BEYOND COMPLIANCE:

THE STATE OF CYBER RESILIENCE IN MALAYSIA 2026

CYBERSECURITY

by PIKOM

Published by:

PIKOM

E1, Empire Damansara,
No. 2, Jalan PJU 8/8 A, Damansara Perdana
47820 Petaling Jaya, Selangor
T : +(603) 7622 0079
E :info@pikom.org.my
W :www.pikom.org.my

Release date: April 2026

TABLE OF CONTENTS

PIKOM Chairman's Message: The Resilience Imperative

Adj. Practice Prof. Alex Liew

As we convene for the **Future of Cybersecurity Summit (FOCS) 2026**, I look back at the journey we began with PIKOM's inaugural cybersecurity landscape report in 2024. Two years ago, our conversations centered on protecting databases and hardening perimeters; today, the narrative has fundamentally shifted. We are no longer merely discussing "IT security", we are discussing **National Economic Stability.**

The intervening 24 months have seen a relentless evolution in the threat landscape. The rise of **AI-powered attacks**, including deepfake impersonations and automated vulnerability scanning, has proven that traditional defenses are no longer enough. Furthermore, the enforcement of the **Cyber Security Act 2024** has signalled a new era of accountability for National Critical Information Infrastructure (NCII).

However, legislation alone cannot secure our future. My call to action for Malaysia c-suites and boardrooms is clear: we must move beyond **"check-the-box"compliance.** True resilience is not found in a static certificate on a wall, but in a proactive culture that treats cybersecurity as a core business pillar.

As we navigate the complexities of **Zero-Trust architectures, cloud-native security**, and the looming challenges of **quantum computing**, let this 2026 report serve as your benchmark. Together, we can ensure that Malaysia remains a trusted, secure and resilient hub in the global digital economy.

Also taking this opportunity to thank the sponsors who have made FOCS 2026 and in particular this publication a success.

Finally, I would like to convey my heartfelt appreciations to PIKOM Cybersecurity Chapter team including the Chair Mr. Desmond Teo for this initiative and also the PIKOM Research Committee (2026) for their relentless effort in producing this report.

Message from PIKOM Cybersecurity Chapter Chair

Desmond Teo

On behalf of the PIKOM Cybersecurity Chapter, I would like to extend my profound gratitude to the individuals and organizations whose dedication made the **State of Cyber Resilience in Malaysia 2026** report possible.

First, my sincere thanks go to our **Sponsors**. Your visionary support and investment in this project including the Future of Cybersecurity Summit 2026 (FOCS). This event demonstrates a shared commitment to elevating Malaysia's digital defences. This publication is more than just a report; it is a vital tool for national benchmarking that would not have reached this scale without your partnership.

I also wish to recognize our **Research Team**. Your tireless efforts in designing this follow-up to our 2025 survey and analysing the complex data surrounding AI-powered attacks, ransomware evolution and Zero-Trust adoption have been exemplary. By aggregating and anonymizing these critical industry insights, you have provided a clear, evidence-based roadmap for our members and the wider nation.

Finally, thank you to the respondents including our members. Your participation is what transform these statistics into a living narrative of our collective resilience. We look forward to discussing these findings furtherat the **Future of Cybersecurity Summit 2026**.

Preface - PIKOM Research Committee Chair

Woon Tai Hai

In today's hyper-connected digital landscape, cybersecurity stands as one of the most critical pillars of organizational resilience, economic stability, and national security. As businesses, governments, and individuals increasingly depend on interconnected systems, cloud computing, artificial intelligence (AI), and the Internet of Things (IoT), the risks posed by cyber threats have escalated dramatically.

Closer to home in Malaysia, these global pressures are acutely felt amid rapid digital adoption under the Malaysia Digital Economy Blueprint and the National Cyber Security Strategy 2025-2030. Cybersecurity Malaysia and MYCERT data indicate and billion ringgit online scam losses.

Regardless, the momentum of Malaysian digital economy continues to accelerate at an unprecedented pace, bringing with it transformative opportunities alongside increasingly complex cybersecurity risks. Since PIKOM's last cybersecurity survey in 2024, the threat landscape has evolved significantly shaped by rapid cloud adoption, artificial intelligence advancements, expanding digital ecosystems, and new regulatory expectations. Against this backdrop, cybersecurity is no longer solely a technical concern but a fundamental pillar of business resilience, national competitiveness, and trust in the digital ecosystem.

The PIKOM Cybersecurity Survey 2026 was commissioned to provide and updated and evidence-based view of the cybersecurity posture of Malaysia's technology industry and its broader business environment. This study serves as a follow-up to the 2024 assessment, enabling meaningful benchmarking while capturing emerging realities that organisations now face between 2024 and 2026.

The questions in this survey were intentionally designed with dual objectives. First, to measure quantifiable shifts in cybersecurity maturity, including incident prevalence, investment levels, workforce capabilities, adoption of Zero-Trust architectures, cloud transformation and the use of AI-driven defence mechanisms Second, to capture deeper qualitative insights into how organisations are experiencing and responding to new forms of cyber risk, ranging from AI-powered attacks and ransomware evolution to supply-chain vulnerabilities, regulatory compliance under the Cyber Security Act 2024, and preparedness for future challenges such as quantum computing threats.

