Stuxnet and Elderwood Gang used zero-day vulnerabilities strategy for their attacks, which increased by 14% in 2012.
v. Attribution and motives are not easily determined in hackings, despite people claiming responsibility. For instance, a group calling itself the “Cutting Sword of Justice” claimed responsibility for a malware named Shamoon, aimed at wiping computer hardware drives of energy companies in the Middle East. Similarly, DDoS launched attacks on financial institutions, but it was Izz ad-Din al-Qassam that claimed responsibility. In essence, constant innovation from malware authors and expansion of traditional threats such as spam and phishing attacks into social media and mobile devices warrant due attention in safeguarding online security.

Recognizing the growing cyber threat and market potential, it is imperative for Government and private sector organizations to mobilize resources to R&D, development, testing and manufacturing in relation to security relevant ICT products and services. Indeed as shown in Table # awareness and adoption of security and risk management practices as well as threat mitigation efforts among user agencies in Malaysia are considered is high. This is partly attributed to factors such as visionary leadership, talent retention and knowledge sharing.

In Malaysia, CyberrSecurity Malaysia’s statistics show that fraud constituted 37.5% of cyber crimes followed by intrusion at 32%. Other incidents include cyber harassment, denials of service, intrusions and malicious codes.

Estimated losses as a result of cyber crimes amounted to RM241 million from 2010 to 2012 and the trend is expected to continue.

It is also interesting to note that ICT security has evolved into a billion dollar market, globally worth about USD60 billion in 2011 and growing at an annual rate 10%. The bulk of the expenses is directed at four key areas, namely network security (41%), security operations (18%), data security (18%) and identity and access control (15%).

BRANDING / COMPETENCY AND STANDARDS

The five variables attributed to the branding component are shown in Table 10. Specifically the survey findings revealed that the ICTS user companies provide adequate allocation for accessing new ICT initiatives so that they do not lag behind in embracing new technologies entering the market. Technology upheavals are so rapid that even larger companies that have an inherent affordability find it difficult to keep up. Indeed, as postulated by Gartner the Nexus of Forces entailing the convergence and mutual reinforcement of social, mobility, cloud and information patterns are creating a plethora of new business and social opportunities. Social media is only at the beginning of this journey.

The trend is calling on all senior IT leaders to embrace new changes as their existing architecture is becoming obsolete and to take advantage of the nexus of forces so they can respond effectively. Frost and Sullivan has surmised nine technological areas - pervasive computing, green innovation to zero, smart infrastructure, pay as you use, preventive health care, rise of machines, real time and all time, flexibility manufacturing and cyber warfare – that are poised to change not only the landscapes of ICT Services producers but also that of the ICT Services users in the years ahead. Recognizing these trends the Malaysian government has also outlined six technology focus areas for R&D and commercialization namely cloud computing, e-services, ubiquitous connectivity, security platforms, wireless intelligence and analytics that may be of interest to ICT user companies.

The next factor that warrants due attention is business networking and marketing, which is more a reflection of the innate quality of human capital. ICTS user companies can help to further improve employees' business networking capabilities by providing adequate exposure to learning opportunities such as forums and international conferences and workshops. They can also learn from multinational companies with a strong R&D and innovation presence in the country while also acquiring knowledge from universities through strengthening industry and university linkages pertaining to R&D, innovation, patenting and commercialization endeavours (NEAC, 2010; Wahab, 2012).

Indeed, effective networking and strong relationships are critical for the transfer of technology and knowledge and the exchange of ideas as well as building global business networks (NEAC, 2010; Yu, 2012). Business networking and marketing capability development should not be the sole responsibility of the companies alone. In tandem, the employees should also keep up to date and equip themselves with the ever-evolving information and technology out there (Wahab, 2012; NEAC, 2010; EPU, 2001). They could also participate in Government supported initiatives such as CMMI, PCMM, ITIL, ISO, Green Computing, IAOP Outsourcing, Six Sigma and Lean Six Sigma as well as subject matter specific certifications and accreditations (Nandyal and Ramasamy, 2011; Nandyal, 2003; Pyzdek, 2003).

For branding a product or service, the voice of the customer (VOC) plays a significant part as it helps to identify the true customer needs, demands and requirements. Therefore,

organizations that have aligned their products and services directly with the needs of customers are able to offer the best. Quality and process improvement practices such as Six Sigma or Lean Six Sigma or Design for Six Sigma have explicitly called for the deployment of VOC in the operations of companies.

This will greatly assist in improving competitiveness, increasing market share and improving profitability. Within the life cycle of each product or service, there are a number of touch points when the company interacts with the customer. Each touch point is an opportunity to collect data and to influence customer behavior. Several touch point examples include customer product/service inquiry, customer visits to sales channels, the actual sales transaction, customer service contact, and warranty services. Essentially, VOC data can be collected either reactively or proactively.

The reactive data can be derived from customer complaints, compliments, feedback, hotline data, product returns and/or warranty claims. Not surprisingly, this data is usually negative and although not exactly encouraging, offer valuable insight on weaknesses and represent significant improvement opportunities.

Meanwhile, proactive data collection includes surveys, focus groups, observations and/or test customers. In the current information era social media platforms such as Facebook, Twitter and blogs or dedicated portals can be used to solicit ratings and feedback for products or services. In these instances, it is imperative that the right questions be asked in the right format. Towards this end, companies need to first clearly identify the kind of information they need, the target customers and what the collected data is to be used for so the information can be used to effectively make the necessary improvements and adjustments. Therefore, it's important for companies to strengthen their VOC channels through top-down strategic support so that the VOC solicitation becomes company culture.

Another important aspect is administrative support and adequate resource allocation, where rewards and recognition for innovations will greatly help in branding products and services especially when value added services that can delight customers are incorporated.

BUSINESS INTELLIGENCE

Adequate organizational capability in developing a dynamic business intelligent (BI) system or a knowledge management system (KMS) is imperative for recognizing and detecting changes in policy, market and business dynamics (Lavalle, et al, 2011; Saleh, 2012). Gartner defines BI as an umbrella term that covers the people, processes and applications / tools to organize information, enable access and analyse it to improve decisions and manage performance. In the future, more business decisions will be supported by facts that only analytics can provide; and fewer decisions will be made on the basis of instinct and guesswork (Davenport and Harris, 2007).

With business information increasing over time with a simultaneous increase in complexity, the scope and coverage and the demand for analytic capabilities, especially Big Data Analytics (BDA), is on the rise (TATA, 2012). Besides focusing on traditional structured information, BI supported with BDA is able to undertake data that is found organically within organizations, albeit in an unstructured form. This will require capabilities in areas pertaining to various analytics such as text, context, speech, predictive, prescriptive and embedded analytics (TATA, 2012). As reflected in the Table 11 , on an average only 24.5% of the ICTS user companies deploy big data analytics (BDA), which is increasingly becoming a critical method in culling out business intelligence

ICT Services User Companies	Big Data Analytics	
	Frequency	%
Business & Professional Services	4	57.1
Logistics Services	4	50.0
ICT Services	3	18.8
Distributive Trade Services	2	50.0
Construction Services	1	10.0
Education & Training Services	0	0.0
Environmental Services	1	50.0
Healthcare Services	1	20.0
Advertising Services	0	0.0
Tourism Services	0	0.0
Oil & Gas Services	1	20.0
Other	11	18.0
	Average	24.5

Table 11:

from a company's business and customer database.

As revealed in the survey, many companies do not pay much attention in building such BI and analytics capabilities. This may be due to a lack of understanding on how BI can help in improving internal processes in terms of cost savings, cycle time reductions, identifying opportunity costs, managing technical obstacles in engineering, paving the way for new technology adoption, assessing product relevance, studying market trends and undertaking SWOT analysis, product differentiation analysis as well as to make informed business decisions with real-time data that can put a company ahead of its competitors (TATA, 2012) .

BUSINESS DEVELOPMENT EFFICACY

The analysis showed that Malaysian ICTS user companies are also weak in business development. This variable garnered a mean score value of only 3.29. The variables that are requisitely important and have the highest correlation (0.768) with business development efficacy is research and development and commercialization. To provide strategic focus and direction, it is essential for universities and research institutions to align their R&D endeavors and business development strategies in line with the technology focus areas (TFA) that the Government promulgates in the ICT Roadmap 2012.

The TFAs that are highlighted in the roadmap include the provision of e-services, wireless intelligence, ubiquitous connectivity, big data analytics (BDA), security and platforms and cloud computing. Such alignments are imperative for setting up centres of excellence to enhance the rate of technology development and deployment. More importantly, it will help to decrease the wastage of resources, especially when research and commercialization agencies are involved in areas that have are not priority sectors of are of not interest nationally.

The next important parameter that has high correlation with business development efficacy aspects is quality. As shown in Table 12, three pertinent questions were probed, focusing namely on the awareness of globally recognised quality, standards, process and accreditations as well as the sensitivity of the level and quality of services and customer satisfaction. The results indicated that the

Variables Probed	Mean Score
Awareness on globally recognised quality, standards and processes	3.53
Pursuing globally recognised quality accreditations like CMMI	3.08
Sensitive to service level quality / customer satisfaction practices	3.72

Table 12:

Malaysian ICTS user companies are adequately aware of global standards as reflected in the mean score of 3.5 but the pursuance of such accreditations is rather low, coming in at only 3.08. Nonetheless, sensitive to service level quality and customer satisfaction practices registered a high mean score of 3.72, indicating that Malaysian ICT user companies do listen to the voice of customer (VOC).

Branding and patenting also registered high correlations, as high as 0.736 within the business development efficacy parameters. Nonetheless, detailed tabulation revealed that branding and patenting practices and processes secured a mean score of only 3.07, indicating there is room for further improvement. Specifically, in the ICT user sector the companies can build their brands through innovation activities. Towards this aspiration Malaysian companies in the ICT usage realm ought to embrace the knowledge seeking culture and nurture an entrepreneurial spirit at grass-root level among the Malaysian workforce and school going children at the tender age. Meanwhile, the inhibitors of progress i.e. a low level or private sector participation in research, development and commercialization, the patent culture within the research community, lack of good corporate governance and numerous other factors, also warrant due attention.

GOVERNMENT RELATIONS

Of the five latent constructs derived from the factor analysis, the Government relations component secured the lowest mean score of 2.99; see Figure 2. As in many countries, the Malaysian Government has created a host of support institutions and facilities to create risk capital, provide matching grants, offer business plan development and marketing advice, attract foreign direct investment, furnish R&D investment, set up incubator units that provide space and infrastructure for business beginners and innovative companies, run quality control programmes, carry out export promotions, foster foreign partnerships as well as disseminate information on regulations, standards, taxation and customs duties (Wahab, 2012).

However, in probing Government relations, the survey covered only three key items pertaining to knowledge, awareness and perception, particularly awareness levels on government incentives for ICT development; ability in soliciting Government grants like InnoFund offered by the Ministry of Science, Technology and Innovation (MOSTI); and networking capabilities with mainstream agencies. Table 13 shows the outcome of this probe. It is seen that some companies have reported that developing government ties is not directly applicable to the ICT activities undertaken by them. Nonetheless, between 20 to 30 % have reported that weak Government relations in seeking Government incentives or Government supported research fund or networking with mainstream agencies.

Specifically, the survey probed the knowledge, awareness and perception (KAP) of ICTS companies in seeking incentives, facilities and support services from the named mainstream agencies involved in the development of ICTS activities. The investigation revealed that all the five variables under Government relations secured low mean scores, ranging between

Variables	KAP on Government Incentives		Ability in Solicing Government ICT Grants		Networking Capabilities with Mainstream	
Likert Scale	**Frequency**	**Percent**	**Frequency**	**Percent**	**Frequency**	**Percent**
Not Applicable	3	3.1	11	11.5	8	8.3
Very Weak	2	2.1	12	12.5	10	10.4
Weak	19	19.8	15	15.6	14	14.6
Average	31	32.3	24	25.0	25	26.0
Strong	28	29.2	24	25.0	26	27.1
Very Strong	13	13.5	10	10.4	13	13.5
Total	96	100.0	96	100.0	96	100.0

Table 13

2.24 to 2.38. This dismal showing reflects the poor working relationship between the Government and industry. There could be a number of reasons for this, with two standing out clearly. One is the lack of awareness and adequate knowledge on the incentives and facilities offered by the Government and the other is the rigid bureaucratic environment that often an encumbrance and a deterrent. If poor working relationships prevail between the Government and private companies, especially with industry associations that represent the interests of these companies, it is highly probable that the companies will lack the awareness or knowledge of the types of institutional services and incentives offered by the government agencies (Wahab, 2012). Such problems can be only overcome provided Government agencies play a proactive role in sharing and disseminating information, as opposed to waiting for the industries to search them out. It will be a lot easier and convenient for Government agencies to make the first move whenever new policies, programmes, strategies or business incentives are introduced. The challenge is that Government agencies typically tend to play a reactive role unless a mindset change occurs. In India for example, the proactive involvement of the Government made the country one of the leading software exporters of the world (Salmenkaita and Salo, 2002; Carmel, 2003). However, reciprocal willingness and responsive participation of industry players are also critical. Dealing with a rigid, bureaucratic and unfriendly government agency can be a monumental task (Maniam and Halimah, 2008). Sometimes, tough and tense situations arise when private sector customers are not accorded the right treatment or cooperation from the civil service counters. Consequently, customers may refrain from making future visits in search of support services from Government agencies.

This age old bureaucratic issue has to be seen from a broader context of "re-inventing the quality of the civil service", which has a broader connotation (Maniam and Halimah, 2008). It is not only quality, standards, productivity and service that have become key words in the lexicon of public sector reform, but also includes de-bureaucratization and the implementation of good governance elements promoting transparency, accountability and responsibility, including public participation in decision making processes (Maniam & Halimah, 2008). Despite increasing prominence given to these concerns in line with the rising expectations and changing perceptions of customers, who constantly crave for the delivery of high quality services, much of the challenges dealing with government agencies still linger. The customer relationship management issue in the civil service can be handled effectively by increasing the level of quality service, continually improving services, implementing the monitoring and evaluation of service performances, and most importantly changing the mindset of service providers (Maniam & Halimah, 2008). These clarion

calls are not new but they can definitely be further enhanced through the deployment of e-Government services. This will not only improve the efficacy of routine tasks, but also provide information and networking facilities to a wider public audience at a greater comfort level and with minimized bureaucratic interactions.

CONCLUSION

One of the fundamental requisites for any development of progress is the innate quality of human capital. In developing top-notch ICT platforms, services and competencies, this same requirement is fundamental as well. This survey probed three areas pertaining to the quality of human capital. Table 14 shows that human capital in the ICTS user environment among the companies covered indicated a high capacity for acquiring ICT skills and competencies, good project management and inter-disciplinary skills and a responsive, innovative and knowledge seeking culture.

Nevertheless the capability in human capital especially in relation to resilience, confidence and maturity can be further enhanced by providing personnel adequate exposure to learning platforms such as forum, international conferences and workshops and hands on experience with multinational companies which employ best practices and have a good work culture, R&D and innovation base. Knowledge can also be further acquired from universities, pursuant of course to a strong link between industry and university pertaining to R&D, innovation, patenting and commercialization endeavours as well as the transfer of technology (NEAC, 2010; Wahab, 2012). It also helps if employees in the ICT user sector are interested and motivated to achieve global standards in process and quality improvement activities (Wahab, 2012; NEAC, 2010; EPU, 2001). In tandem, Government's support in pursuit of CMMI, PCMM, ITIL, ISO, Green Computing, IAOP Outsourcing, Six Sigma and Lean Six Sigma as well as subject matter specific certifications and accreditations (Nandyal and Ramasamy, 2011; Nandyal, 2003; Pyzdek, 2003) for ICTS user sectors also need to be extended.

Without appropriate recognitions and accreditations, it is quite difficult for ICTS companies to bid for deals in the international market, especially in the United States and Europe where stringent conditions prevail on quality acceptance. It is also conjectured that Malaysian ICTS companies may lack a sense of urgency in equipping themselves with adequate capacities and capabilities in harnessing the fast moving globalization and market liberalization phenomena (Wahab, 2012). With an increasing number of countries liberalizing their markets for foreign investments and business participation, countless global opportunities are emerging. Also, the playing field of the ICT business is being leveled between developed and developing countries, as new inventions, creations and innovations are proliferating at an unprecedented rate. The early bird catches the worm, so it is up to the individual companies to equip themselves to effectively reap these benefits and opportunities of this advancing technological age. If a lackadaisical attitude continues to prevail in the business sector, it could lead to a disaster when competitors take over existing businesses by developing business models that are better, leaner and more attractive

Variables Probed	Mean Score
Adequacy of ICT Skills & Competencies	3.60
Project management and inter-disciplinary skills	3.65
Responsive, Innovative and Knowledge seeking workforce	3.71

Table 14

to consumers. Anderson (2011) cited the best medicine to use in the fight against such complacency is developing a sense of urgency that can create an internal alertness, focus, business re-engineering and continuous improvement processes.

More importantly, businesses need to recognize that change is continuous and not episodic. For instance, the Research in Motion Company grew exponentially from a scrappy upstart to become a market leader with their BlackBerry phones that provided e-mail push technology. However, in less than two years, they lost out to Apple, which focused on delivering an entirely new kind of product supported with multimedia content and highly superior features that appealed to the technology-savvy Y generation. However, both Apple and Blackberry have realized a significant portion of their market share has been taken up by the Android operating system – a classic example of complacency in business.

REFERENCES

1. Arikan, A.M. and McGahan, A.M. (2010). 'The Development Capabilities in New Firms. *Strategic Management Journal* 31 (1): 1-18.
2. Azzman, Shariff adeen (2000). *The Changing World: ICT and Governance. NITC Malaysia Publication, 2000, Paper I. Access, Empowerment and Governance In Th e Information Age: Building Knowledge Societies Vol. 1. p 1-14.*
3. Bakru, Anjali and Grant, Robert M. (2010). 'Creating Organizational Capability in New Businesses: Building Sets of Complementary Capabilities".
4. Bhatnagar, S. (2006). *"ICT to Build a Vibrant Knowledge Society". Information for Development (i4d), Volume IV, Number 3, March 29-30.*
5. Breshnaham, Timothy F., Brynjolfsson, Erik and Lorin M. Hiit (1999). Information Technology Workplace Organization and the Demand for Skilled labour: Firm-level evidence, *Working Paper 7136*, National Bureau of Economic Research.
6. Buenstorf G. Klepper S. (2005). Heritage and agglomeration: The Akron Tire cluster revisited. *Working paper*, Carnegie Mellon University, Pittsburgh, PA.
7. Carlton, Darry l (2012). Th e Nexus of Forces: Social, Mobile, Cloud and Information. Gartner Research. Paper published in the *ICT Strategic Review 2012/13: Innovation for Digital Opportunities.*PIKOM publication series.
8. Carmel, Erran (2003). The New Software Exporting Nations. Success Factors. *The Electronic Journal on Information Systems in Developing Countries (EJISDC) 13, 4, 1-12.*
9. Castells, Manuel. (2001). *The Internet galaxy.* Oxford & New York: Oxford University Press.
10. Christensen, Clayton (2011). *The Innovator's Dilemma: The Revolutionary Book that will change the Way You Do Business.*
11. Curry, E., Guyon, B., Sheridan, C. and Donnellan, B. (2012). "Developing a Sustainable IT Capability: Lessons From Intel's Journey," *MIS Quarterly Executive*, vol. 11, no. 2, pp. 61–74.
12. De Feo, Joseph A.; Barnard, William (2005). *JURAN Institute's Six Sigma Breakthrough and Beyond - Quality Performance Breakthrough Methods.* Tata McGraw-Hill Publishing Company Limited. ISBN 0-07-059881-9.
13. Drucker, Peter F. & Maciariello, Joseph (2008). *Management revised edition.* An imprint of HarperCollins Publishers. New York.
14. EPU (2001). *The Third Outline Perspective Plan: 2001-2010 (OPP3: 2001-2010).* Economic Planning Unit, Prime Minister's Department, Putrajaya, Malaysia.
15. Ethiraj S.K.; Kale P,; Krishnan M.S. and Singh J.V. (2005). Where Do Capabilities Come from and How do They Matter?' A Study in the Software Services Industry. *Strategic Management Journal 26 (1):* 25-45.
16. Field, A.P. (2005). *'Discovering Statistics Using SPSS (2nd Edition)'.* London: Sage.
17. Finden-Browne, Chris (2007). An Integrated Process Model as a Foundation for ITSM. SMSG IBM Global Services. BCS Service Management Specialist Group.
18. George, Michael (2003). *'Lean Six Sigma for Service: How to Use Lean Speed and Six Sigma Quality to Improve Services and Transactions'.* McGraw Hill publications.
19. Graham, Mark. (2008). *Warped Geographies of Development: The Internet and Theories of Economic Development. Geography Compass, 2(3),* 771-789.
20. Hair, Joseph F., Andersan, Rolph E., Tatham, Ronald L. and Black, William C. (1992). *'Multivariate Data Analysis with Readings'.* Third Edition by MacMilan Publishing Company, New York.
21. Hair, Joseph F., Black, William C, Babin, Barry J., Andersan, Rolph E., and Tatham, Ronald L. (2006). *'Multivariate Data Analysis'*. Sixth Edition by Pearson Prentice Hall, New Jersey.
22. Helfat, C.E., and Peteraf M.A., (2003). The Dynamic Resource Based View: Capability Life Cycles. *Strategic Management Journal 24 (10):* 997-1010.
23. Hollis, Nigel (2008). *The Global Brand.* Published by Palgrave Macmillan Ltd , New York.
24. IAOP (2013): *IAOP website.* http://www.iaop.org/.
25. IBM (2012). 'Social Business: Advent of New Age' IBM Institute paper published in the *ICT Strategic Review 2012/13: Innovation for Digital Opportunities.* PIKOM publication series.
26. ITIL (2013): *ITIL website.* http://www.itil-offi cialsite. com/ home/home.asp.
27. 27. Kanter, R.M. (1989) Swimming in new streams: Mastering innovation dilemmas. *California Management Review*, 45–69.
28. Kazanjian RK and Rao H. (1999). Research note: The Creation of Capabilities in new Ventures – a longitudinal study. *Organization Studies 20(1):* 125-42;
29. Kelchner, Luanne (2012). *The Importance of Organizational Capability. By Demand Media* (http://smallbusiness.chron.com/ importance-organizational-capability-13295.html).
30. Keller, Paul A. and Keller, Paul (2010). *Six Sigma Demystified.* McGraw-Hill Professional. p. 40. ISBN 978-0-07-174679-3. Retrieved 20 September 2011.
31. Knight, Gary A. and Cavusgil, Tamar S. (2004). 'Innovation, Organizational Capabilities, and the Born-Global Firm'. *Journal of International Business Studies (2004) 35*, 124-141. Palgrave Macmillan Ltd.
32. Lavlle, Steve, Hopkins, Michael, Lesser, Eric, Shockley, Rebecca and Kruschwitz, Nina (2011). Analytics: The new path to value: How the smartest organizations are embedding analytics to transform insights into action. *IBM Global Business Services. Business Analytics and Optimization.* Paper published in the *ICTStrategic Review 2011/12: Transcending into High Value.* PIKOM publication series.

33. Lawson, Benn and Samson, Danny (2001). 'Developing Innovation Capability in Organizations: A Dynamic Capabilities Approach'. *International Journal of Innovation Management Vol.5, No 3 (September 2001)* pp. 377-400. Imperial College Press.
34. Leroy, Coryea R.; Carl E. Cordy; (2006). *Champion's Practical Six Sigma Summary.* Xlibris Corporation. p. 65. ISBN 978-1- 4134-9681-9. Retrieved 20 September 2011.
35. Liu, Shujie, Onwuegbuzie, Anthony J. and Meng, Lingqi (2011). 'Examination of the score reliability and validity of the statistics anxiety rating scale in a Chinese population: Comparisons of statistics anxiety between Chinese college students and their Western counterparts'. *Journal of Educational Enquiry, Vol. 11, No. 1, 2011*, 29-42.
36. Mansor, Dzahrudin (2012). 'Embracing the consumerization of IT to enable workplace transformation'. *Microsoft Malaysia paper published in the ICT Strategic Review 2012/13: Innovation for Digital Opportunities.* PIKOM publication series.
37. Nair, Mahendhiran (2007). 'Th e DNA of the new economy". *Economic Bulletin, Volume 8*, 27-59.
38. Nandyal (2003). *"People CMM"*, Nandyal, R.S. Tata McGraw- Hill, 2003.
39. Nandyal, Raghav S.; Ramasamy, Ramachandran. (2011). Building a mature software industry: Multidisciplinary strategy with CMMI constellations, PCMM and Six Sigma. Paper published in the *ICT Strategic Review 2011/12: Transcending into High Value.* PIKOM publication series.
40. NEAC (2010). *New economy model (NEM) for Malaysia.* National Economic Action Council (NEAC), Putrajaya, Malaysia.
41. Nerkar A. and Parachuri, S. (2005). Evolution of R&D capabilities: Role of knowledge networks within a firm. *Management Science 51(5):*771-785.
42. Nonaka I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science 5(1):* 14-37.
43. PIKOM (2013). *ICT Job market outlook in Malaysia June 2013.* PIKOM salary report annual series, edited by Ramasamy Ramachandran.
44. Prahaland, C. and Hamel G. (1990).' The core competence of the corporation'. *Harvard Business review, 66*, 79-91.
45. Prencipe A, and Tell F. (2001). Inter project learning: processes and outcomes of knowledge codification in project based firms. *Research Policy 30(9):* 1373-1394.
46. Pyzdek, Th omas (2003). Th e Six Sigma Handbook. Revised and expanded. *A Complete Guide for Green Belts, Black Belts and Managers at all levels.* McGraw-Hill publication.
47. Rajendra, Mathew(2012). 'Green jobs for a low carbon economy: Nurturing the next-gen green collar IT professions. *Green computing Initiative paper published in the ICT Strategic Review 2012/13: Innovation for Digital Opportunities.* PIKOM publication series.
48. Ramasamy, Ramachandran. (2008). Measuring information development in the new millennium. *Thesis submitted in fulfillment of the requirement for the Degree of Master of Philosophy.* Multimedia University, Cyberjaya, Malaysia.
49. Rasiah, R. (2009). *Expansion and slowdown in Southeast Asian electronics. Journal of Asia Pacific Economy, 14(2):* 123-137.
50. Saleh, Shaifubahrim (2012). Prelude: Disruptive innovation the way forward for high value adding economy: *Prelude chapter published in the ICT Strategic Review 2012/13: Innovation for Digital Opportunities.* PIKOM publication series.
51. Schienstock, Gerd (2009). 'Organizational capabilities: Some reflections on the concept' *Intangible Assets and Regional Economic Growth (IAREG) Working Paper 1.2c.*
52. SEI (2013). *CMMI website.* http://www.sei.cmu.edu/cmmi/
53. Tapscott, Don (1997). *Growing up digital: The rise of the net generation.* Published June 1st 1999 by McGraw-Hill Companies (first published 1997).
54. Timm, Neil H. (2002). *Applied multivariate analysis.* Springer, New York.
55. Wahab A., Amirudin; (2012) 'Essence of ICT roadmap 2012 for innovation driven growth'. *Paper published in the ICT Strategic Review 2012/13: Innovation for Digital Opportunities.* PIKOM publication series.
56. Wahab A., Amirudin; Ramasamy, Ramachandran (2011) 'Endogenous growth through ICT enabled innovation: A Malaysian strategy' *Paper published in the ICT Strategic Review 2011/12: Transcending into High Values.* PIKOM publication series.
57. Zollo, M., and Winter, S.G. (2002). Deliberate learning and the evolution of dynamic capabilities. *Organization Science 13(3):* 339-51.
58. (TATA, 2012). Gartner's business analytic framework published in *Future Proofing the Organization through Analytics by TATA Consultancy Services.*
59. Van Esch W., Gerritsen M., de Groot C., Vogels M. and Boesen N. (2010). *The Sector Approach version 2.0: Getting Results as the World Gets Flatter.* http://capacity4dev.ec.europa.eu/paperssector- approaches-version-20
60. Boesen, Nils (2008). *Working towards Supporting Capacity Development through Joint Approaches - Emerging lessons and issues.*
61. (OECD, 2010) Capacity Development at the Sector Level. *Discussion Note.*
62. Maniam, K. & Ha;imah, A. (2008). ICT to enhance administrative performance: A case study from Malaysia: *International Journal of Business & Management (IJBM), 3(5)*, 78-84.
63. Anderson, Dave (2011). Ten truths about complacency. *Dealer Business Journal*, Volume 8-Issue 6, page 14.

CHAPTER 9

SOCIAL NETWORK TECHNOLOGY AND SOCIOECONOMIC BEHAVIOUR IN MALAYSIA

EWILLY LIEW J.Y
ewilly.liew@monash.edu

SANTHA VAITHILINGAM
santha.vaithilingam@monash.edu

MAHENDHIRAN NAIR
mahendhiran.nair@monash.edu

Monash University Sunway Campus Malaysia

MONASH University
Sunway campus

ABSTRACT

Social network technology (SNT) has advanced from traditional information communication technology (ICT) to become the hallmark of online social interaction. With better access to the network intelligence, SNT can act as key enabler to motivate socially connected users for greater reach and richness of connectivity, entertainment, knowledge resources, business avenues and opportunities and digital lifestyle. This study shows that while Facebook has become an integral part of social communication among Malaysian users, they are also increasingly aware of the economic and utilitarian benefits of using Facebook. Results also show that users' utilitarian use is about half their hedonic use of Facebook. Further, the empirical results show that the use of Facebook for businesses has yielded positive economic outcomes in terms of increased productivity, profit, customer attraction and retention. This study argues that change of perception among users, that is having positive perceived socio-economic benefits of using Facebook, is vital to motivate users from hedonic use to more advanced use for economic and utilitarian purposes. Obstacles that hinder non-users from benefiting from the use of Facebook include privacy and security concerns, lack of interest and inadequate time to use. Strategies to encourage more advanced use of SNT that will enable the diverse population in Malaysia to leapfrog to a high income economy are discussed in this paper.

Keywords: *Social Network Technology, Facebook, Socio-economic Benefits, Utilitarian Use, Hedonic Use*

I. INTRODUCTION

Rapid innovation in information and communication technology (ICT) has enabled greater convergence of various digital communication platforms. Among the ICTs, social networks technology (SNT) such as Facebook, Twitter and Google+ has emerged to become key platforms for facilitating online social interaction. Better access to this network intelligence has enabled global communities to enjoy richer digital lifestyle in the form of greater reach of social connectivity, entertainment, information, knowledge resources and new opportunities for businesses. SNT has more recently evolved into a strategic tool for communication, collaboration and commerce across the globe. Its widespread geographical flexibility and scalability facilitate knowledge and resources distribution more efficiently, enabling new generation digital communities to enhance their reach to resources for better socio-economic status.

Many developed countries have experienced positive spillover benefits of SNT for wealth creation and social capital development (Giannakos, Chorianopoulos, Giotopoulos, & Vlamos, 2013; Johnston, Tanner, Lalla, & Kawalski, 2013; Liew, Vaithilingam, & Nair, 2014; Shin, 2013).

Figure 1 shows that those countries with high Facebook penetration rate also record high wealth accumulation with increasing returns to scale. This implies that Facebook penetration rate is strongly correlated with wealth creation opportunities, close to 50 per cent of the variation of national wealth (measured by real gross domestic product; GDP) is explained by variation in the penetration rate of Facebook. Note that Facebook penetration rate has increasing returns to scale to wealth – that is a 1% increase in Facebook penetration will lead to more than 1% increase in national wealth. This has encouraged developing countries to view SNT as a leap-frogging technology for enhancing their socio-economic status.

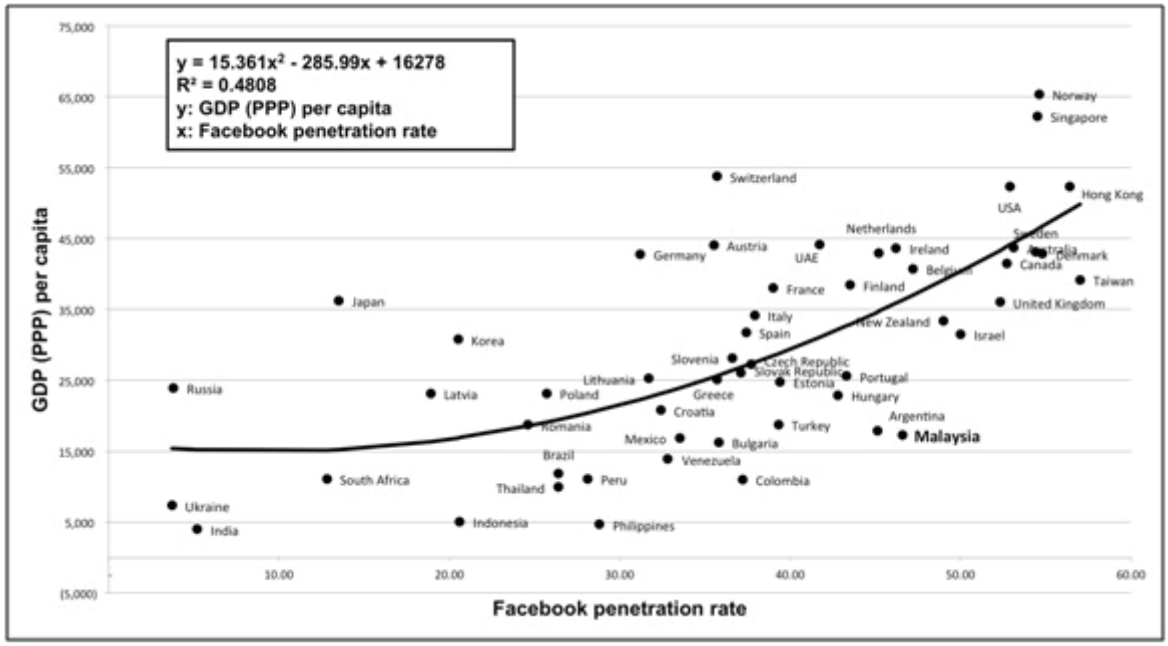


Figure 1: Wealth Accumulation with High Facebook Penetration Rate
(Data Source: Internet World Stats, 2014b; World Economic Forum, 2014)

However, Liew, Vaithilingam, and Nair (2014) argued that individuals' perception on the socio-economic benefits of Facebook may differ as the enabling environment supporting the adoption and use of SNT vary based on a country's development stage.

While SNT is widely accepted for social communication and entertainment, other uses of SNT for information seeking and commerce, however, have not been widely recognized (Liew et al., 2014; Shin, 2013; Stefanone, Hurley, & Yang, 2013) and may be more vulnerable to the external enabling environment of a country. For example, developing countries continue to face challenges of network connectivity interruption due to poor quality ICT infrastructure and ineffective digital regulatory governance (Datta, 2011; Liew et al., 2014; Sharma & Gupta, 2009). Further, affordability could be an issue since access to SNT requires access to the Internet infrastructure, the cost of which is closely associated with the quality of connection (Liew et al., 2014).

This accounts for why some users are more conscientious to the use of SNT for economic and utilitarian purposes, or even not using it, for fear of negative network externalities such as breach of trust (Gefen, Karahanna, & Straub, 2003; Lu & Zhou, 2007; Wu & Chen, 2005), privacy (Gross & Acquiti, 2005; Stutzman, Capra, & Thompson, 2011; Timm & Duven, 2008), security (Flavián & Guinalíu, 2006) and cybercrimes (Sharma & Gupta, 2009). Low or non-adoption may also be attributed to people's lack of awareness of the socio-economic potentials of SNT or lack of readiness to fully engage its features, functions and applications for creating real socio-economic benefits.

This study focuses on Facebook, the largest SNT with 1.32 billion monthly active users (Facebook, 2014). Along with Twitter and YouTube, these are the top-three SNT considered as the cornerstones of most social media strategies for commerce (Vollmer & Premo, 2011). Though economic use of Facebook has been previously sidelined by its popular social use, the former is now gaining momentum as Facebook ventures more pervasively into commerce. In 2012, Facebook filed for a USD5 billion initial public offering (IPO) and valued the company at USD104 billion, making Facebook the most valuable company in the United States (Protalinski, 2012a, 2012b). Facebook's financial statements for the six-month period ended 30 June 2014 reported total revenue of USD5.412 billion, a 65 per cent increase from same period last year, USD2.68 billion of which was generated through advertising alone (Facebook, 2014). Other statistics estimated that Facebook's advertising revenue would reach USD 12.6 billion in 2008 across desktop, mobile and Facebook exchange platforms (Statista, 2014c). Through Facebook-Microsoft partnership, the information seeking experience on Facebook is also greatly enhanced and personalised by the Bing's search engine, where web results would appear alongside with social information (people, photos, places, interests) from Facebook.

This study argues that the economic and social benefits of SNT should not be viewed as mutually exclusive, but rather both can progress in tandem with SNT reaching wider and richer audience across the world. More often than not, users who have experienced the social benefits of Facebook will be more aware of its economic potentials and opportunities. Such positive perceptions on the economic benefits of Facebook will lead users to be more engaged with the utilitarian features, functions, or applications of Facebook and consequently creating actual social and economic values for themselves. Nair (2010) also observed "people who are ICT savvy tend to use the digital medium more regular than others to create value for themselves in the form of accessing information, knowledge and purchasing products and services" (p. 198).

Malaysia, a rapidly developing country with high SNT usage and aspiration to be an innovation-driven economy is at the crossroad of becoming a knowledge-intensive society. More than 90 percent of the Malaysian web population spent one in every three minutes online (Ramachandran & The National ICT Association of Malaysia, 2012; Statista, 2014d). Facebook is the leading SNT in Malaysia, and the country is ranked 9th in the Asian region (Statista, 2014a) with its total Facebook users of 13, 589, 520 as of December 2012 (Internet World Stats, 2014a). With its 19 million Internet users, Malaysia is ranked 11th in the Asia Pacific region as of January 2014 (Internet World Stats, 2014a; Statista, 2014b).

While Malaysia records one of the highest Facebook penetration rates and is located in a region with the most active users, Figure 1 show that the wealth in Malaysia is relatively lower than other countries with similar Facebook penetration rates. This implies that Malaysians are not maximizing the use of Facebook for economic benefits compared to their counterparts with similar Facebook penetration rates such as Netherlands, Ireland and Belgium. Thus this study will examine the social and economic use behaviour of Facebook through understanding users' perceived purposes of using Facebook and their actual use of its features, functions or applications.

This study also seeks to identify key factors that encourage or hinder the adoption of Facebook in Malaysia. Results from this study will provide valuable insights into the key policy initiatives to enhance the adoption and use of Facebook across diverse groups of population in Malaysia. The study will also highlight the potential of Facebook for utilitarian purposes by addressing the following question. How do we tap the huge potential of SNT for utilitarian purpose by moving the current users up the value chain from hedonic use to utilitarian use? The paper is structured as follows. Section 2 provides a brief review of key national ICT policies to better understand the current trends of SNT in Malaysia. The conceptual framework of this study is outlined in Section 3. Section 4 and 5 presents the empirical methodology and key findings of the study. Section 6 discusses key policy implications and strategies to improve the adoption and use of Facebook for social and economic development of the communities. Finally in Section 7, concluding remarks are provided.

2. KEY NATIONAL POLICIES IN MALAYSIA

With information revolution transforming the global economy, the Malaysian government introduced a series of initiatives under the 7th Malaysia Plan in efforts to transition the country from a production-driven to information-driven economy. In view of this transformation, the National Information Technology Council (NITC) was formed in the early 1990s. National Information Technology Agenda (NITA) was rolled out by the NITC in 1996 as part of the national informatisation strategy to integrate ICT into every facet of Malaysian lifestyle. NITA focused on transforming the nation progressively from information-driven to knowledge-driven through the use of ICT.