Beyond measuring risk exposure, the survey seeks to understand intent; how Malaysian organisations are adapting strategies, strengthening resilience, and redefining governance in response to an increasingly intelligent and interconnected threat environment. The inclusion of perspectives on cyber resilience, AI governance, and national policy impact reflects PIKOM's commitment to supporting a secure and sustainable digital economy aligned with Malaysia's Cyber Security Strategy and National Critical Information Infrastructure (NCII) priorities.

Importantly, this report is not merely a reflection of past incidents. It is a forward-looking assessment aimed at guiding industry-leaders, policymakers, and technology practitioners toward informed decisions. The findings are intended to:

- Provided industry benchmarks to supports organisational cybersecurity planning and investment.
- Highlight emerging systemic risks affecting Malaysian enterprises.
- Inform policy dialogue between industry and government.
- Strengthen collaboration across the digital ecosystem to enhance national cyber resilience.

As cyber threats become more sophisticated; increasingly leveraging automation, artificial intelligence, and cross-border attack vectors; collective awareness and coordinated action become essential. The insights contributed by participating organisations therefore represent more than survey responses; they form a shared foundation for shaping Malaysia's cybersecurity future.

PIKOM extends its sincere appreciation to all respondents and industry stakeholders whose participation makes this report possible. We hope the findings will serve as a catalyst for stronger partnerships, improved preparedness, and continued progress toward a trusted and secure digital nation.

Acknowledgment: This survey and publication is initiated by PIKOM Cybersecurity Chapter chair, Mr. Desmond Teo in collaboration with the PIKOM Research Committee (2026).

"Cybersecurity is no longer solely a technical concern but a fundamental pillar of business resilience, national competitiveness, and trust in the digital ecosystem"

PUBLICATION TEAM:

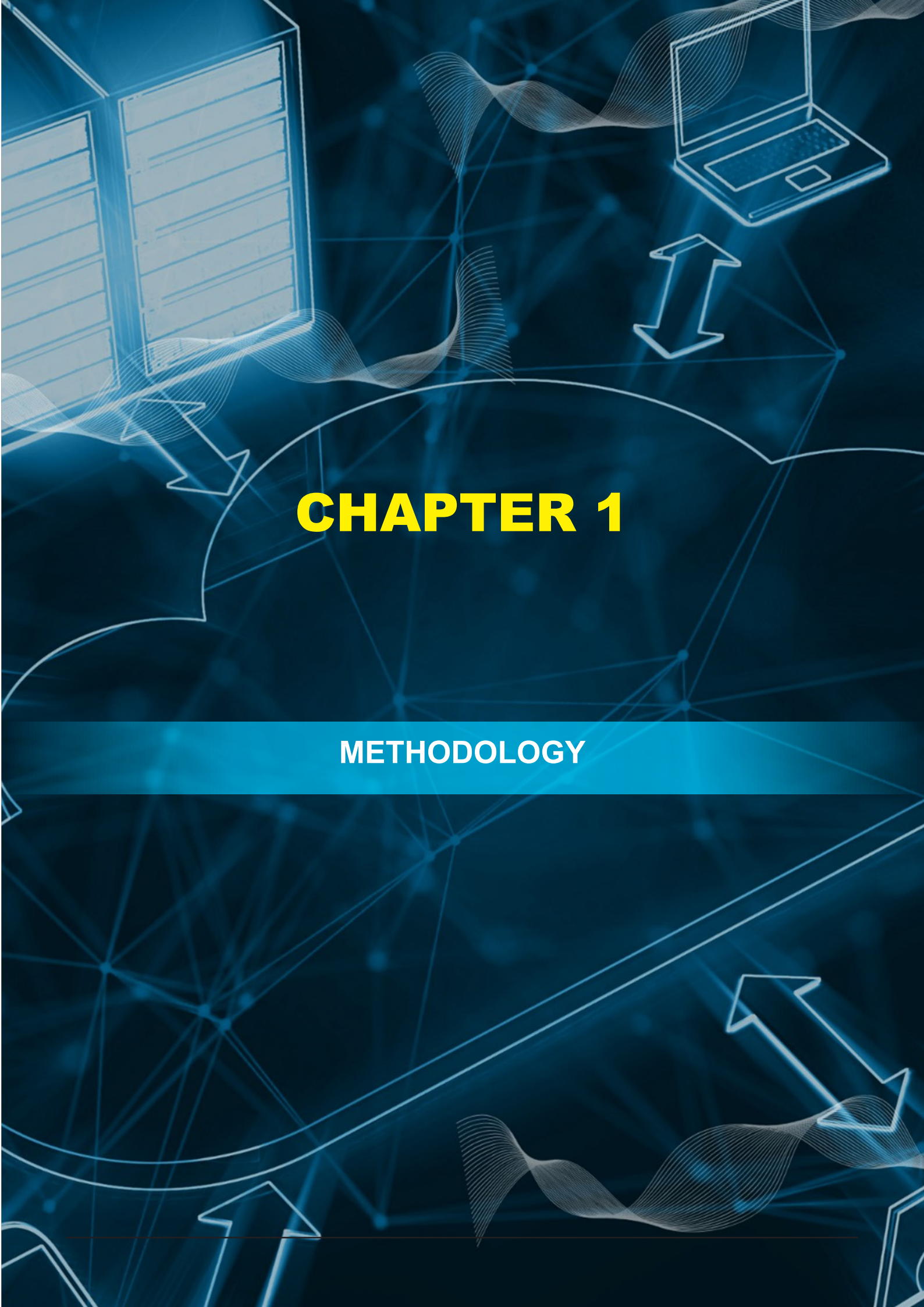
WOON TAI HAI
PIKOM RESEARCH COMMITTEE CHAIR