The convergence of IT and communication technology led to the first Communications and Multimedia Act being enacted in 1998. Under this Act, the Malaysia Communication and Multimedia Commission (MCMC) were established to ensure effective regulatory environment for ICT was in place to support the development of a sound and resilient national digital ecosystem. More recently, Malaysia Personal Data Protection Act (PDPA), the first data privacy legislation in the ASEAN region, became fully effective in 2013 across the communications, banking and financial, insurance, healthcare and other industries.

While much improvement is needed in its enforcement, the existence of this Act proved a significant milestone for better privacy protection in the country.

Increasing demands for high-speed information flow have called for government intervention in the diffusion of broadband services. In 2004, the National Broadband Plan (NBP) was rolled out to systematically deploy broadband services across the country. The initiative was followed closely by a five-year plan called the Malaysian Information, Communication, and Multimedia Services (MyICMS886, 2006 – 2010) in eight service areas, eight infrastructure areas and six growth areas to strategically coordinate the development of advanced ICT infrastructure that supported an increasing converging Internet, mobile phones and broadcasting platforms. Under this plan, infrastructure that supported multiservice convergence networks emerged and among them included high speed broadband, 3G cellular networks, satellite networks, as well as next-generation Internet protocol (IPv6), Universal Service Provision (USP), home internet adoption, information and network security, competence development, product design and manufacturing.

In 2007, National Broadband Initiative (NBI) was formulated to intensify and support the MyICMS886 plan. The aim is to provide broadband services to all segments of the population. As part of the NBI initiative, two flagship projects namely, Broadband for General Population (BBGP) and High Speed Broadband (HSBB) programs were introduced to complement the supply side initiatives. MCMC spearheaded these bold initiatives envisioning "Broadband for All" Malaysians in urban, semi-urban, rural and even remote areas.

The HSBB program was regarded as a catalyst for connecting homes and businesses to nationwide next-generation network (NGN) i.e. 'broadband superhighway' via new fiber connections, beginning in high economic impact areas such as the inner Klang Valley region (MCMC, 2010). The demand side initiatives of the NBI were to create greater awareness on the benefits of use of online contents and portals such as the e-government, e-education and e-commerce. Other demand side initiative included ensuring various incentives in place to encourage people to use broadband by making sure it was affordable and tax deductions were given to encourage greater use of this new medium of communication.

The Malaysia's Internet penetration rate was reported at 61 per cent in 2011 (Economist Intelligence Unit, 2011). The subscription trend is increasing for broadband Internet, Asymmetric Digital Subscriber Line (ADSL) and Worldwide Interoperability for Microwave Access (WiMAX). To ensure the poor are not left behind in the move to become an information-savvy nation, the government has also established several public facilities for Internet access and among them included new 339 1Malaysia Internet centres (PI1M), 99 community broadband libraries (CBL), 1 million 1Malaysia netbook distribution, 4210 kampung tanpa wayar (KTW) (wireless villages), and 824 public cellular towers.

Through these efforts, the government anticipated the broadband speed to increase from current average of 5.8Mbps to 50Mbps by 2018 (The Star, 2014). The government also envisioned developing an advanced ICT ecosystem that will increase Malaysian's global competitive advantages, particularly of the bottom 40% of the population (Nair & Vaithilingam, 2013; Performance Management and Delivery Unit (PEMANDU), 2010a, 2010b). This vision is incorporated as part of the Government Transformation Program (GTP) and Economic Transformation Program (ETP) under the 10th Malaysia Plan.

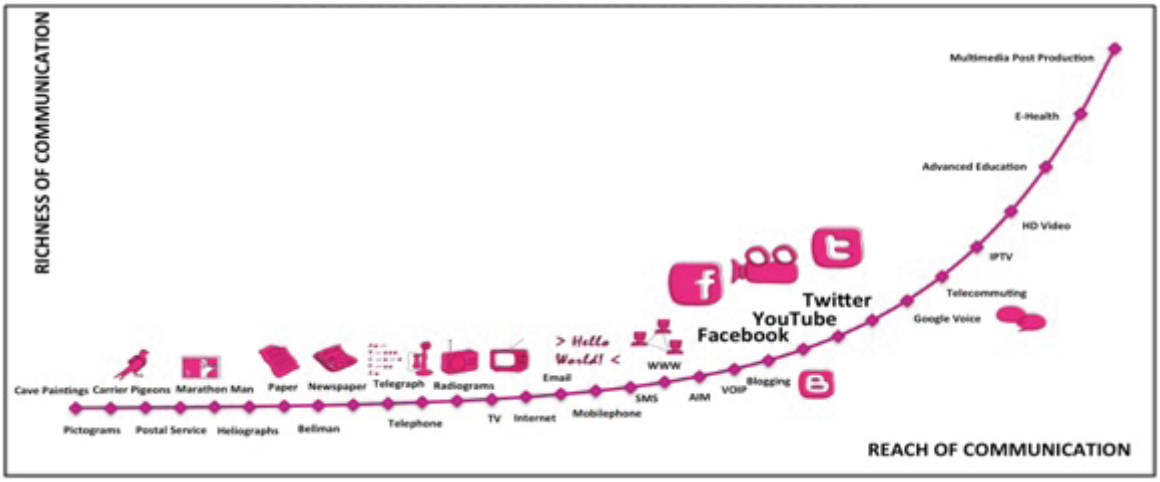


Figure 2: The evolution of communication technology

(Note: Data and graphical source of the historical timeline of various communication technology were obtained from Jasmin, 2012; Malaysian Communications and Multimedia Commission (MCMC), 2013)

Figure 2 shows the evolution of communication technology. The hallmark of SNT, Facebook is strategically positioned in between of traditional information resources via email servers, websites, portals, file sharing, VoIP, blogs and the more advanced digital media, multimedia interactive system, e-education, e-hospital. This allows Facebook to become strategically effective in bridging the obsoleting technology and the more advanced high bandwidth applications.

While advanced content development and excellent broadband services are vital in building an advanced ICT ecosystem, the role of SNT is two-fold. Firstly, SNT can act as a "meeting-point" to build stronger social networks around every user and connect them to the innovation value chain, both locally and globally. Secondly, SNT can motivate these socially connected users to be more engaged in using the seemingly low-value added features, functions, and applications of SNT towards generating higher productivity, social capital, and wealth. This is plausible in Malaysia, which is well known for its heavy online social networking activities (comScore, 2011) and higher number of Facebook friends per user (CNN, 2010). The 91 per cent of the Malaysia's Internet users who are social media savvy also found to have outpaced others in the utilitarian use of SNT such as search navigation, photos, multimedia and blogs (Ramachandran & The National ICT Association of Malaysia, 2012).

Facebook integrates separate social media services such as email, instant messaging, chat, photo and video sharing, forum, blog, broadcasting, personal homepage, news feed, webpage or URL bookmark through a range of applications, features, and functions all in one digital platform (Boyd & Ellison, 2008; Cardon, 2009; Liew et al., 2014). Along with rapid expansion of OpenID, single sign-on (SSO) authentication, application program interface (API), and cloud computing framework, SNT has advanced towards constructing more complete and complex social graph of its users to better connect them between networks and other services in the broader Web environment. Pervasive use of SNT is increasingly observed among the worldwide communities for deeper networking, sharing, discussing, and publishing beyond the boundaries of closed website, discrete login, and physical devices.

3. CONCEPTUAL FRAMEWORK

In this section, the conceptual framework of the study is discussed. This study will identify key factors that encourage the adoption and use of Facebook among users. The focus is on users' perceived socio-economic benefits of Facebook, and their use behaviour in meeting their perceptions and creating socio-economic value for themselves. Figure 3 shows the conceptual framework for this study adopted from Liew, Vaithilingam, and Nair (2014).

This study argues that "adopters" may use Facebook casually or some may remain inactive after adopting it (Facebook, 2011; Liew et al., 2014). Unless they perceive that some socio-economic benefits can be derived from using Facebook, they will not become "repeaters" of using it regularly to generate real socio-economic benefits for themselves. User perceived socio-economic benefits is defined as "a person's self-evaluation or perception on the degree to which one expects to derive real socio-economic benefits of using Facebook" (Liew et al., 2014; p. 348). Positive perception and a sense of purpose increase the possibility of realising true benefits through targeted use of certain features, functions, or applications on Facebook. Thus, encouraging the adopters to become repeat users (Liew et al., 2014; Shih & Venkatesh, 2004).

Studies have found that the use of Facebook can be generally categorised into utilitarian use and hedonic use. Utilitarian use refers to the use of Facebook through which users attain instrumental value for achieving productivity needs (Liew et al., 2014; Van Der Heijden, 2004). Hedonic use refers to the use of Facebook through which users attain self-fulfilling value for achieving personal needs (Liew et al., 2014; van der Heijden, 2004). The utilitarian use of Facebook is broadly classified as business development and information seeking activities, while the hedonic use of Facebook is related to socialisationsocialisation and entertainment.

This conceptualisation of utilitarian use and hedonic use of Facebook is consistent with existing social network literature (Gibbons, 2004; Tichy & Fombrun, 1979; Umphress, Labianca, Kass, & Scholten, 2003; Van Der Heijden, 2004). While many studies believe that Facebook is more for hedonic-oriented use (Hu, Poston, & Kettinger, 2011; Sledgianowski & Kulviwat, 2009; Theotokis & Doukidis, 2009), recent studies increasingly suggested that SNT such as Facebook is "dual information technology which is both utilitarian- and hedonic-oriented" (Ernst, Pfeiffer, & Rothlauf, 2013, p. 3; Liew et al., 2014).

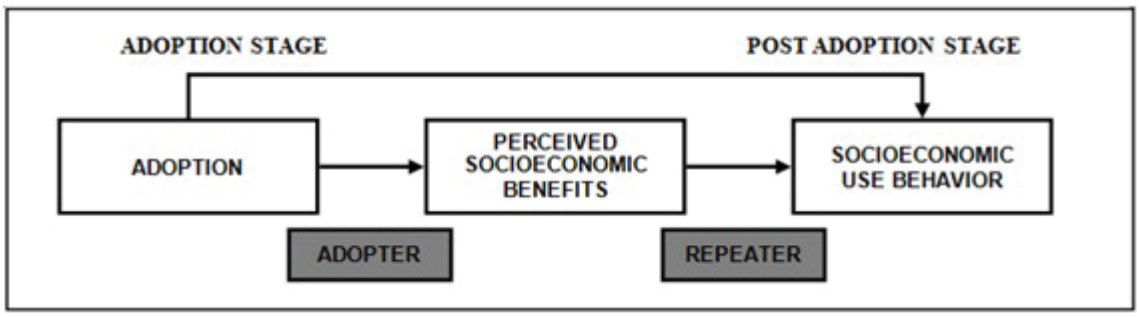


Figure 3: Conceptual Framework
(Source: Liew, Vaithilingam, & Nair, 2014)

4. EMPIRICAL METHODOLOGY

This section examines the hedonic and utilitarian use behavior of Facebook. Data for this study was collected using questionnaire survey administered in ten different locations such as hospitals, shopping malls, public and private universities around Klang Valley, the fastest growing region in Malaysia. Stratified random sampling was used to stratify each survey location based on employment status – the student, working and nonworking (unemployed, housewives, retired) communities in both public and private sectors.

A simple random sample comprised only of Malaysian participants above 18 years old was drawn from each location. Of the 506 questionnaires collected, a total of 460 questionnaires were completed. 389 questionnaires represent Facebook user population and the remaining 71 of which represent the non-user population in Malaysia, yielding an effective response rate of about 91%. A summary statistics of the sample, including demographic breakdowns of user and non-user group, is presented in Table 1.

The sample consists of a broad range of demographic information to profile diverse Facebook users across the multiracial Malaysian population. This includes age, gender, ethnicity, religion, marital status, education, language, type of sector and income level. The Malays, Chinese and Indians are three major ethnic groups in Malaysia and the religions commonly practiced are Islam, Buddhism, Christianity and Hinduism. Whilst language may not have salient moderating effect in most English-speaking developed countries, Nair (2009) showed that language is an important moderator on ICT use in Malaysia. Most digital contents are in English whereas other vernacular languages are the main medium of communication in many parts of the country.

The moderating effect of these demographic factors has been tested in past social networks and information systems studies (Grasmuck, Martin, & Zhao, 2009; Honeycutt & Cunliffe, 2010; Lewis, Kaufman, Gonzalez, Wimmer, & Christakis, 2008; Mazman & Usluel, 2010; Thelwall, 2008; Venkatesh, Morris, Gordon, & Davis, 2003). Empirical studies from developed countries have found that age (Valkenburg & Peter, 2009), gender, ethnicity (Lewis et al., 2008; Valenzuela, Park, & Kee, 2009), minority language (Honeycutt & Cunliffe, 2010), education (Kirschner & Karpinski, 2010; Mazman & Usluel, 2010), job employment and marital status (Helsper, 2010), and income (Lewis et al., 2008) respectively influence the adoption and use of SNT.

For content validity, 11 purposes of using Facebook and a checklist of 16 most frequently used features, functions, or applications on Facebook at the point of survey were identified from Facebook Application Directory. A total of 27 questionnaire items of the use purposes and use behaviour are measured on a multiple-item 5-point Likert scale (5=using every day, 4=using a few times each week, 3=using between once a week and once a month, 2=using less than once a month=2, or 1=never use before). Another 4 items were introduced to measure business experience with Facebook among the users who use Facebook for work or business on a 5-point Likert scale (5=strongly agree, 4=agree, 3=neutral, 2=disagree, 1=strongly disagree).

The quality of questionnaire items was assessed by exploratory factor analysis (EFA) using principal axis factoring technique on Promax oblique rotation to better identify a simple factor structure for items reduction (Finch, 2006). Each item represented one observed variable and was restricted only to load on one pre-specified construct (Hair, Anderson, Tatham, & Black, 1992). The criterion for convergent and discriminant validity was

Demographics	n	%	n	%	n	%
Total respondents	460	100%				
Facebook users			383*	83.3%		
Facebook non-users					71	15.6%
Age:						
18-24	284	61.7%	246	64.2%	18	25.4%
25-34	101	22.0%	78	20.4%	11	15.5%
35-44	39	8.5%	34	8.9%	12	16.9%
45 or above	36	7.8%	25	6.5%	30	42.2%
Gender:						
Male	180	39.1%	147	38.4%	27	38.0%
Female	279	60.7%	235	61.4%	44	62.0%
No response	1	0.2%	1	0.2%		
Ethnicity:						
Malay	130	28.3%	110	28.7%	5	7.1%
Chinese	257	55.9%	214	55.9%	51	71.8%
Indian	55	11.9%	46	12.0%	11	15.5%
Others	18	3.9%	13	3.4%	4	5.6%
Marital Status:						
Single	347	75.5%	294	76.8%	30	42.3%
Married	106	23.0%	83	21.7%	38	53.5%
Divorced/ Widow/Widower	7	1.5%	6	1.5%	3	4.2%
Education:						
Secondary Level or below	132	28.7%	110	28.7%	34	47.9%
High School Level	89	19.4%	78	20.4%	10	14.1%
Tertiary Level or above	236	51.3%	194	50.7%	27	38.0%
No response	3	0.6%	1	0.2%	3	4.2%
Preferred Language:						
Malay	108	23.5%	90	23.5%	3	4.2%
English	227	49.3%	187	48.8%	46	64.8%
Mandarin	107	23.3%	88	23.0%	14	19.7%
Tamil	9	2.0%	9	2.4%	3	4.2%
Others	8	1.7%	8	2.1%	5	7.1%
No response	1	0.2%	1	0.2%	-	-
Type of sector:						
Public	101	22.0%	89	23.2%	6	8.5%
Private	297	64.5%	243	63.5%	50	70.4%
Others	30	6.5%	25	6.5%	4	5.6%
None (Unemployed)	32	7.0%	26	6.8%	11	15.5%
Employment						
Students	234	50.9%	202	52.7%	17	23.9%
Working Adults	197	42.8%	159	41.5%	41	57.8%
Non-Working Adults	29	6.3%	22	5.7%	13	18.3%
Monthly Personal Income:						
No regular income	270	58.7%	231	60.3%	27	38.0%
RM2,000 or less	52	11.3%	42	11.0%	9	12.7%
RM2,001 to RM4,000	76	16.5%	59	15.4%	19	26.8%
RM4,001 or more	61	13.3%	50	13.1%	16	22.5%
No response	1	0.2%	1	0.2%	-	-

Table 1: Sample Statistics

** Note: User sample is reduced from 389 to 383 after removing non-response data.*

relaxed in order to explore perceived (purpose of) use and actual use behaviour determinants. Eight loadings were less than 0.60 (but greater than 0.25) and three cross-loadings were greater than 0.30. Items that have non-confirming cross-loadings were removed from further analysis. They are using Facebook for 'event', 'groups/ fan pages' and 'send private messages'. However, items that have low loadings were retained in the analysis given the sufficient discriminant validity between low-loading constructs that have low cross-loadings. The final 28 items are loaded on six constructs for 'utilitarian use' (6 items), 'hedonic use' (5 items), 'business' (4 items), 'information seeking' (5 items), 'socialisationsocialisation' (5 items), and 'entertainment' (3 items).

5. KEY FINDINGS OF THE STUDY

In this section, key findings of this study will be presented in two parts. The first part shows results on Facebook users, whereas the second part focuses on the non-users of Facebook.

5.1 FACEBOOK USERS

Table 2 shows the average utilitarian use and hedonic use of users across age, gender, ethnicity, marital status, education, language, sector, employment and monthly personal income.

The results show that users who use Facebook the most for utilitarian purposes have the following demographic profiles: age group between 35 to 44 years old (2.23), male (2.19), Malay (2.32), single (2.21), high school education level (2.16), proficient in Bahasa Malaysia (2.33), in the public sector (2.34), non-working adults such as unemployed, retiree, housewives (2.33), and having an income level of RM2000 or less (2.14).

On the other hand, users who use Facebook the most for hedonic purposes are found in the following demographic profile: age group between 18 to 24 years old (3.98), female (3.93), Chinese (3.99), single (4.43), high school education level (2.16), proficient in Chinese Mandarin (4.01), in the public sector (4.02), students (4.02), and having no regular income (4.01).

The findings indicate that users use Facebook for hedonic purposes more than utilitarian purposes. This is as expected because Facebook is more popularly known for social communication and entertainment. However, generally there was a rise in terms of utilitarian use among Facebook users. Users are using the hedonic features, functions, applications of Facebook 'a few times each week' to 'everyday' while their utilitarian use of Facebook is 'less than once a month' to 'between once a week and once a month'. Study on Facebook in Malaysia shows that gender, employment, and ethnicity are among the important demographic factors influencing users' perception and actual use behaviour on Facebook (Liew et al., 2014).

Thus, the interacting effects are examined between gender and employment (Table 3-1) and gender and ethnicity (Table 3-2) on the utilitarian use and hedonic use of Facebook. Table 3-1 and 3-2 show that Malay non-working adults use Facebook the most for utilitarian purposes whereas Chinese students use Facebook the most for hedonic purposes. Results also show that the same pattern is observed regardless of gender, thus gender effect is indifferent to the utilitarian use and hedonic use of Facebook.