DESMOND TEO
PIKOM CYBERSECURITY CHAPTER CHAIR

RODNEY LEE
PIKOM CYBERSECURITY CHAPTER ADVISOR

ONG KIAN YEW
PIKOM CEO

NURUL ASYIQIN MOHD NASIR
PIKOM HEAD OF STRATEGIC RELATIONS & COMMUNICATIONS



CHAPTER 1

METHODOLOGY

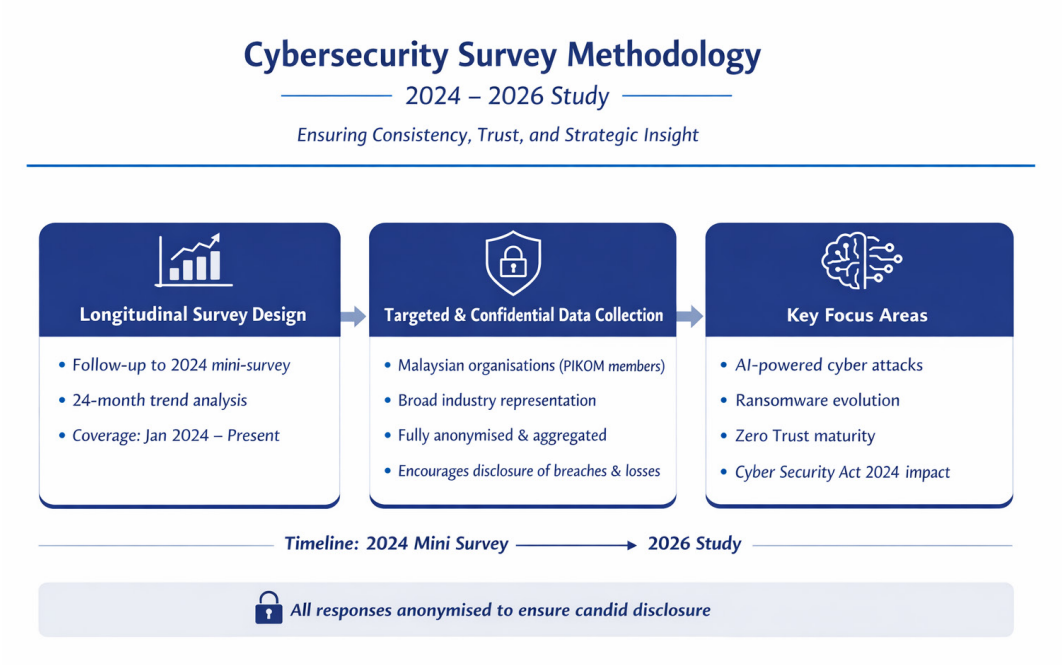
A Multi-Dimensional Approach

To ensure the **State of Cyber Resilience in Malaysia 2026** report provides both granular accuracy and high-level strategic foresights, a hybrid research methodology was employed, combining primary data collection with rigorous secondary research.

Primary Research: The 2026 Industry Survey

The primary data of this report is derived from a survey conducted in March 2026.

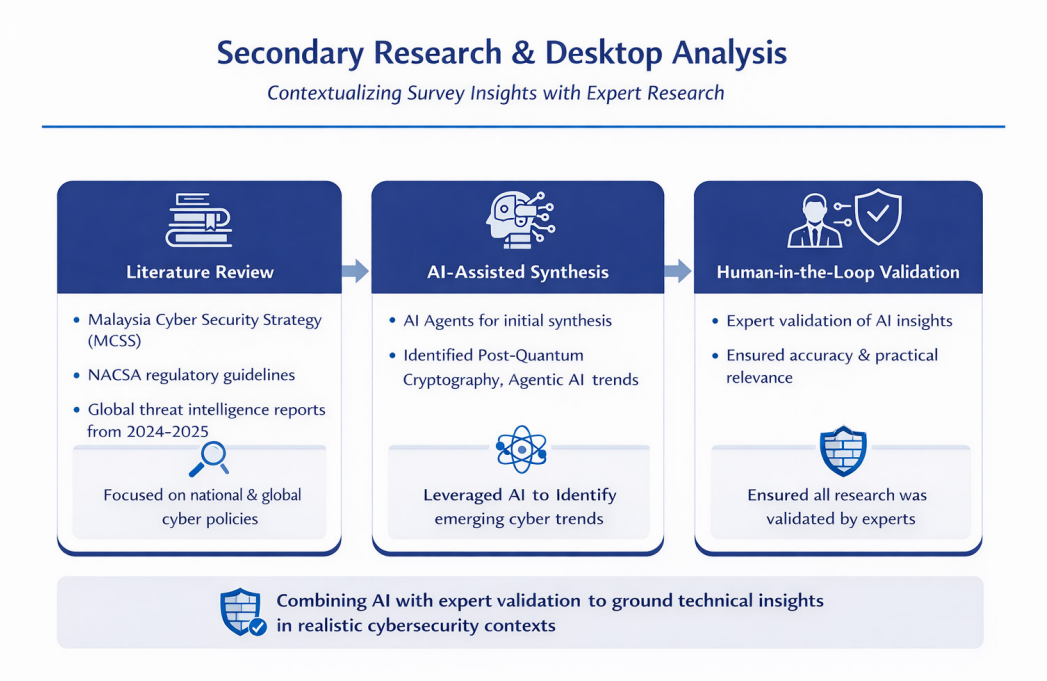
- **Survey Design:** The instrument was designed as a direct longitudinal follow-up to the 2024 mini-survey, allowing for trend analysis across a 24-month horizon (January 2024-present)
- **Targeting & Anonymity:** Responses were gathered from a broad spectrum of Malaysian organization largely from PIKOM Members. To encourage honest reporting of sensitive data-such as successful breaches and financial losses-all data was captured on an aggregated and anonymized basis.
- **Core Themes:** The primary data collection focused on AI-powered attacks, ransomware evolution, Zero-Trust maturity and the impact of the **Cyber Security Act 2024.**



Secondary Research & Desktop Analysis

To contextualize the survey findings, the project team also conducted extensive desktop research into the global and local cybersecurity landscape.

- **Literature Review:** Analysis included the Malaysia Cyber Security Strategy (MCSS), official NACSA regulatory guidelines, and global threat intelligence reports from 2024 and 2025.
- **AI-Assisted Synthesis:** In a reflection of the modern technology stack, the research team utilized AI Agents to assist in the initial synthesis of vast regulatory documents and the identification of emerging global trends such as Post-Quantum Cryptography and Agentic AI.
- **Human-in-the-Loop Validation:** To ensure the highest levels of practical accuracy, all AI-generated insights and survey data underwent human confirmation by the project team. This ”human-in-the-loop” approach ensured that technical data remained grounded in the practical realities and accuracy of the environment.



Demographics and Scope

The methodology was designed to capture a representative snapshot of the Malaysian industry and economy (which is always a challenge in a survey exercise; hence, secondary research was needed)

Another important factor ingrained in the survey is understanding how resilience scales with resources. To achieve this, respondents were grouped by workforce size, ranging from micro-SMEs to large-scale enterprises:

- SMEs: Organizations with fewer than 50 employees.
- Mid-Market: Organizations with 55 to 999 employees.
- Enterprises: Large-scale organizations with 1,000+ employees.

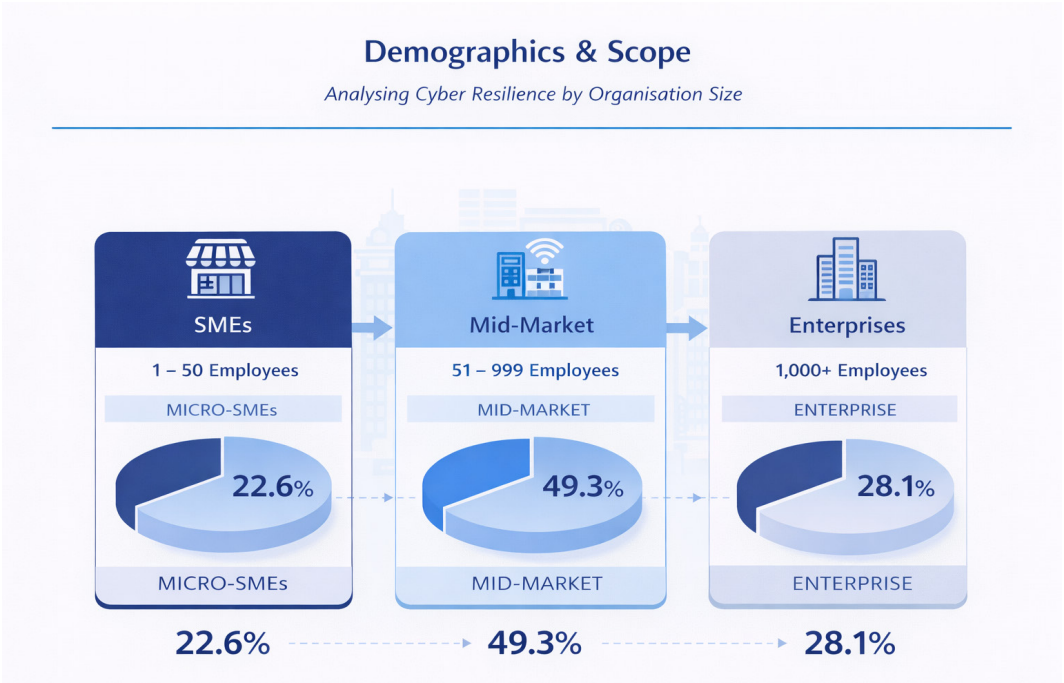


Figure 1: Respondents Grouping and response for PIKOM Cybersecurity Survey 2026

CHAPTER 2

Beyond Compliance: The Continuing Saga of Malaysia's Cybersecurity Landscape (2024-2026)