Next, the top 5 most important purposes of using Facebook ranked by the users are presented in Figure 4. Results show that the most important purpose popularly ranked as top 1 is using Facebook for "family and friends"

Demographics	Utilitarian Use *	Hedonic Use *
Age:		
18-24	2.11	3.98
25-34	1.97	3.89
35-44	2.23	3.63
45 or above	1.87	3.72
Gender:		
Male	2.19	3.90
Female	2.01	3.93
No response	-	-
Ethnicity:		
Malay	2.32	3.89
Chinese	1.96	3.99
Indian	2.04	3.65
Others	2.17	3.87
Marital Status:		
Single	2.21	4.43
Married	2.02	3.66
Divorced/ Widow/Widower	2.09	3.98
Education:		
Secondary Level or below	2.11	3.85
High School Level	2.16	4.14
Tertiary Level or above	2.02	3.86
No response	-	-
Preferred Language:		
Bahasa Malaysia	2.33	3.92
English	2.00	3.89
Mandarin	1.98	4.01
Tamil	2.32	3.80
Others	2.06	3.48
No response	-	-
Type of sector:		
Public	2.34	4.02
Private	1.96	3.91
Others	2.26	3.80
None (Unemployed)	2.17	3.72
Employment		
Students	2.09	4.02
Working Adults	2.04	3.81
Non-Working Adults	2.33	3.75
Monthly Personal Income:		
No regular income	2.11	4.01
RM2,000 or less	2.14	3.91
RM2,001 to RM4,000	2.01	3.68
RM4,001 or more	2.00	3.74
No response	-	-

Table 2: Users Sample Statistics

** Note: Average index is calculated based on the average of 'utilitarian use' and 'hedonic use' items measured respectively on a 5-point Likert scale ((5=using every day, 4=using a few times each week, 3=using between once a week and once a month, 2=using less than once a month=2, or 1=never use before).*

Gender:	Male			Female		
Employment:	Students	Working Adults	Non-Working Adults	Students	Working Adults	Non-Working Adults
Utilitarian Use	2.21	2.12	2.65	2.00	1.99	2.18
Hedonic Use	3.96	3.83	3.80	4.06	3.80	3.73

Table 3-1: Utilitarian and Hedonic Use of Facebook: Gender and Employment

Gender:	Male			Female		
Ethnicity:	Malay	Chinese	Indian	Malay	Chinese	Indian
Utilitarian Use	2.71	2.38	2.53	2.57	2.11	2.19
Hedonic Use	4.12	4.23	3.40	4.09	4.18	4.06

Table 3-2: Utilitarian and Hedonic Use of Facebook: Gender and Ethnicity

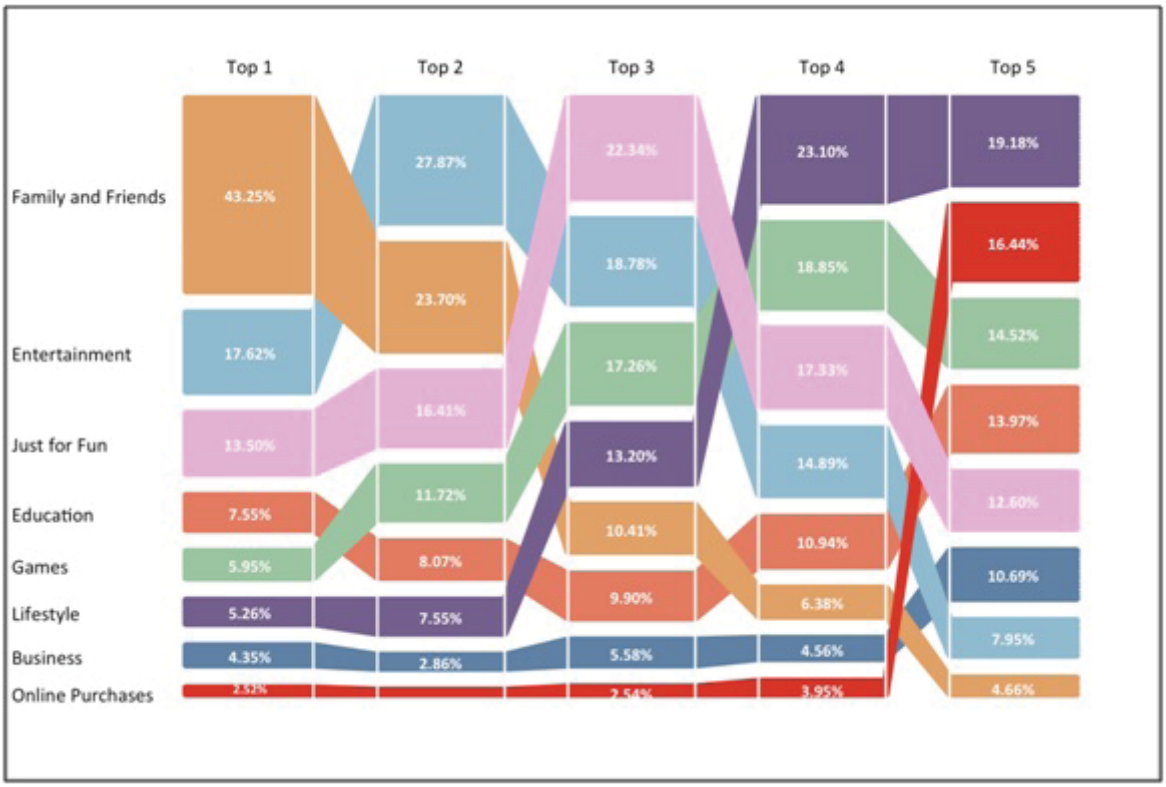


Figure 4: Top Five Most Important Purposes of Using Facebook

(43.25%), followed by "entertainment" (27.87%) ranked as top 2, "just for fun" (22.34%) ranked as top 3, and "lifestyle" popularly ranked as top 4 (23.10%) and top 5 (19.18%). Interestingly, using Facebook for "online purchase" (16.44%) is increasingly recognized by users and is ranked in the top 5, followed by "games" (14.52%) and "education" (13.97%).

Our results imply that the hedonic benefits of Facebook have been widely recognized by the Malaysian users. They use Facebook to connect and communicate with family and friends, as well as for entertainment and fun not related to study or work. This is consistent with the extant literature, which shows that Facebook is becoming an integral part of social communication, providing social and entertainment benefits to users. The results also show a rise in the use of Facebook for utilitarian-related purposes such as lifestyle, online purchase, education and business. This observation is consistent with the findings in Table 2. Though the utilitarian benefits of Facebook are ranked secondary to hedonic benefits, users who perceive that using Facebook could improve their lifestyles would also consider using Facebook to access online products and services catalog, promotions, e-learning materials, exchange information or knowledge, or even creating their own company Facebook pages and advertisement.

This study further examines how these use purposes ranked as important by users manifest in their actual utilitarian and hedonic use of Facebook, which could translate into real socio-economic benefits. While users are using Facebook for both utilitarian and hedonic purposes, Figure 5 shows that 65.3% of use is attributed to hedonic purposes whereas 34.7% is for utilitarian purposes. The utilitarian use is about half the hedonic use among users.

More specifically, users are using Facebook for utilitarian purposes such as business development (14.1%) and information seeking (20.6%) activities. Their utilitarian use for information seeking is manifest in using

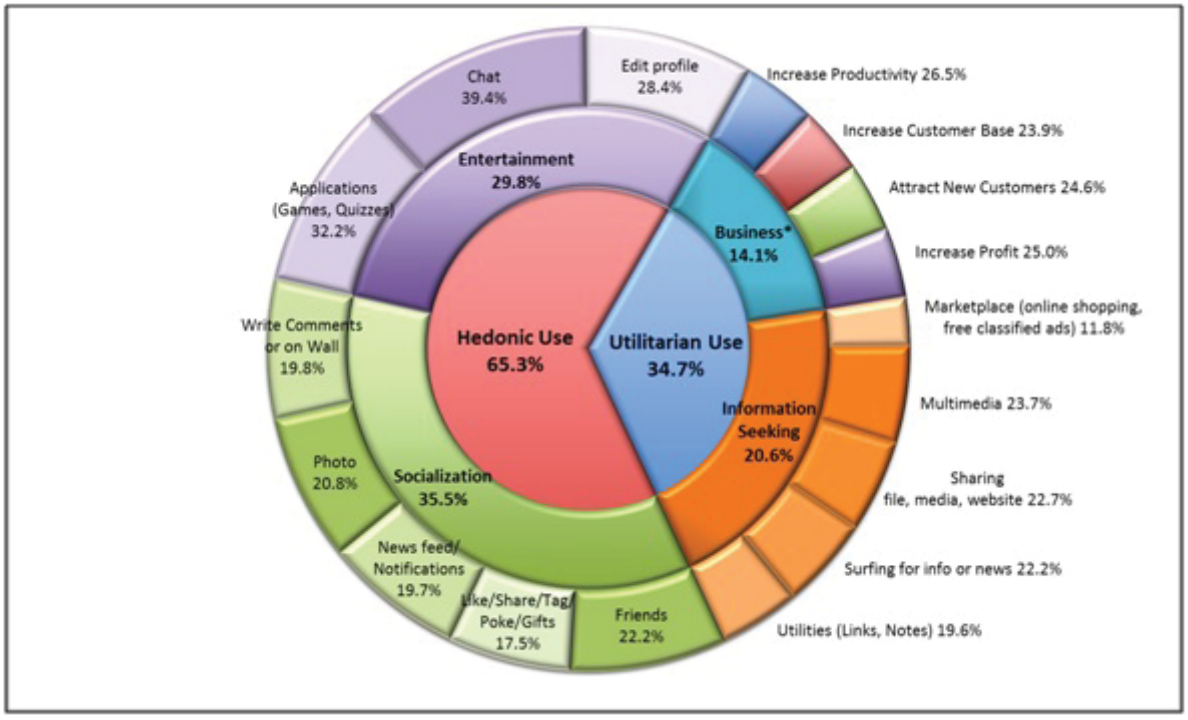


Figure 5: Hedonic and Utilitarian Use Behaviour of Facebook

Facebook features, functions, applications for multimedia (23.7%), sharing information such as files, media, websites (22.7%), surfing for information or news (22.2%), utilities such as links, notes, and accessing marketplace for online shopping, free classified ads (11.8%). Among users who are using Facebook for work or business purposes (*), they have reported increased productivity (26.5%), increased profit (25.0%), new customer attraction (24.6%), and increased customer base (23.9%).

Users are widely using Facebook for hedonic purposes such as socialisation (35.5%) and entertainment (29.8%). Their socialisation use of Facebook is manifest in using features, functions, application for friends request and acceptance (22.2%), photos (20.8%), writing comments in posts or Wall (19.8%), getting in touch via news feed notification (19.7%), and social interaction such as like, share, tag, poke, gifts (17.5%).

The current use of Facebook in Malaysia tends to lean more towards the hedonic use than utilitarian-use, emphasizing more on social values to the users. While the hedonic benefits of Facebook for socialisation (36.3%) and entertainment (30.5%) are obvious and consistent with past studies (Giannakos et al., 2013; Theotokis & Doukidis, 2009), the growing use of Facebook for business (14.1%) and information seeking (20.6%) should not be undermined. Other studies (Liew et al., 2014; Shin, 2013) have similarly demonstrated that the more socially active users will be more aware of what Facebook could offer, thus better perceive the socio-economic benefits of Facebook, which leads them to a higher use of Facebook for utilitarian purposes.

5.2 FACEBOOK NON-USERS

This section presents key findings on the non-users of Facebook. Figure 6-1 to Figure 6-9 shows the different reasons of not using Facebook across diverse demographic groups of population – age, gender, ethnicity, marital status, education, preferred language, sector, personal income and employment status.

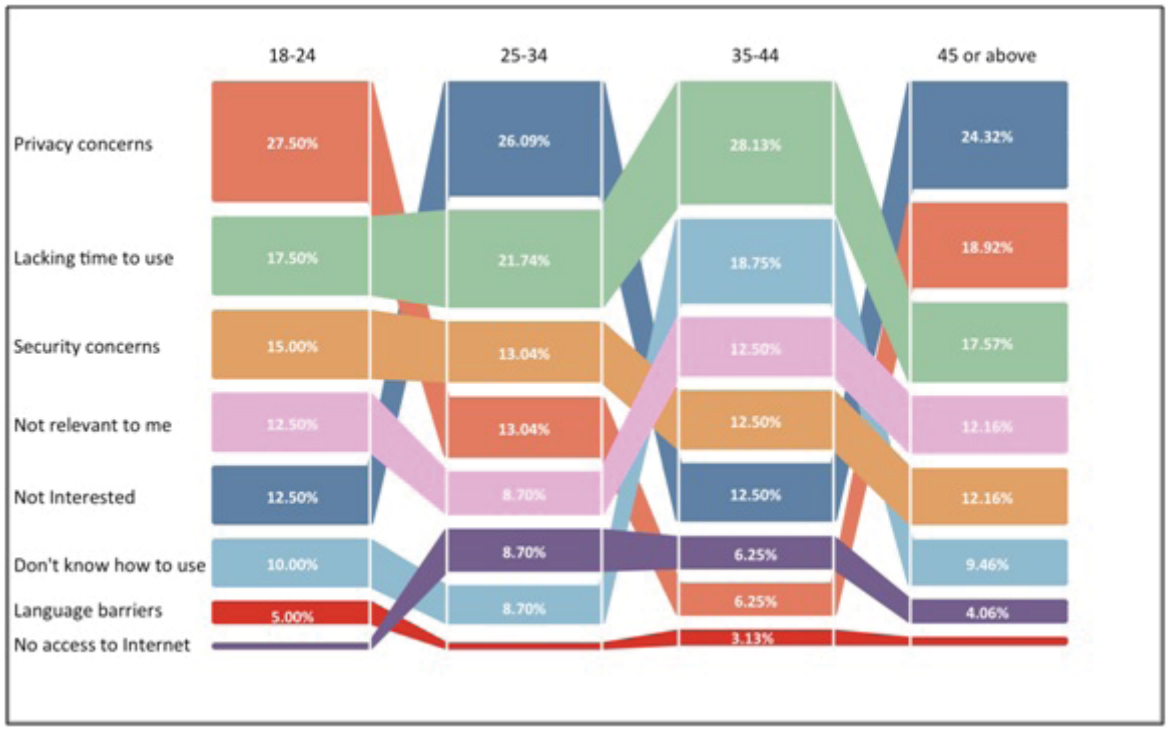


Figure 6-1: Reasons for not using Facebook by Age

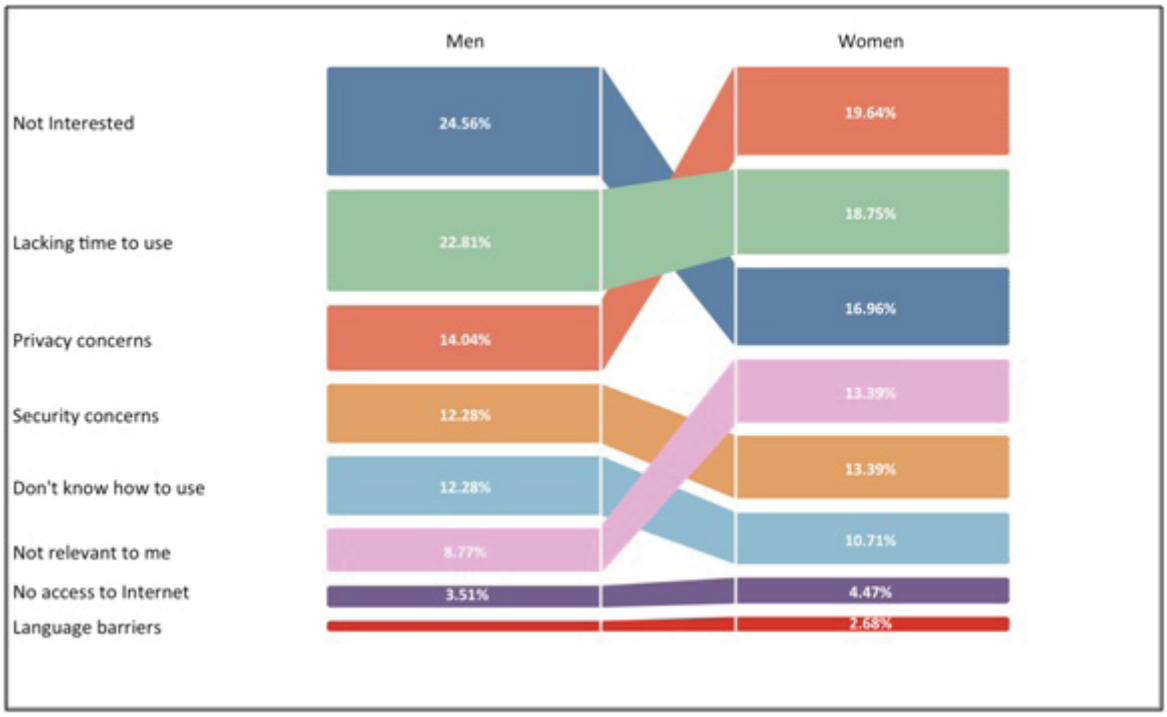


Figure 6-2: Reasons for not using Facebook across Gender

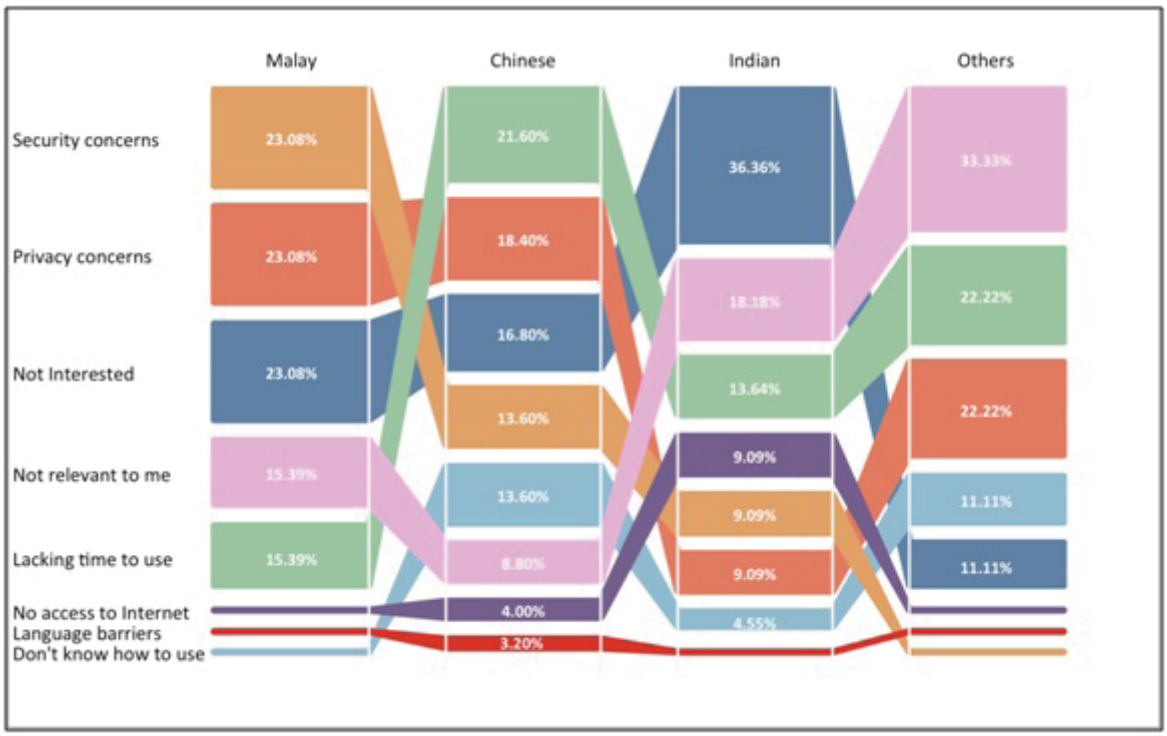


Figure 6-3: Reasons for not using Facebook across Ethnicity

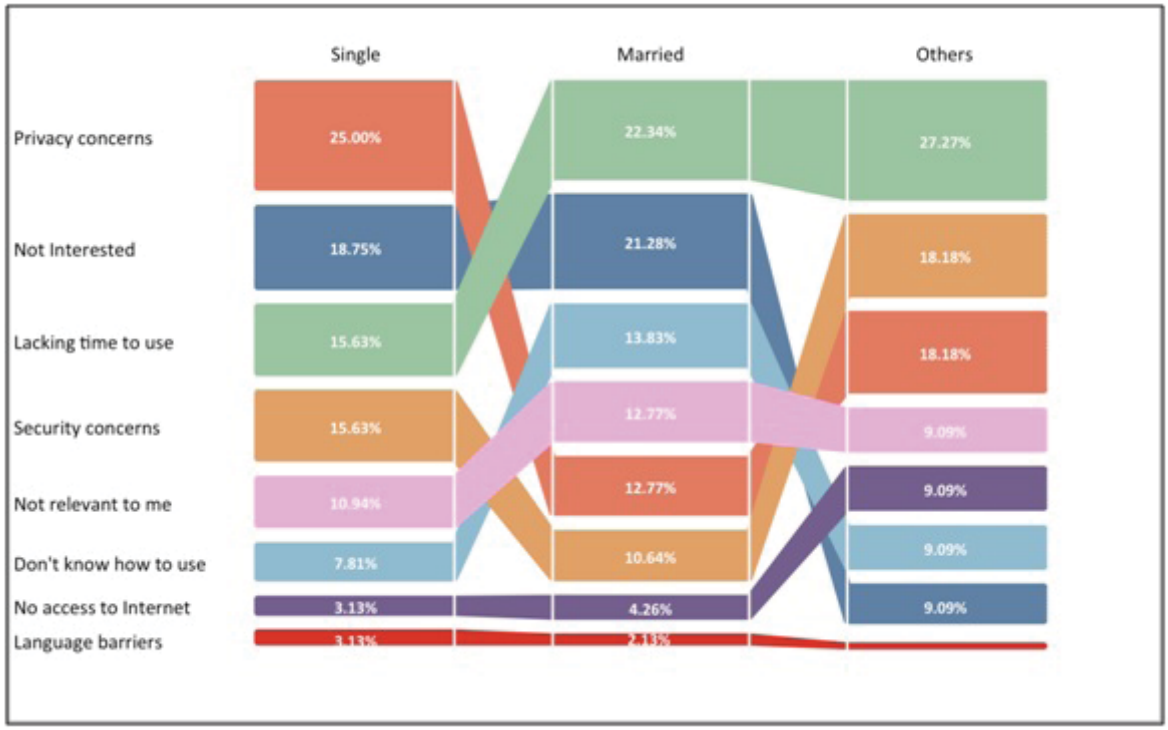


Figure 6-4: Reasons for not using Facebook across Marital Status

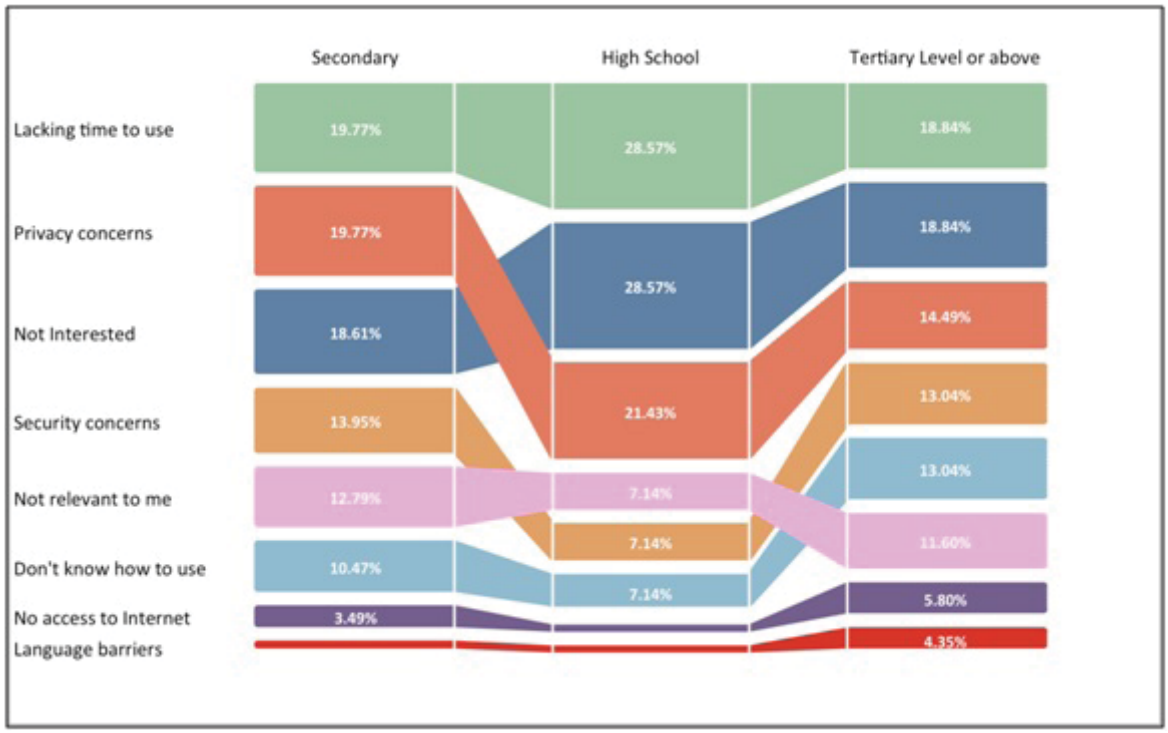


Figure 6-5: Reasons for not using Facebook across Education

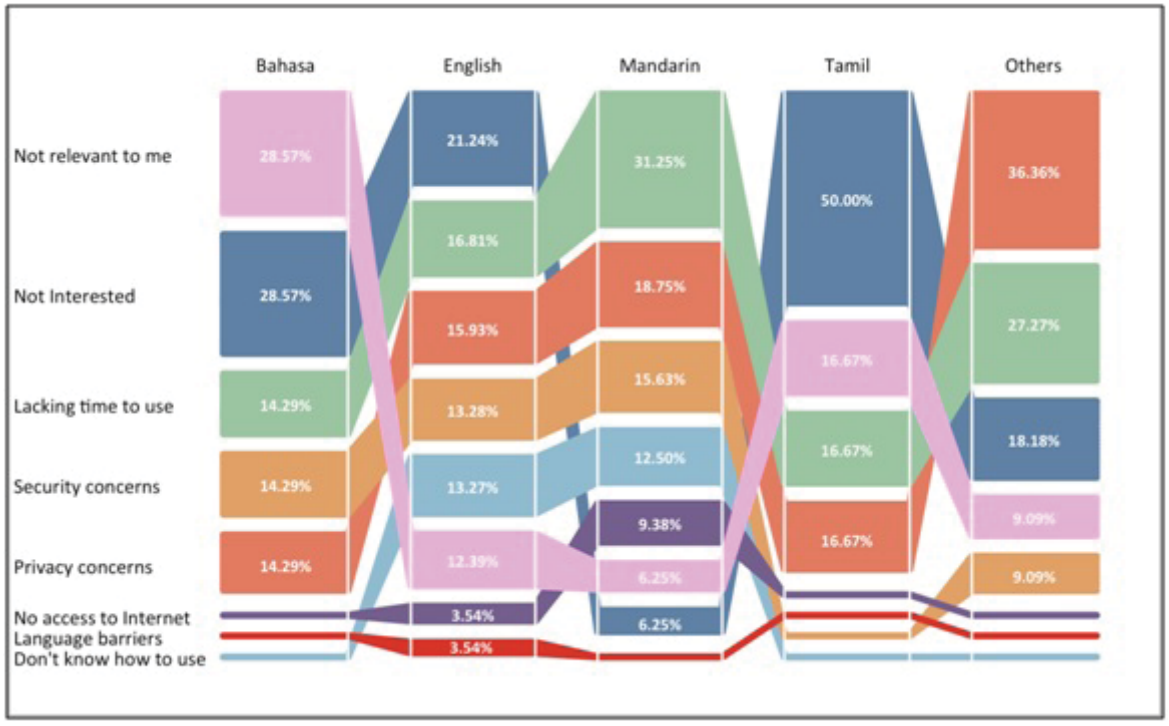


Figure 6-6: Reasons for not using Facebook across Language

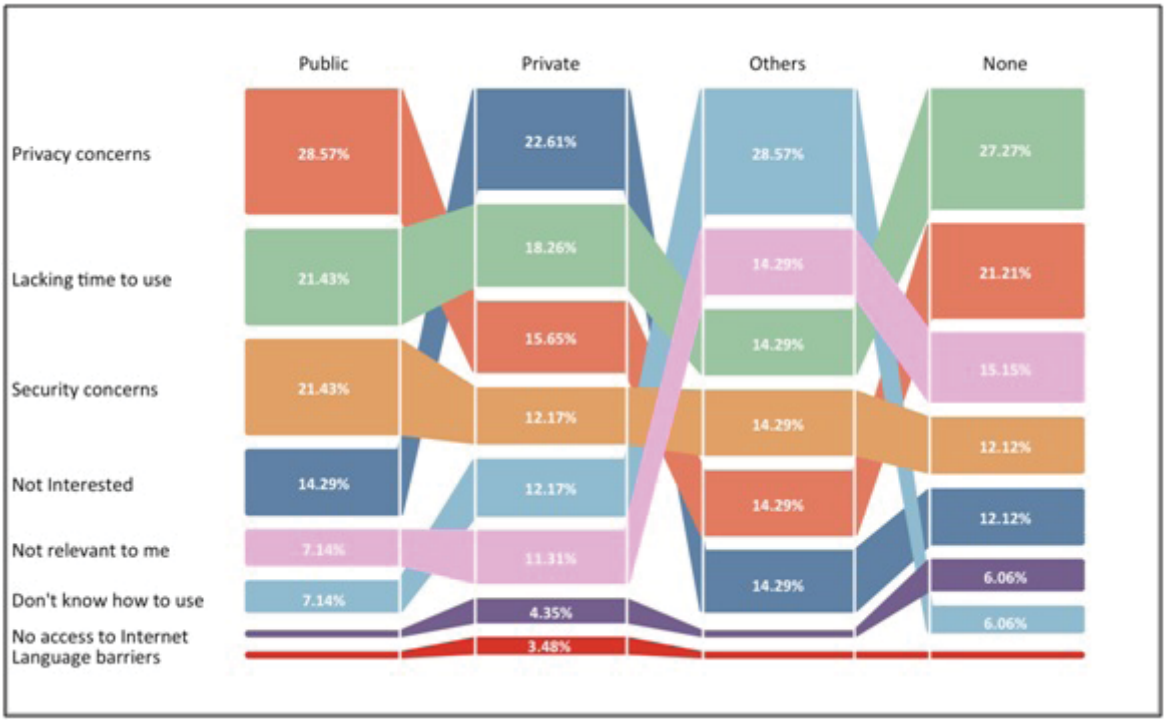


Figure 6-7: Reasons for not using Facebook across Sector

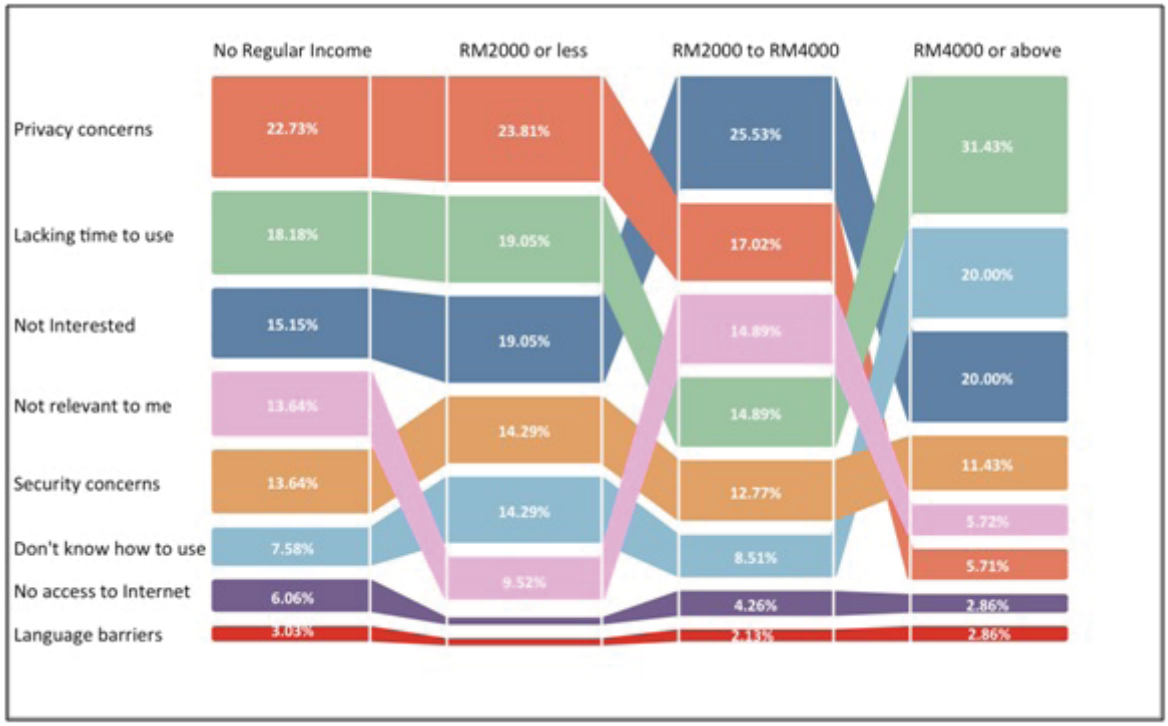


Figure 6-8: Reasons for not using Facebook across Income

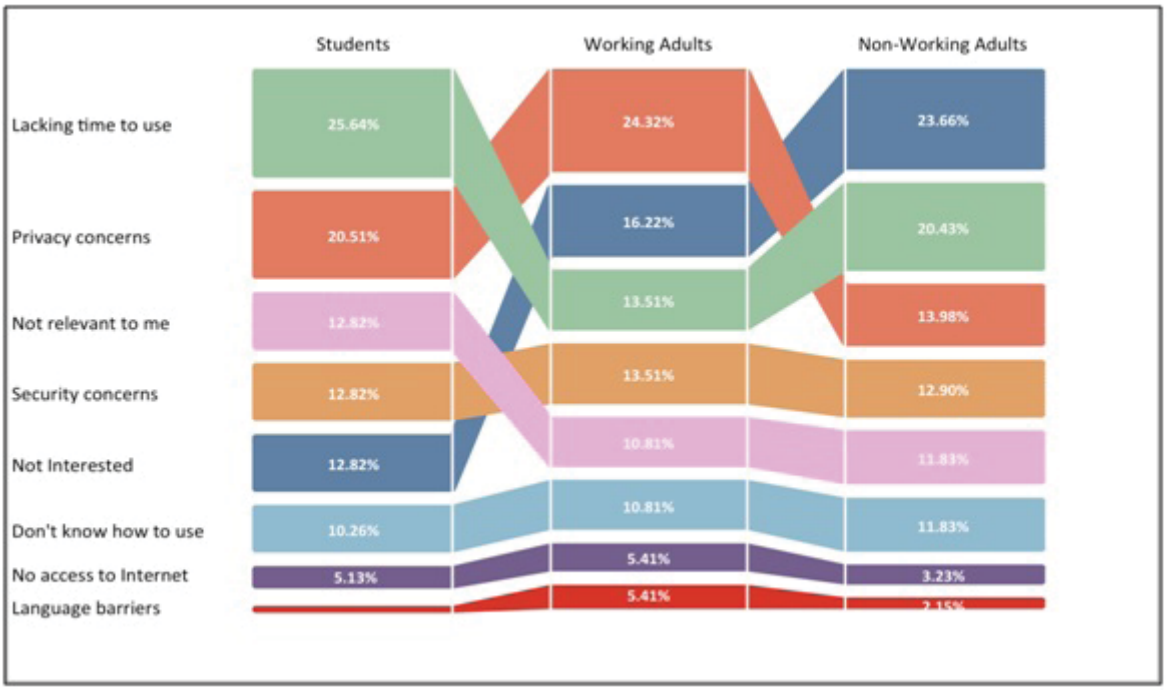


Figure 6-9: Reasons for not using Facebook across Employment

The results show that 'privacy concern' is the top reason for not using Facebook among non-users aged between 18 to 24 (27.50%), women (19.64%), single (25.00%), proficient in other languages than Bahasa, English, Mandarin, or Tamil (36.36%), working or studying in the public sector (28.57%), having no regular income (22.73%) and RM2000 or less (23.81%), working adults (24.32%). 'Security concern' is the top reason for not using Facebook among the Malay non-users (23.08%).

Non-users 'not interested' in using Facebook are in the age group of 25 to 34 (26.09%) and 45 or above (24.32%), men (24.56%), Indian (36.36%), proficient in English (21.24%) and Tamil (50.00%), working or studying in the private sector (22.61%), earning an income of RM2000 to RM4000 (25.53%), non-working adults i.e. unemployed, retiree, housewives (23.66%). Non-users who reported that Facebook is 'not relevant' to them are from the minority ethnic group (33.33%), and proficient in Bahasa Malaysia (28.57%).

Non-users who are neither in the public nor private sector such as unemployed, retirees and housewives reported that their top reason for not using Facebook is because they 'don't know how to use' it (28.57%). Other non-users who 'lack time using Facebook' are aged between 35 to 44 (28.13%), Chinese (21.60%), married (22.34%) and divorced/ widow/ widower (27.27%), irrespective of education level (secondary, 19.77%; high school, 28.57%; tertiary level 18.84%), proficient in Chinese Mandarin (31.25%), not working or studying in any sector (27.27%), earning an income of RM4000 or above (31.43%), students (25.64%).

Interestingly, non-users reported that 'language barriers' and 'no access to Internet' are the least important reasons for not using Facebook. This shows that most of the non-users are generally proficient in English, which is the lingua franca of Facebook, and having access to Internet. Language may not be a barrier to adoption as Facebook supports a wide range of languages input and non-users are aware that other vernacular languages can be used as a medium to communicate on Facebook. Furthermore, Internet accessibility is less of a concern for non-users largely due to the government's rigorous broadband diffusion initiatives particularly in high economic impact areas around Klang Valley.

The interaction of gender and employment (Table 4) on reasons for not using Facebook among non-users is also examined. The result shows that 33.34% of the male students and 20.00% of the female students found that

Gender:	**Male**			**Female**		
Employment:	**Students**	**Working Adults**	**Non-Working Adults**	**Students**	**Working Adults**	**Non-Working Adults**
Privacy concerns	33.34%	7.50%	20.04%	20.00%	18.87%	20.59%
Security concerns	16.67%	10.00%	20.04%	12.00%	15.09%	11.76%
Not Interested	25.00%	25.01%	20.04%	12.00%	22.64%	11.76%
Not relevant to me	0.00%	12.51%	0.00%	16.00%	11.32%	14.71%
Don't know how to use	0.00%	15.01%	20.04%	16.00%	9.43%	8.82%
Lacking time to use	25.00%	22.51%	19.84%	8.00%	18.87%	26.47%
Language barriers	0.00%	2.50%	0.00%	8.00%	1.89%	0.00%
No access to Internet	0.00%	4.95%	0.00%	8.00%	1.89%	5.88%

Table 4: Utilitarian and Hedonic Use of Facebook: Gender and Employment

privacy concerns are the top reason for their non-adoption. 25.01% working men and 22.64% working women were not interested in the use of Facebook. Non-working men found that the top reason for not using Facebook is due to the following reasons – privacy concerns, or security concerns, or not interested, or don't know how to use (20.04% respectively). While 26.47% of the non-working women found that lacking time to use Facebook is the top reason for their non-adoption.

6. DISCUSSION AND POLICY IMPLICATIONS

The empirical analysis demonstrates users' positive perception on the socio-economic benefits of Facebook and their active use of Facebook for business development, information seeking, socialisationsocialisation,and entertainment. The study also examined users' utilitarian use and hedonic use of Facebook across diverse demographic groups in Malaysia. On the other hand, privacy and security concerns, attractiveness of Facebook usability, and time constraint are the top reasons for non-adoption. Key findings are summarized as following:

- Younger users use Facebook the most for hedonic purposes while older users for utilitarian purposes.
- Users in the public sector use Facebook the most compared to those in the private sector or others who are unemployed.
- Malays use Facebook the most for utilitarian purposes and Chinese for hedonic use, which corresponds to their medium of language Bahasa Malaysia and Chinese Mandarin respectively.
- Most users perceive utilitarian benefits as secondary to the hedonic benefits of using Facebook.
- The utilitarian use is about half of hedonic use of Facebook.
- The most frequently used Facebook features for socialisationsocialisation is related to friends and photos, chat for entertainment, and multimedia for information search.
- Users who use Facebook for business reported increased productivity, profit, new customer attraction and retention.
- 'Privacy concerns', 'not interested', and 'lack time to use' are the top three reasons for not using Facebook among non-users.