The narrative of Malaysia's digital defense has shifted from a series of isolated technical skirmishes to a sophisticated, high-stakes saga of national resilience. Since PIKOM published its first landmark report in 2024, the landscape has been reshaped by the "triple-threat" of AI-driven attacks, an evolving regulatory and compliance pressures, and a critical talent shortage.

As we look toward the Future of Cybersecurity Summit (FOCS) 2026, the latest industry survey reveals a nation moving beyond more "check-the-box" compliance toward a proactive, albeit challenging, posture of cyber resilience.

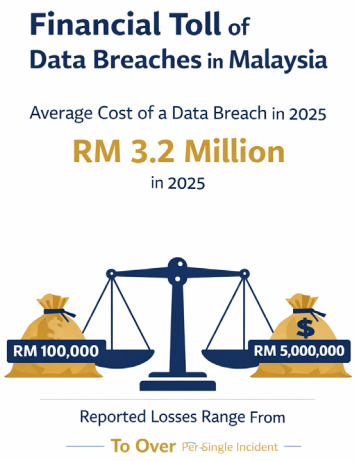
1. The Threat Evolution – AI and the Breach Epidemic

In 2024, AI-powered attacks were largely theoretical; by 2026, they are fully operational and relentless. Data from the past 24 months (Jan 2024 – Dec 2025) shows that successful breaches are no longer a matter of "if" but "how often".

- **The AI Pivot:** Organizations are now battling **deepfake impersonations**, quishing (QR phishing), and **agentic AI** that automates vulnerability scanning at scale. AI-generated phishing and deepfake impersonation were the most cited category among impacted organisations, ahead of traditional ransomware. Credential theft and quishing also ranked high. This suggests that the human attack surface remains central, but the tactics have become more convincing, faster, and harder to detect.

Figure 2: Extracted from PIKOM Cybersecurity Survey 2026

- **Financial Toll:** The average cost of a data breach in Malaysia climbed to **RM 3.2 million** in 2025. Within the current survey, organizations are reporting losses ranging from **RM 100,000** to over **RM 5 million** for single significant incident.



2. The Regulatory & Compliance Pressures – Cyber Security Act 2024

The most significant shift since the 2024 report is the enforcement of the **Cyber Security Act 2024**, which came into effect on June 26, 2024.

- **NCII Focus** – The Act mandates that National Critical Information Infrastructure (NCII) entities – spanning finance, healthcare and energy adhere to strict codes of practice and mandatory incident reporting.
- **The Cost of Non-Compliance:** Failure to implement these codes can result in fines up to RM 500,000 or imprisonment for up to **10 years**.
- **Strategic Impact:** This legislation is forcing a board-level shift, moving cybersecurity from an IT expense to a mandatory regulatory, operational and strategic pillar.

Whilst 2024 served as a foundation stone, 2025 clearly became the 'Implementation Crucible' for Malaysia's cybersecurity landscape. In essence 2024 was defined by the passing of new laws, 2025 was the year those laws met the reality of a rapidly evolving, AI-driven threat environment.

3. Modern Architectures – The Shift to Zero-Trust

As organizations migrate toward hybrid and cloud-based infrastructures (with many now operating **more than 40%** of their stacks in the cloud), traditional perimeter defences have crumbled.

- **Zero-Trust Adoption:** There is a marked transition toward **Zero-Trust architecture**, with many Malaysian firms now in the "partially implemented" or "planning" stages to verify every user and device regardless of location.
- **Defensive AI:** To counter AI-powered threats, organizations are deploying **AI/MLtools** for automated threat detection and SIEM (Security and Event Management) augmentation.