Next, this study will provide insights into the appropriate strategies to leverage users' perceived socio-economic benefits to act as a stimulus to move them from hedonic use to more advanced utilitarian use of Facebook. Liew, Vaithilingam, and Nair (2014) found that strategies to manage users' perception are critical to ensure people would get better socio-economic value from Facebook. One of the key challenges faced by policy-makers and practitioners is to increase the use of SNT platforms from lower-level hedonic use to the higher-level utilitarian use that will create actual socio-economic benefits for users. A number of policy initiatives should be in place to develop holistic information dissemination and engagement strategies, fostering and customising the use of Facebook for daily activities based on demographic profiles.

Over the past decade there has been a push by the government to enhance broadband diffusion across the nation; strategies now should focus on creating awareness and training for people to use SNT as a mainstream communication tool and free information dissemination channel. Particularly in the suburban and rural areas, publicly funded schools, tele-centers, and community centers can be used to improve users' skills in using SNT for creating socio-economic value. Creating local content to generate interest among community leaders is another way to

ensure that this mode of communication is encouraged. Greater incentives in the form of tax-incentives for the purchase of ICT tools and broadband subscription and support for training should be provided for social groups to use Facebook as means of communication, education and wealth generation. With positive social influence, users will be more socially driven to learn or use the utilitarian and hedonic features of Facebook, and interactively communicate and share information on their social networks.

Users who are aware of the economic potential and opportunities of Facebook may be uncertain about how to fully materialize them. Two misconceptions may be the roadblock to adopting the utilitarian use of Facebook. People may be skeptical about using Facebook for creating economic value and misperceive that Facebook is solely for communication and entertainment only. Another reason of underutilizing Facebook for utilitarian purposes is their concerns regarding privacy and security. Key regulators such MCMC play an important role in safeguarding users' privacy, integrity of online transactions, creditability of sellers, and accountability of information, product or service providers. The recently enacted Personal Data Protection Act should be reinforced more specifically in areas where users may be potentially exposed to any violation of privacy and cybercrimes. Users should also be informed about their limited autonomy to adjust their privacy level on Facebook and other SNT platforms.

With greater transparency and accountability via SNT platforms, government and firms can encourage fair play that is vital for a competitive economy and in reducing market failures. SNT is conducive for targeted marketing and can act as enabler for users to access information, knowledge and affordable services in various innovative ways. Policy-makers and practitioners may leverage on existing e-services such as online education, online financial services, online government and hospital care, and customise these services for users with different demographic profiles. This can be aligned with the government's demand stimulation programs under the NBI such as on-going broadband awareness, training, and promotion through mass media, affordable broadband distribution, and communication content and infrastructure development and commercialisation.

In the education space, Facebook can be used as an important tool for students and teachers to not only communicate more effectively among themselves, but also to tap into the collective 'network-brain' of educators from around the globe. The international exposure will enable teachers to design and develop innovative teaching pedagogies and methods, and students can be an integral part of this creative learning value chain. Facebook provides a creative learning platform for students to interact with multiple stakeholders to enhance their learning. It will also enable them to be contributors to information, knowledge and wealth, setting Malaysia on the path to becoming a knowledge-intensive high-income economy.

7. CONCLUSION

The Malaysian government has a vision of transforming the country into a high income nation by 2020 and the key enabler for the realization of the vision is the use of advanced ICT such as Facebook and other SNTs. Various initiatives have been put in place over the last two decades to position Malaysia on an information- and knowledge-drive trajectory and this has enabled the country to become competitive and be a source of foreign direct investment. Democratisation of information and knowledge due to SNT platforms have

intensified competition for resources and markets and countries that do not keep up to translating investments in technological infrastructure into wealth creation opportunities will be lose their competitive and comparative advantages.

While Malaysia is one of the highest users of Facebook in the region, much of it is for hedonic use. Hence, the potential of utilitarian use of this new technology has not been fully explored for wealth creation purposes. Not harnessing the potential of Facebook for utilitarian purpose will lead to untapped market and wealth creation opportunities in the digital economy, which is increasingly important for GDP of the country. This new space is going to be the source for firms and customers to derive greater economies of scale and scope. It will be imperative for Malaysian firms to close the chasm between Facebook use and wealth creation to remain globally competitive. This paper provides some insights into the various patterns of Facebook use and key factors that enhance and hinder the use of Facebook for wealth creation. Development initiatives that set the pace for Malaysia's transition to a high-income economy should take into consideration key policies and strategies that will encourage the use of new technologies such as Facebook and other SNTs by firms, consumers and other stakeholders for both hedonic and utilitarian purposes.

ACKNOWLEDGEMENT:

The authors would like to thank Monash University Malaysia and the Ministry of Higher Education Malaysia for financial support for this project under the Fundamental Research Grant Scheme (Grant No: FRGS/2/2010/SS/MUSM/012).

REFERENCES

1. Boyd, D. M., & Ellison, N. B. (2008). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication,* 13(1), 210–230.
2. Cardon, P. W. (2009). Online Social Networks. *Business Communication Quarterly,* 72(1), 96–97.
3. CNN. (2010). Study: Malaysians have the most friends, at least on social media - CNN.com. Retrieved October 15, 2010, from http://edition.cnn.com/2010/TECH/social.media/10/11/digital.life.study/
4. Communications Timeline. (2011). Retrieved July 15, 2014, from http://smilecastcommunications.com/timeline.html
5. comScore. (2011). Social Networking Accounts for One Third of All Time Spent Online in Malaysia. Retrieved November 15, 2011, from http://www.comscore.com/Press_Events/Press_Releases/2011/10/Social_Networking_Accounts_for_One_Third_of_All_Time_Spent_Online_in_Malaysia
6. Datta, P. (2011). Preliminary study of e-commerce adoption in developing countries. *Information Systems Journal,* 21(1), 3–32.
7. Economist Intelligence Unit. (2011). Technology Briefing on Malaysia Internet: sub-sector update as at December 1, 2011. Retrieved from http://www.eiu.com/index.asp?layout=ib3Article&article_id=458699030&country_id=1600000160&pubtypeid=1162462501&industry_id=&category_id=&rf=0
8. Ernst, C.-P., Pfeiffer, J., & Rothlauf, F. (2013). The Influence of Perceived Belonging on Social Network Site Adoption. In AMCIS 2013 Proceedings. Chicago, Illinois, USA: Association for Information Systems. Retrieved from http://aisel.aisnet.org/amcis2013/SocialTechnicalIssues/GeneralPresentations/11
9. Facebook. (2011). Facebook Deomographics Revisited - 2011 Statistics by Ken Burbary - March 7, 2011. Retrieved from http://www.facebook.com/note.php?note_id=197149076992338
10. Facebook, 2014. (2014, July 23). Facebook Reports Second Quarter 2014 Results [Official Website]. Retrieved August 14, 2014, from http://investor.fb.com/releasedetail.cfm?ReleaseID=861599
11. Finch, H. (2006). Comparison of the Performance of Varimax and Promax Rotations: Factor Structure Recovery for Dichotomous Items. *Journal of Educational Measurement,* 43(1), 39–52.
12. Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management & Data Systems,* 106(5), 601–620.
13. Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly,* 27(1), 51–90.
14. Giannakos, M. N., Chorianopoulos, K., Giotopoulos, K., & Vlamos, P. (2013). Using Facebook out of habit. *Behaviour & Information Technology,* 32(6), 594–602.
15. Gibbons, D. E. (2004). Friendship and advice networks in the context of changing professional values. *Science Quarterly,* 49, 238–262.
16. Grasmuck, S., Martin, J., & Zhao, S. (2009). Ethno-racial identity displays on Facebook. *Journal of Computer-Mediated Communication,* 15(1), 158–188.
17. Gross, R., & Acquiti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on privacy in the electronic society (Alexandria, VA)* (pp. 71–80). New York: ACM Press.
18. Hair, J. F., Anderson, R. E., Tatham, E., & Black, W. C. (1992). *Multivariate Data Analysis with Readings (7th ed.).* New York: Macmillan Publishing.
19. Helsper, E. J. (2010). Gendered Internet Use Across Generations and Life Stages. *Communication Research,* 37(3), 274–352.
20. Honeycutt, C., & Cunliffe, D. (2010). The use of the Welsh language on Facebook. Information, *Communication & Society,* 13(2), 226–248.
21. Hu, T., Poston, R. S., & Kettinger, W. J. (2011). Nonadopters of online social network services: is it easy to have fun yet? *Communications of the Association for Information Systems,* 29(1), 441–458.
22. Internet World Stats. (2014a). Asia Marketing Research, Internet Usage, Population Statistics and Facebook Information - Malaysia. Retrieved August 1, 2014, from www.internetworldstats.com/asia.htm
23. Internet World Stats. (2014b). Facebook users in the world - Facebook usage and Facebook growth statistics by world geographic regions. Retrieved August 1, 2014, from www.internetworldstats.com/facebook.htm
24. Jasmin. (2012, April 28). The Evolution of Communication [infographic] [Social Media]. Retrieved from http://dailyinfographic.com/the-evolution-of-communication-infographic
25. Johnston, K., Tanner, M., Lalla, N., & Kawalski, D. (2013). Social capital: the benefit of Facebook "friends." *Behaviour & Information Technology,* 32(1), 24–36.
26. Kirschner, P. A., & Karpinski, A. C. (2010). Facebook and academic performance. *Computer in Human Behavior,* 26(6), 1237–1245.
27. 27. Lewis, K., Kaufman, J., Gonzalez, M., Wimmer, A., & Christakis, N. (2008). Tastes, ties, and time: A new social entwork dataset using Facebook.com. *Social Networks,* 30, 330–342.
28. Liew, E. J. Y., Vaithilingam, S., & Nair, M. (2014). Facebook and Socio-economic Benefits in the Developing World. *Behaviour & Information Technology,* 33(4), 345–360.
29. Lu, Y., & Zhou, T. (2007). A Research of Consumers' Initial Trust in Online Stores in China. *Journal of Research and Practice in Information Technology,* 39(3), 167–180.

30. Malaysian Communications and Multimedia Commission (MCMC). (2013, September 25). *Malaysia's Broadband Initiatives and Future Plans.* Public information and advocacy materials presented at the Expert Consultation on the Asian Information Superhighway and Regional Connectivity, organized by United Nations Economic and Social Commission for Asia and the Pacific (ESCAP), Manila, Philippines. Retrieved from http://www.unescap.org/resources/presentation-malaysia's-broadband-initiatives-and-future-plans-mcmc
31. Mazman, S. G., & Usluel, Y. K. (2010). Modeling educational usage of Facebook. *Computers and Education,* 55(2), 444–453.
32. Nair, M. (2010). The e-commerce ecology: Leapfrogging strategies for Malaysia. In R. Ramachandran (Ed.), *ICT Strategic Review 2010/2011: E-Commerce for Global Reach* (pp. 193–211). Malaysia: PIKOM and MOSTI.
33. Nair, M., & Vaithilingam, S. (2013). Broadband diffusion, innovative capacity and sustainable economic development: lessons for Malaysia. In R. Ramachandran (Ed.), *ICT Strategic Review 2013/2014: The Digital Opportunity* (pp. 195–211). Malaysia: PIKOM and MOSTI.
34. Performance Management and Delivery Unit (PEMANDU). (2010a). *Economic transformation Programme: A Roadmap for Malaysia.* Prime Minister's Department, Putrajaya.
35. Performance Management and Delivery Unit (PEMANDU). (2010b). *Government Transformation Programme.* Prime Minister's Department, Putrajaya.
36. Protalinski, E. (2012a, February 1). Facebook files for $5 billion IPO. ZDNet. Retrieved from http://www.zdnet.com/blog/facebook/facebook-files-for-5-billion-ipo/8320
37. Protalinski, E. (2012b, May 17). Facebook sets IPO share price at $38: $104 billion valuation. ZDNet. Retrieved from http://www.zdnet.com/blog/facebook/facebook-sets-ipo-share-price-at-38-104-billion-valuation/13281
38. Ramachandran, R., & The National ICT Association of Malaysia. (2012). Broadband for Science and Innovation: Imperative for Business Growth. In R. Ramasamy (Ed.), *ICT Strategic Review 2012/2013: Innovation for Digital Opportunities* (pp. 193–211). Malaysia: PIKOM and MOSTI.
39. Sharma, S. K., & Gupta, J. N. D. (2009). Identifying Factors for Lack of E-commerce in Developing Countries. *In K. Rouibah, O. Khalil, & A. Hassanien (Eds.), Emerging Markets and E-Commerce in Developing Economies* (pp. 70–88). Hershey, PA: Information Science Reference.
40. Shih, C. F., & Venkatesh, V. (2004). Beyond adoption: Development and application of a use-diffusion model. *Journal of Marketing,* 68(1), 58–72.
41. Shin, D.-H. (2013). User experience in social commerce: in friends we trust. *Behaviour & Information Technology,* 32(1), 52–67.
42. Sledgianowski, D., & Kulviwat, S. (2009). Using social network sites: the effects of playfulness, critical mass and trust in a hedonic context. *The Journal of Computer Information Systems,* 49(4), 74–84.
43. Statista. (2014a). Most popular social network sites in Asian countries in 2013. Retrieved August 6, 2014, from http://www.statista.com/statistics/224746/leading-social-network-sites-in-asian-countries/
44. Statista. (2014b). Number of internet users in the Asia Pacific countries 2014 | Statistic. Retrieved August 6, 2014, from http://www.statista.com/statistics/265153/number-of-internet-users-in-the-asia-pacific-region/
45. Statista. (2014c). Quarterly revenue of Facebook 2010-2014. Retrieved August 22, 2014, from http://www.statista.com/statistics/277963/facebooks-quarterly-global-revenue-by-segment/
46. Statista. (2014d). Social network usage of the Asia Pacific regions' online populations in 2011. Retrieved August 6, 2014, from http://www.statista.com/statistics/214694/social-network-usage-penetration-of-the-asia-pacific-online-populations/
47. Stefanone, M. A., Hurley, C. M., & Yang, Z. J. (2013). Antecedents of online information seeking. *Information, Communication & Society,* 16(1), 61–81. doi:10.1080/1369118X.2012.656137
48. Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior,* 27, 590–598.
49. The Star. (2014). Ahmad Shabery: Malaysian broadband speeds to reach 50mbps by 2018 - Nation | The Star Online. Retrieved August 12, 2014, from http://www.thestar.com.my/News/Nation/2014/06/18/Broadband-to-reach-50mbps-2018/
50. Thelwall, M. (2008). Social Networks, Gender, and Friending: An analysis of MySpace Member Profiles. *Journal of the American Society for Information Science and Technology,* 59(8), 1321–1330.
51. Theotokis, A., & Doukidis, G. (2009). When Adoption Brings Addiction: A use-diffusion model for social information systems. In *Proceedings of the 30th International Conference on Information Systems* (ICIS) (p. Paper 138). Phoenix.
52. Tichy, N. M., & Fombrun, C. (1979). Network analysis in organisational settings. *Human Relations,* 32, 923–965.
53. Timm, D. M., & Duven, C. J. (2008). Privacy and social networking sites. *New Directions for Student Service,* 124.
54. Umphress, E. E., Labianca, G., Kass, E., & Scholten, L. (2003). The role of instrumental and expressive social ties in employees' perceptions of organisational justice. *Organisation Science,* 14(6), 738–753.
55. Valenzuela, S., Park, N., & Kee, K. F. (2009). Is there social capital in a social network site?: Facebook user and college students' life satisfaction, trust and participation. *Journal of Computer-Mediated Communication,* 14(4), 875–901.

56. Valkenburg, P. M., & Peter, J. (2009). Social consequences of the internet for adolescents: A decade of research. *Current Decisions in Psychological Science,* 18(1), 1–5.
57. Van Der Heijden, H. (2004). User acceptance of hedonic information systems. *MIS Quarterly,* 28(4), 695–704.
58. Venkatesh, V., Morris, M. G., Gordon, B. D., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly,* 27(3), 425–478.
59. Vollmer, C., & Premo, K. (2011). Campaigns to Capabilities Social Media & Marketing 2011 - *Selected Insights October* 2011 (pp. 1–18). Booz & Company and Buddy Media. Retrieved from http://www.booz.com/media/file/BoozCo-Campaigns-to-Capabilities-Social-Media-and-Marketing-2011.pdf
60. World Economic Forum. (2014). *The Global Competitiveness Report 2013-2014.* Davos-Klosters, Switzerland. Retrieved from http://www.weforum.org/reports/global-competitiveness-report-2013-2014
61. Wu, I. L., & Chen, E. L. (2005). An extension of trust and TAM model with TPB in the initial adoption of on-line tax: an empirical study. *International Journal of Human-Computer Studies,* 62, 784–808.

CHAPTER 10

CROSS-CUTTING TECHNOLOGIES: KEY TO INDUSTRY GROWTH

CHANDRAN ELAMVAZUTHI, PHD
Senior Director, Corporate Research Strategy
chandran@mimos.my

MIMOS BERHAD
www.mimos.my

ABSTRACT

Our domestic market is too small to drive the domestic ICT industry. Without healthy demand, there will be no healthy industry growth. Our industry needs to venture out – being 'kampung king' is not an option anymore. 'Innovate or die' has become a truism. Today, innovation means speed to market so we can outrun competitors; it means patented novel products/solutions/services so we can demand premium prices; and, it also means delivery of value for money so we can be sought after. To accelerate the growth of our ICT industry, we advocate the use of the Open Innovation Platform (OIP) / Open Innovation Framework (OIF) concepts founded upon the principle of cross-cutting technologies to rapidly develop needs-driven high–impact products and solutions, and in the process build a sustainable ICT ecosystem.

1.0 INTRODUCTION

Technologies lead to the development of products and services; hence, company growth and performance. Growth of companies in size and numbers would, in turn, lead to the growth of existing industries or the creation of entirely new industries. Industry growth would bring in Foreign Direct Investment (FDI), create new jobs and establish branding – all vital ingredients towards establish industry competitiveness.

For the Malaysian ICT industry to be globally competitive, it has to develop world-beating innovation products and solutions. For these products and solutions to hold their own in the global markets, they must incorporate home-grown (indigenous) technologies, and whose novelty is protected by Intellectual Property Rights (IPRs).

The question to ask is: *How can we accelerate the growth of the domestic ICT industry to rocket it into the global arena?*

Based on our experience in developing technologies and working with the local industry, we attempt to answer this question by putting forth several ideas that taken together could help speed up the growth of the local ICT industry. In section 2.0, we give an overview on the trends and convergence of technology (with respect to ICT). We follow this, in section 3.0, with an overview of the path of technology development towards meeting market needs. We detail this development path in section 4.0 using MIMOS' Innovation Value-Chain Model which is based on the Open Innovation Platform (OIP)/Open Innovation Framework (OIF) concepts. In this context, we also touch upon the critical need for talent specialization. In section 5.0 we give two examples of how OIP/OIF-driven cross-cutting technologies help in the rapid delivery of solutions to market problems and elaborate how this process could be used to spur industry growth. In section 6.0, we summarize the merits of using the OIP/OIF-driven technology recombinant strategy to move the industry forward.

2.0 TECHNOLOGY CONVERGENCE: AN OVERVIEW

2.1 FUNDAMENTAL TECHNOLOGY TRENDS

The DNA of ICT is 'Devices, Networks and Applications' – devices for computing, networks for communicating and applications for doing useful tasks. The trend for some time has been for computing devices to become smaller and smaller and this is still continuing. With respect to networking, it has been all about connecting up every device, thus giving rise to concepts such as Internet-of-Things or Internet-of-Everything. To cope with the constant demand for new services, applications are getting smarter by the day. Hence, it would not be wrong to tag the ICT evolution as 'smaller, smarter and surround-sensing'. Figure 2.1 pictures the fundamental ICT drivers and scenario just described.

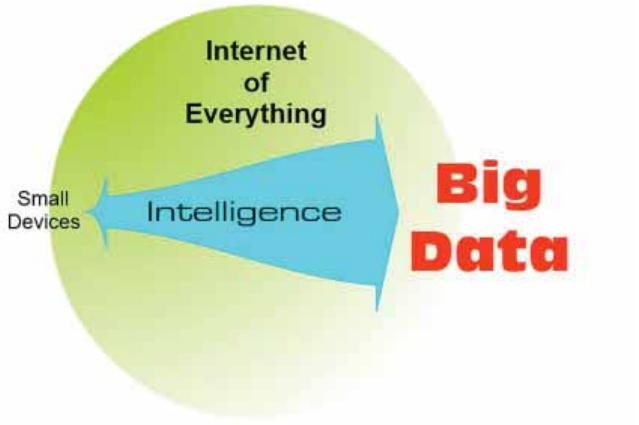


Figure 2.1: 'Smaller, Smarter and Surround-Sensing'

Gartner Nexus of Forces identifies four intertwined forces to create a user-driven ecosystem of modern computing.	IDC's 3rd Platform also identifies four technology focus areas.	The Open Group's Open Platform 3.0™ is centered around 4 - 6 technology trends converging to form new business models and system designs.	IEEE Computer Society's Top 10 Technology Trends for 2014
• Information	• Big Data/Analytics	• Big Data	• From Big Data to Extreme Data
• Mobile devices	• Mobile Broadband	• Mobility • Devices	• Next-generation mobile networks • From Internet of Things to Web of Things
• Social	• Social Business	• Social Networks and Social Enterprise	• Supporting New Learning Styles
• Cloud	• Cloud Services	• Cloud computing	• Emergence of the Mobile Cloud • Scientific Cloud Computing
		• Application architectures	• Smart and Connected Healthcare • E-Government • 3-D Printing • Balancing Identity and Privacy

Table 2.1: Broad comparison of technology trends by 'Technology Watchers'

2.2 WHAT DO 'TECHNOLOGY WATCHERS' SAY?

Table 2.1 broadly compares the technology trend predictions of Gartner, IDC, Open Group and IEEE.

It can clearly be seen that all four 'technology watchers' concur on the key technology trends/ technology areas with respect to ICT. The message is one of 'technology convergence' – the technology focus areas identified are closely interwoven.

We are, thus, looking at an 'ecosystem' of technologies – multi-technology – approach to delivering solutions to problems. This is clearly illustrated in Figure 2.2 which shows the coming together of multiple technologies to deliver technology-based solutions for the 2014 FIFA World Cup.[1]

The take-away here is that market needs/ problems require total end-to-end solutions, and these invariably can only be developed by using a number of different technologies.

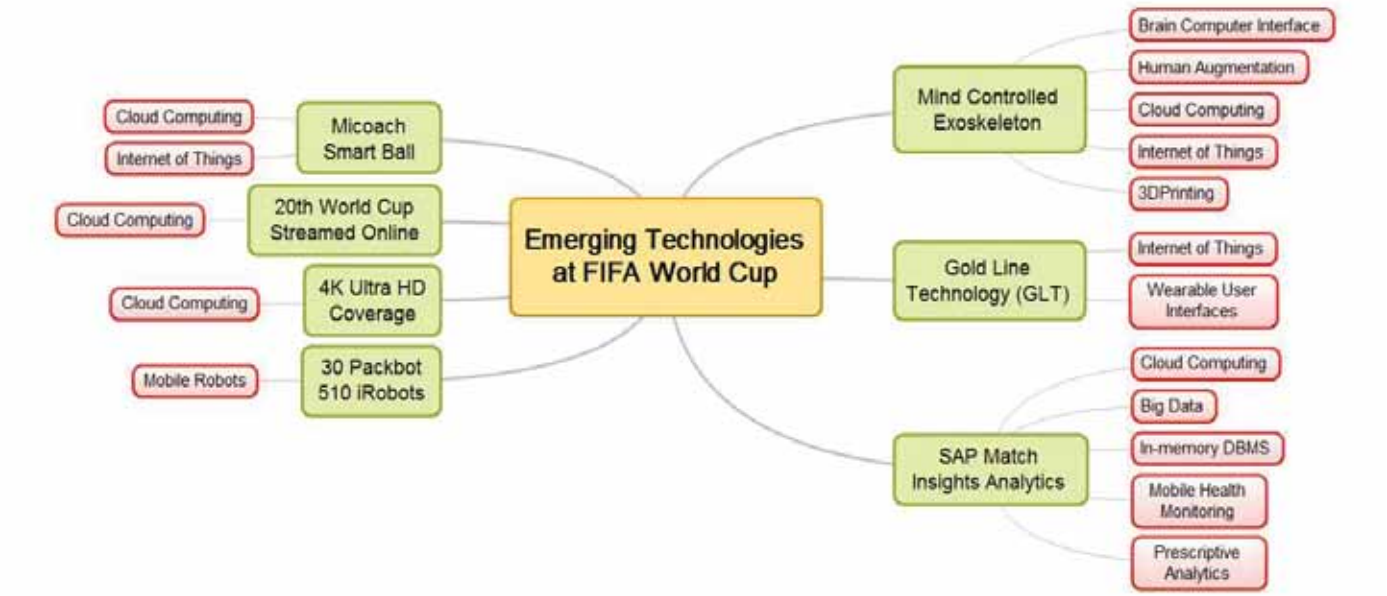


Figure 2.2: Technology Convergence at World Cup 2014

3.0 TECHNOLOGY TO MARKET VERTICAL: AN OVERVIEW

3.1 NEEDS TO NOVELTY AND VICE-VERSA

Figure 3.1 captures in a simple manner the requirements-to-research path. Needs/problems can come from any market segment. A thorough understanding of the customer's pain-points is critical in identifying a potential solution (application) to alleviate the 'pain points'. A clear idea of the potential solution is critical for identifying the technology challenges that need to be overcome in developing a good solution/application. Technology challenges, in turn, pave the way for possible research that may lead to novel ideas. This Needs-to-Novelty value-chain is in fact the R-D-C value-chain, but top-down. Bear in mind that in reality there will be many feedback-back loops amongst the various levels/phases.

Let us now turn our attention to Figure 3.2, which adds a little more detail to the Needs-to-Novelty value-chain just described. The solutions/applications are developed on top of Open Innovation Platforms (OIPs)/Open Innovation Frameworks (OIFs). An OIP is a 'scaffold' that integrates a number of technology modules and which is 'open' for improvement by anyone (e.g., university, research institute or industry). It is modular, scalable and reconfigurable and amenable to rapid development of vertical applications or products. On the other hand, an OIF is essentially a 'platform-of-platforms'. Thus, the Common Framework illustrated consists of a common set of platforms that provide various core functionalities. Notice that atop

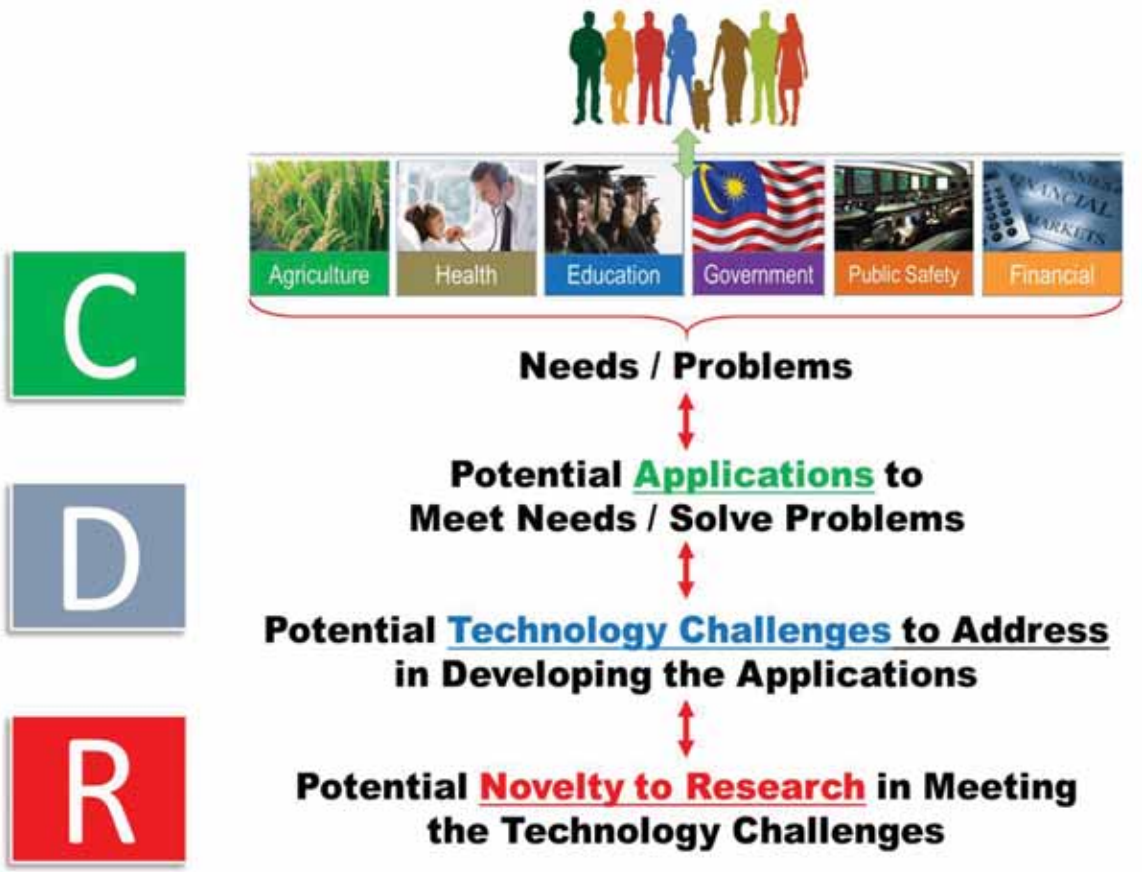


Figure 3.1: Needs-to-Novelty Value Chain

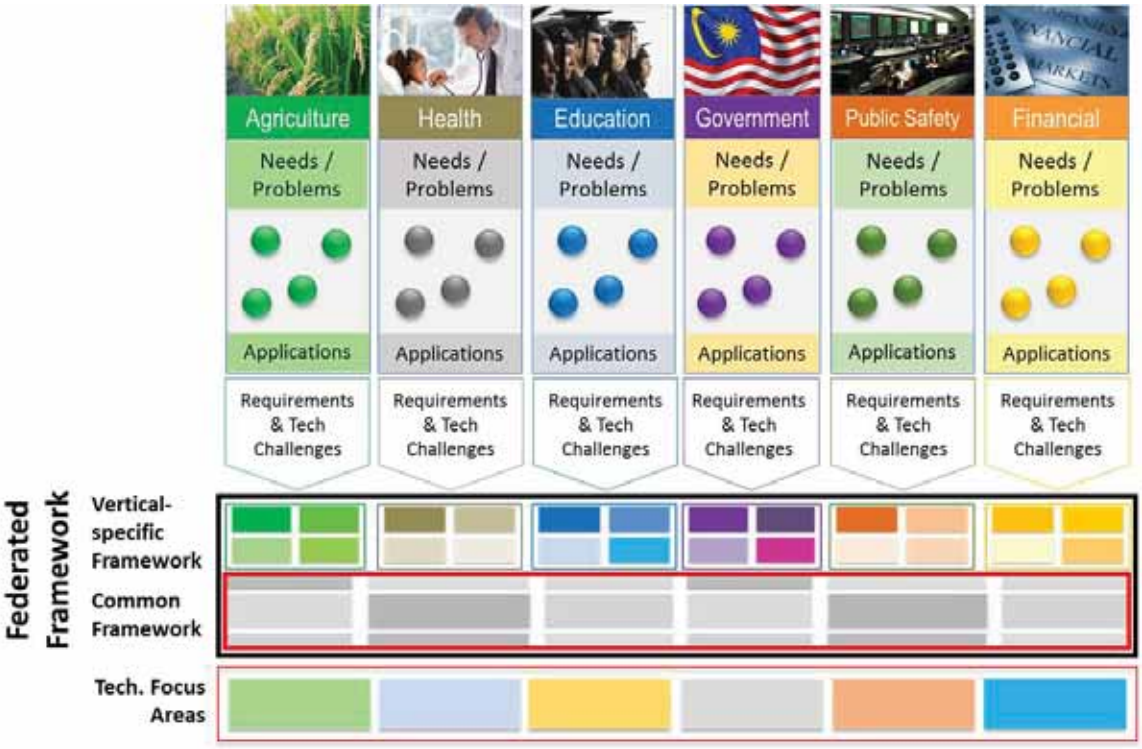


Figure 3.2: Addressing market needs through cross-cutting technologies founded upon OIPs and OIFs

this Common Framework reside a number of market segment (vertical-specific) frameworks. Hence, the Common Framework provides the cross-cutting products/technologies that are selectively used by the vertical-specific frameworks.

In the framework context, the platforms could also be considered as 'products'. You could, therefore, rightly interpret the vertical-specific applications developed on top of the OIF as solutions consisting of integrated sets of products

The above 'layered' approach to developing applications lends itself well to the rapid development of products/solutions and increases speed-to-market manifold. More is said on this approach in section 4.1 when we detail the MIMOS' Innovation Value Chain.

3.2 NEEDS-TO-NOVELTY VALUE CHAIN ANALYSIS: AN EXAMPLE

Figure 3.3 illustrates the needs-to-novelty process using an example from literature. [2] We will not delve into it further since it is self-explanatory.

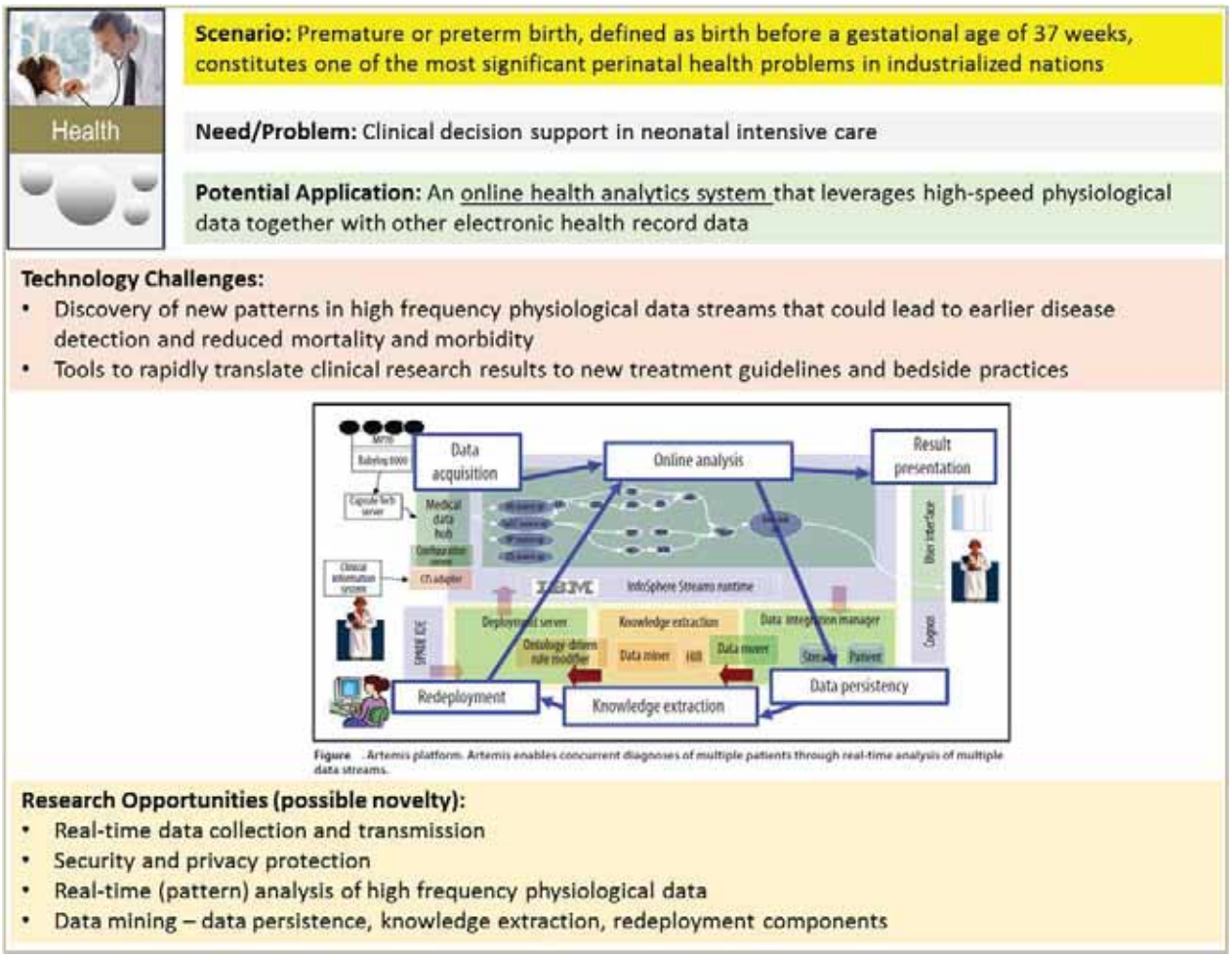


Figure . Artemis platform. Artemis enables concurrent diagnoses of multiple patients through real-time analysis of multiple data streams.

Figure 3.3: An example of addressing market problems through technology solutions

4.0 TECHNOLOGY RECOMBINANT STRATEGY

4.1 MIMOS' INNOVATION VALUE CHAIN

Figure 4.1 illustrates our technology recombinant strategy. The top graphics, technology to market, depicts the R-D-C / innovation value-chain (IVC).[1] Essentially, the Applied Research phase covers the research and the development of robust technology components possessing certain features or functionalities. The Development phase covers three areas i.e. platform, framework and, product and solutions. The Commercialization phase covers part of product/solution area as well as technology transfer and market.

You will notice that there is an overlap in activities at the transition of the phases i.e. at platform and, product and solution areas. This is to be expected as there is a need for feedback and corrections. The platform architects and implementers may want the technology components to be tweaked to meet their requirements. On the other hand, there needs to be dialogue between the platform/ framework developers with those developing the products/solutions so as to ensure requirements are met.

Technology is usually delivered in the form technology components, having certain features/functionalities. The components are incorporated into appropriate platforms. Framework, in our parlance, denotes the stitching together of a number of platforms; in other words, a framework is 'platform-of-platforms'. Products are developed using the platform as the basis or 'chassis'. On the other hand, the framework forms the basis for developing solutions. By solution, we imply the end-to-end means to solve a given problem. A solution will contain a number of integrated products to give the desired functionalities.

To test the efficacy of our platforms, we develop proofs-of-concept (PoCs) of products in accordance with prevailing market needs. Sometimes this is done together with vested technology recipients. However, developing solutions is a different ball-game. You need to first understand the problems i.e. the customer pain points thoroughly before putting a

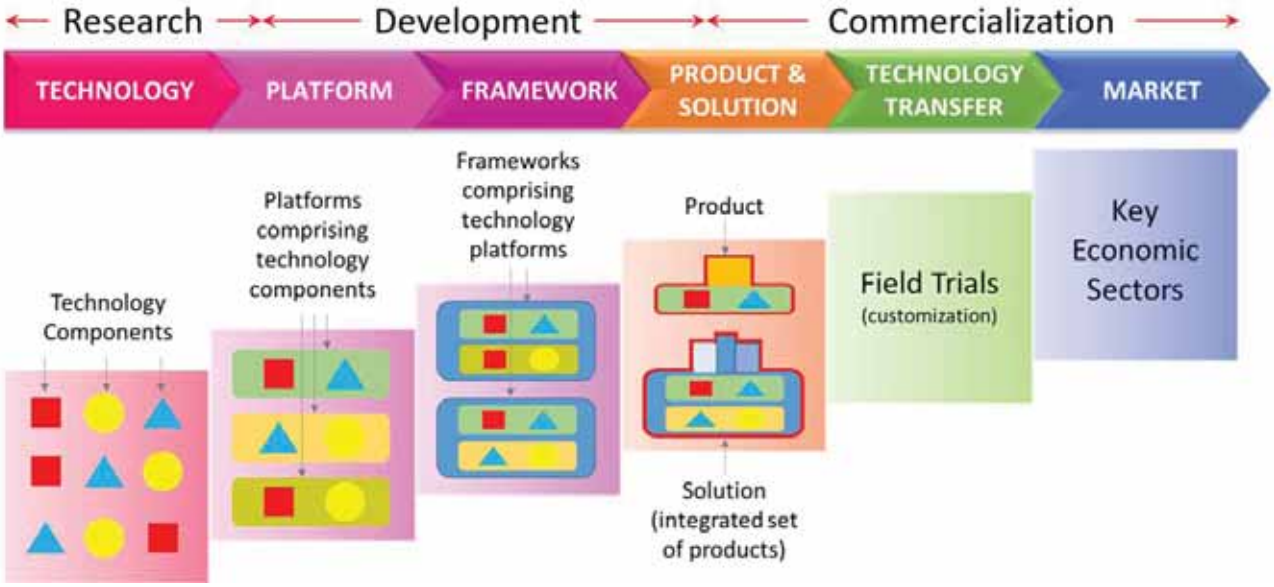


Figure 4.1: MIMOS' Innovation Value Chain

1. *For simplicity, the innovation value-chain is shown as linear. In reality, there will many feedback loops; these are not shown to avoid clutter.*

solution together. Therefore, solution PoCs are not normally developed unless and until a real need and a real customer has been identified.