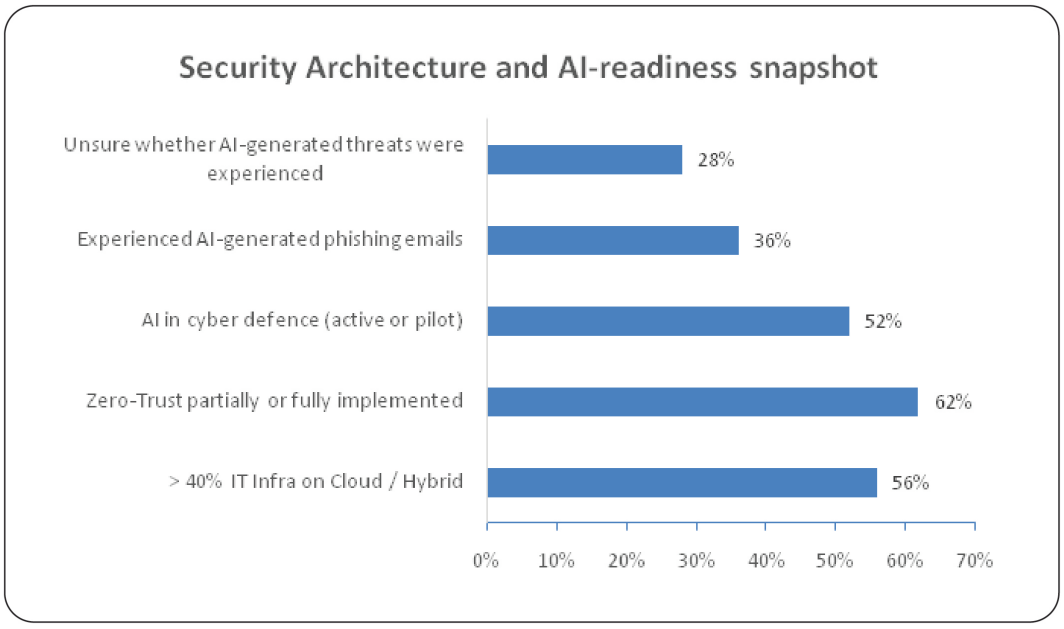


Figure 3: Extracted from PIKOM Cybersecurity Survey 2026

4. The Human Element: Talent and Spending

Resilience gaps in 2026 are shaped as much by economics and workforce capacity as by technology choice. Many organisations are attempting to modernise, but they are doing so with relatively modest budgets and very lean internal teams.

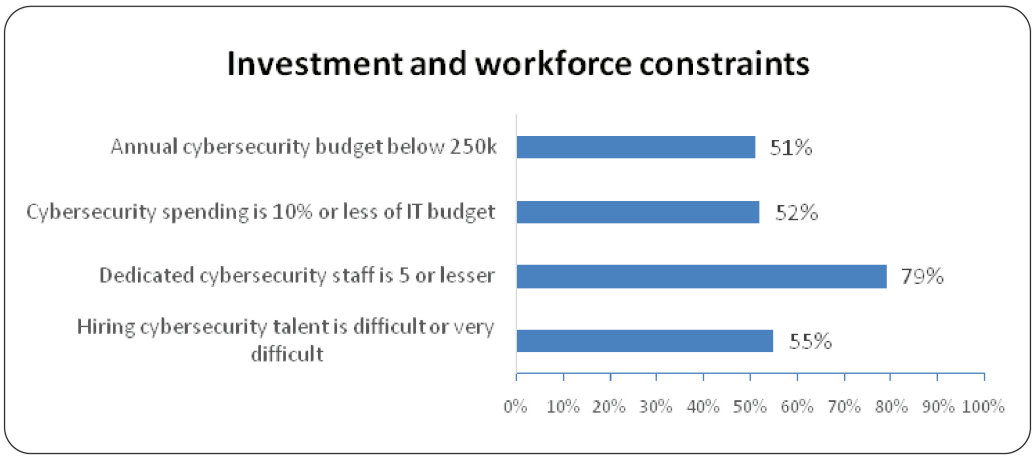


Figure 4: Extracted from PIKOM Cybersecurity Survey 2026

This is a structurally important result. When over half of respondents operate with cyber budgets below RM250,000 and more than three-quarters have five or fewer dedicated cyber staff, resilience becomes highly dependent on prioritisation, managed services, and good governance rather than on building large in-house specialist teams. The hiring picture reinforces this: difficulty recruiting talent is now a persistent operational drag, not a temporary inconvenience.

For SMEs and mid-market organisations, this means the path to resilience will often depend on pragmatic control choices: identity security first, disciplined vulnerability management, tested incident response, strong third-party onboarding, and selective use of managed detection, threat monitoring, and specialist assurance services.

5. Proactive Resilience: Testing the Defenses

The survey highlights a maturing approach to security assessments. While Vulnerability Assessments are now often continuous or monthly, more advanced “adversarial” testing is gaining traction:

- **Red Teaming:** Mimicking real attackers through technical and social engineering to test detection capabilities.
- **Compromise Assessment:** Forensic investigations designed to find hidden threats that have already breached the perimeter undetected.

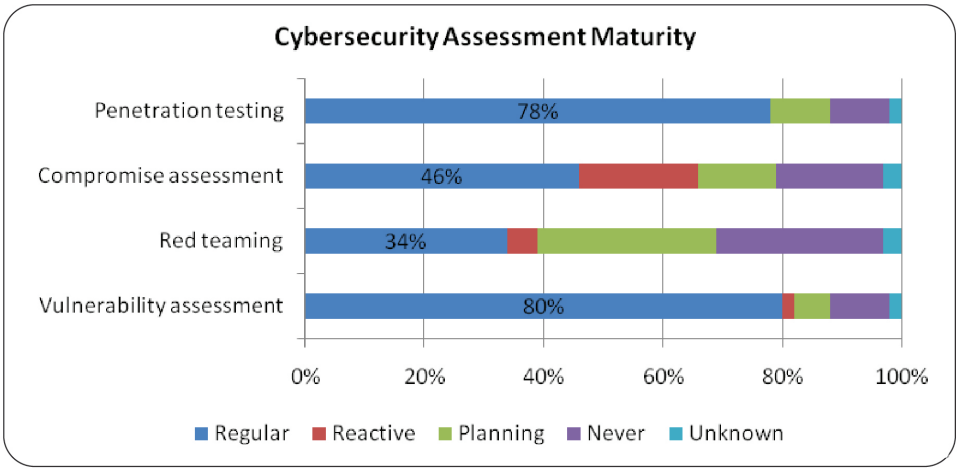


Figure 5: Extracted from PIKOM Cybersecurity Survey 2026

6. Third-party Cyber Risk Management & Emerging Tech Readiness

As we transition into high-tech digital economy, the 2026 landscape is also defined by two frontier technologies that represent both immense opportunity and systemic risk: Agentic AI, from "Content" to "Action" including path to AGI (Artificial General Intelligence) and Quantum Computing. Many Malaysian organizations are perhaps pivoting from experimentation to formal governance in these emerging domains. How many firms actually understands Embodied Intelligence and awareness and planning for Post-Quantum Cryptography (PQC)?

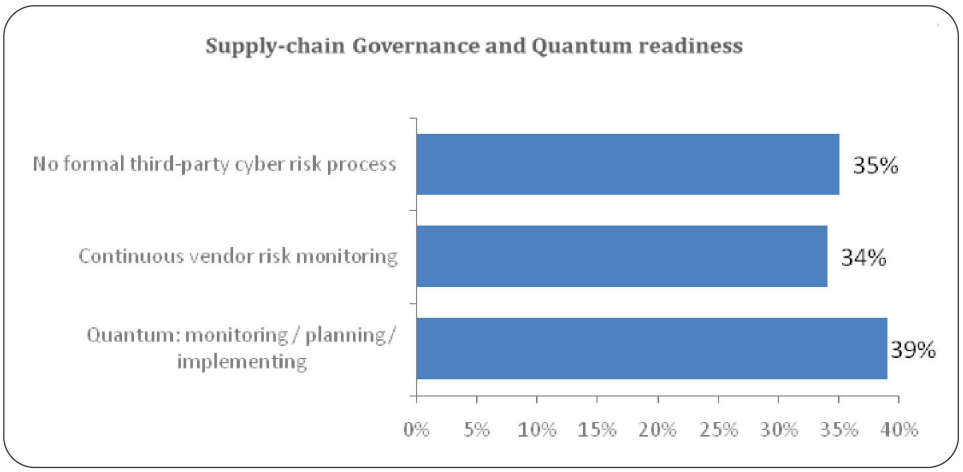


Figure 6:Extracted from PIKOM Cybersecurity Survey 2026

Conclusion: The Road Ahead

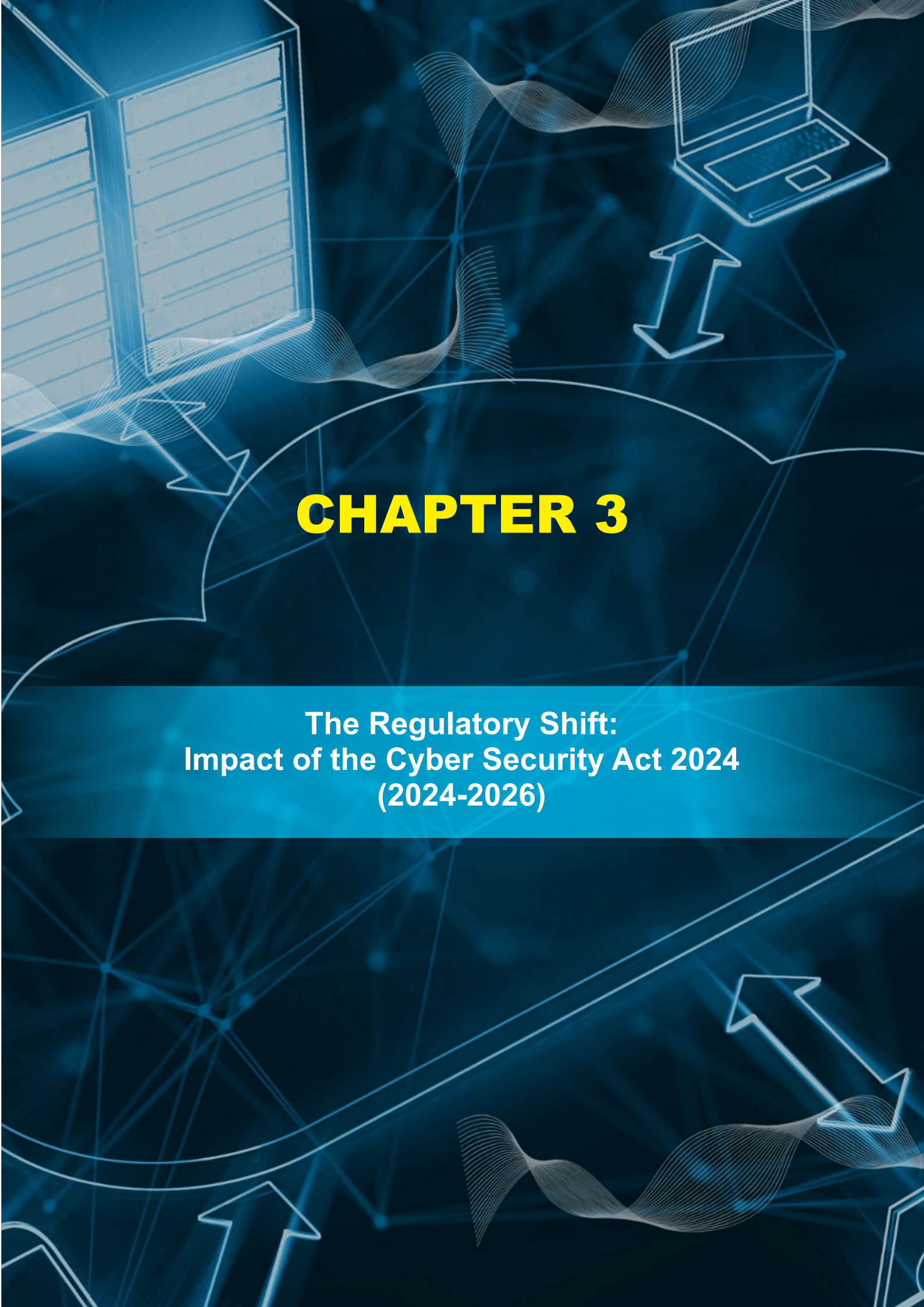
Based on our research the saga continues with a clear directive: resilience is a collective effort. With 67% of Malaysian SMEs being targeted by ransomware in 2025, the focus for 2026-2027 must be on **supply-chain security** and **post-quantum cryptography readiness**.