Technology transfer involves handing over a technology platform / framework or a product / solution PoC to technology recipients. Technology transfer is critical to the success or failure of a platform / framework / product / solution. It involves knowledge transfer, which is a difficult task to accomplish. If a product / solution PoC is jointly developed with technology recipients, it eases the problem of knowledge transfer to some extent. We manage this issue of knowledge diffusion by involving the technology recipients in the live implementation of a product / solution. These 'field-trials' will give hands-on experience and learning when technology recipients learn to address the unforeseen issues that usually arise when deploying the product / solution. The issues could be with respect to meeting customer requirements in terms of functionalities, scalability or robustness of the product / solution.

Field-trials also help to build track-record and hence, to get traction in the market.

When we talk of markets, we mean the key economic sectors. What major problems do these sectors face that could be addressed by ICT solutions? That's how we aim to create big economic impacts!

4.2 TALENT SCOPING: SPECIALIZATION FOR SPEED TO MARKET

As you have seen, the IVC is made up of a number of integrated phases. From the many phases described in the innovation value chain, you can discern that the skillsets required in one phase differ from another.

A perspective on skill-sets is given by the T-model which explains the knowledge-depth versus knowledge-breadth dichotomy. This T-model is depicted in Figure 4.2.

You will see that at the research end, the 'T' is 'deeper' whilst at the product development end it is 'broader'. This means that by virtue of their nature of work, researchers have in-depth knowledge of a narrow field of area. On the other hand, developers have broader knowledge of many areas but lack research

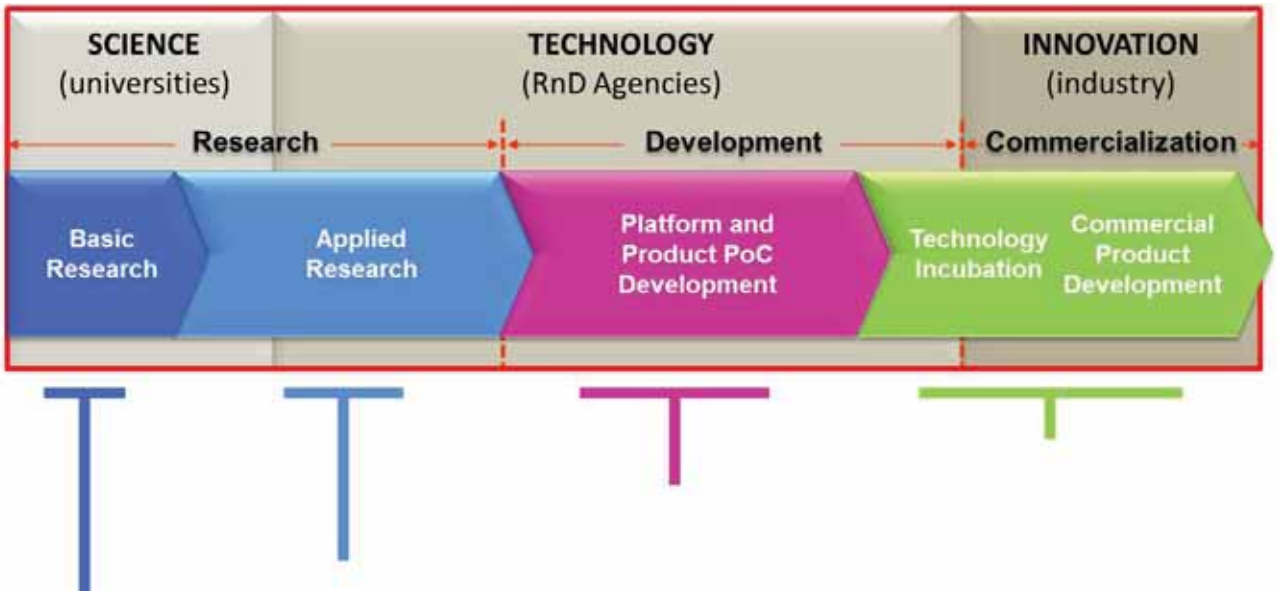


Figure 4.2: The T-Model for RDnC Skill-sets

depth. Succinctly put, going from left-to-right, in general, knowledge is 'more of less' and progressively gets 'less of more'!

It should be emphasized here that the knowledge and skill-sets required for science, technology and innovation work, respectively, are different and seldom reside under one roof.

In view of this, science research should be the dominant play of the universities; technology development, the dominant play of R&D agencies; and, innovation of commercializable products and solutions, the dominant play of the industry (firms).

This would enable the innovation pipeline to be continuously fueled with new ideas, new knowledge, novel intellectual properties, cutting-edge technologies leading to innovative products and solutions. However, there is bound to be some overlap in activities and this is to be expected. But this critical issue of specialization must be addressed to ensure the innovation pipeline works the way it should!

5.0 STITCHING SOLUTIONS: MIMOS' EXPERIENCE

5.1 EXAMPLES OF THE USE OF CROSS-CUTTING TECHNOLOGIES TO REALIZE INDUSTRY-GRADE SOLUTIONS

Figure 5.1 details MIMOS IVC process (explained earlier in section 4.1) with a real-life solution we have developed.

The customer was SOCSO and the problems was one of upgrading their proprietary

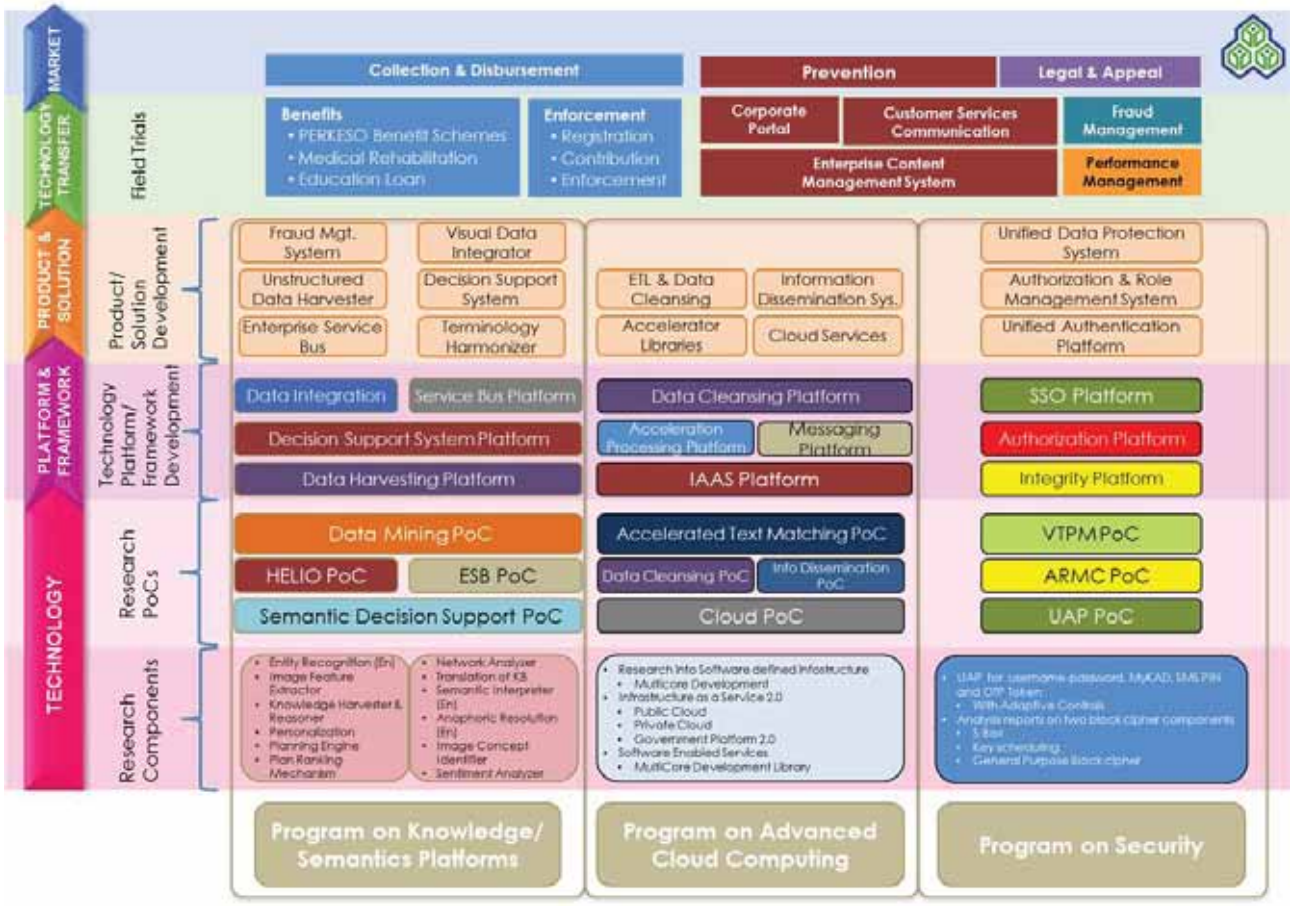


Figure 5.1: OIP and OIF driven solution (Government market segment)

Information Management System to one that is non-proprietary and current.

Three research programs contributed to the development of the research components that eventually went into the platforms. These were Knowledge/Semantics, Cloud Computing and Security. The Research PoCs (proofs-of-concept) comprise research components to validate their viability to deliver functionalities. All the platforms developed went into the development of the framework which incorporates the 'products' developed. The judicial combination of the 'products' delivered the various functionalities for the final solution.

Figure 5.2 illustrates the IVC for the agriculture market segment. Moving from Figure 5.1 to Figure 5.2, you can see that three more research programs have been added. Their inclusion was necessary to deliver the additional functionalities required. The figure shows three solutions i.e., aquaculture, greenhouse management and oil palm pollination.

The point to note is that we have reused the platforms/products from the SOCSO framework for these solutions. Looking the other way around, we can say that we have augmented the SOCSO framework with additional platforms/products to meet the additional/new requirements.

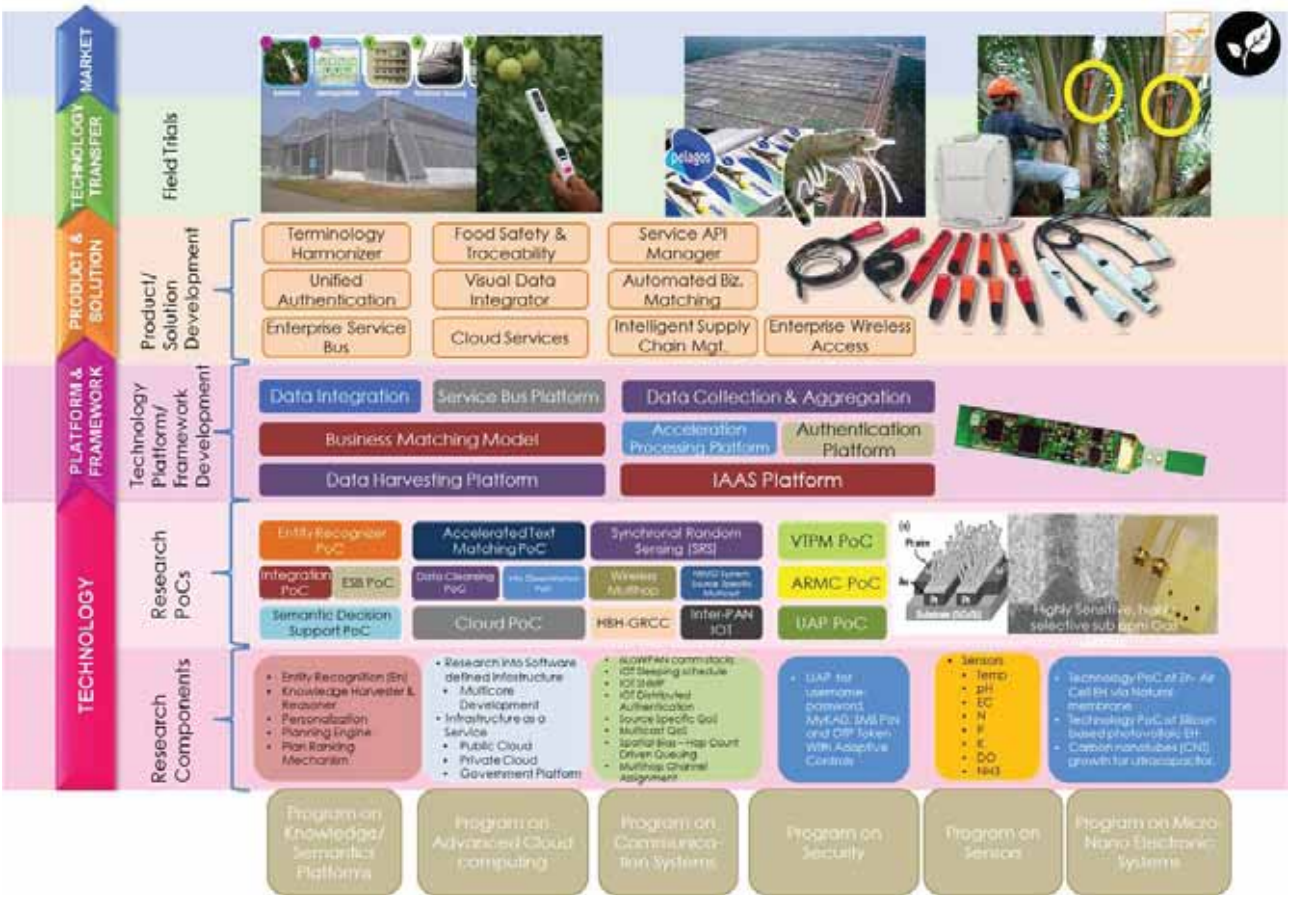


Figure 5.2: Cross-cutting technologies reused via OIPs and OIF to deliver solutions in another market segment (Agriculture)

5.2 GROWING DOMESTIC INDUSTRY THROUGH CROSS-CUTTING TECHNOLOGIES

Seeding the local industry consortia is done through implementing large government projects with potential big economic impact. It has to be a government project because we need trial sites to build track records and no private entity would take this calculated risk or make the commitment. Hence, government support is absolutely necessary.
Large projects give us an opportunity to involve and collaborate with as many industry players as possible, both big and small. By providing a suitable Foundational Framework (comprising several integrated technologies and platforms), vendors could develop the necessary verticals of their specialization towards creating integrated products or solutions of high impact. This is shown in Figure 5.3.

The Framework sets the standards for the various vendor verticals to co-exist and interoperate harmoniously. The coming together of the various industry players could pave the way for the formation of an entity of formidable technology might to take on the global 'Big Boys'!

The entity or consortium is usually led by an anchor Large Domestic Company (LDC).

A number of such consortiums could be formed by working on key high-impact ETP/GTP projects targeting the various economic sectors such as health, education, and agriculture as well as the government sector.

6.0 SUMMARY

In this paper we have discussed several concepts that put together in practice could help the domestic ICT industry to grow in strength and increase productivity.

The key (twin) concepts are Open Innovation Platform (OIP) and Open Innovation Framework (OIF), the latter being the logical extension of the former. The OIP/OIF enables the rapid development and deployment of products/ solutions by virtue of the fact that they supply tested and proven core functionalities/

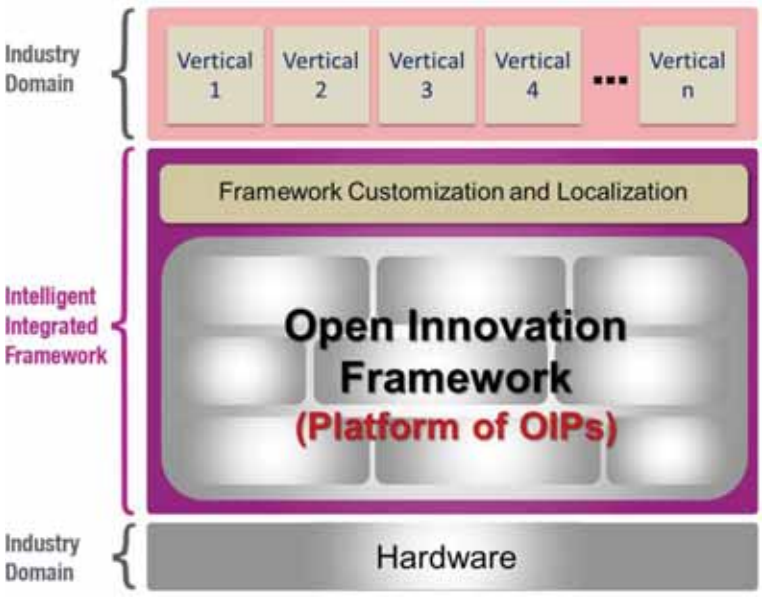


Figure 5.3: Model for developing industry consortia

capabilities that need not be duplicated whenever a new product/solution is developed. This benefit arises due to the application of the principle of cross-cutting technologies.
Since much of the risk involved in technology development has been minimized, the industry could boldly use the platforms/frameworks for innovative product/solution development.

It follows, therefore, that the avoidance of overlapping/duplication activities would in fact increase greatly speed-to-market of new products/ solutions.

Further, by definition and design OIP/OIF are 'open'; hence, collaborators are able to contribute to the enhancement of the OIPs/OIFs to better serve existing market segments as well as to position them for new market segments.

Innovation is synonymous with collaboration because it involves many complex tasks that are just not doable by one party. Since the OIP/OIF can bring together many RDnC parties to a common table, they are also enablers of innovation.

In relation to this, the T-Model argues for the case of 'domain' specialization so that we can grow many domain experts who working together can deliver more rather than having 'Jacks of All Trades' and going nowhere!

The OIP/OIF mode of working is by design suited for tackling large high-impact projects. Large projects imply active collaboration and will bring on board many vendors/industry players. This will directly contribute to the growth of industry through development of patented products/solutions. It would also help in the diffusion of knowledge and provide valuable experience and learning to all players, especially the 'smaller' SMEs.

The greatest gain at the end of the day would be the building of trust amongst all players and the cementing of existing ties between them. This 'unity in diversity' will go a long way in creating an ICT RDnC Ecosystem and specifically, a dynamic domestic ICT industry capable of competing against the best in the world.

REFERENCES

1. Irena Bojanova, IT Enhances Football at World Cup 2014, IT Pro, July/August 2014, pp. 12-17.
2. Carolyn McGregor, Big Data in Neonatal Intensive Care, IEEE Computer, June 2013, pp. 54-59.

Persatuan Industri Komputer Multimedia Malaysia
(The National ICT Association of Malaysia)

E1, Empire Damansara
No 2, Jalan PJU 8/8A Damansara Perdana
47820 Petaling Jaya, Selangor Darul Ehsan
T: (603) 4065 0078
F: (603) 4065 0079
e: info@pikom.my
w: www.pikom.my

ISSN 2180-2548

PIKOM, the National ICT Association of Malaysia, is a not-for-profit organisation. It is the largest association representing information and communications technology (ICT) players in Malaysia. Since its inception in 1986, PIKOM has come of age as the voice of the ICT industry. It has become an ICT referral centre for government and industry players, as well as international organisations. In this regard, PIKOM takes on the responsibility to publish ICT-relevant information in a periodic manner.

Design, production and printing by: MJLAIKC INFOWORKS | Tel: 6012 5050862 | E: mjlaikc@gmail.com