As PIKOM and industry leaders convene at the **Future of Cybersecurity Summit 2026**, the goal is no longer just to prevent attacks, but to ensure that when they happen, Malaysia's digital economy is robust enough to endure and recover.

Executive Insight: The Cyber Security Act 2024 has ended the era of "voluntary" security. In 2026, resilience is the new currency of business trust in Malaysia.

Refer to the PIKOM Cybersecurity Survey 2026 Analysis section.

Cybersecurity is no longer just 'IT security';
it is a pillar of National Economic Stability."



CHAPTER 3

The Regulatory Shift: Impact of the Cyber Security Act 2024 (2024-2026)

The most transformative event since the 2025 publication has been the formal entry into force of the **Cyber Security Act 2024 (Act 854)** on **June 26, 2024**. This legislation has fundamentally altered the cybersecurity obligations of Malaysian organizations, shifting the focus from voluntary adoption to a mandatory regulatory framework.

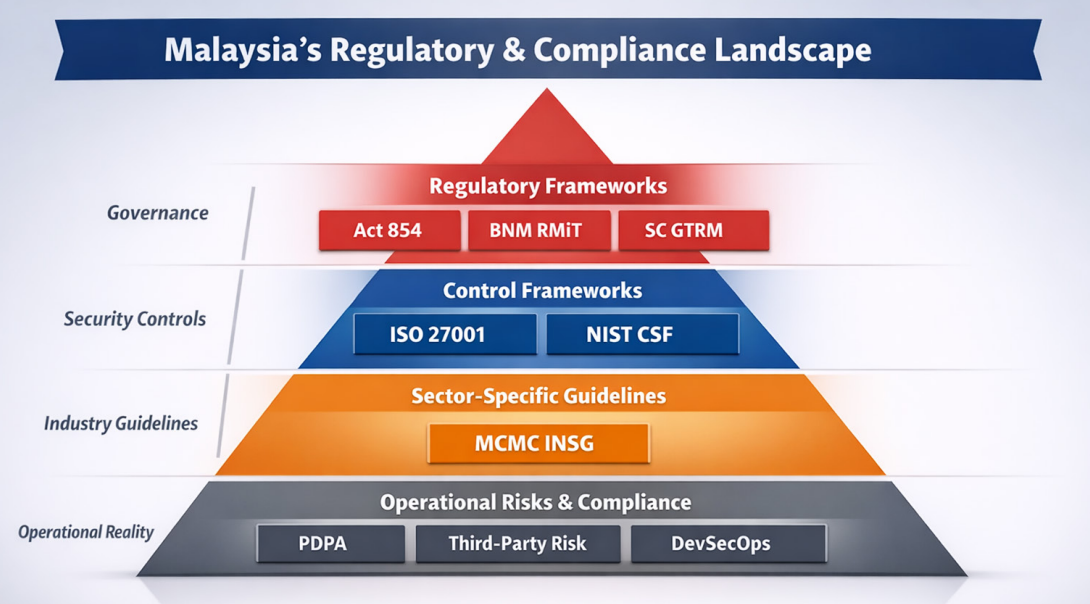


Figure 7: Credit to Rodney Lee

Safeguarding National Critical Information Infrastructure (NCII)

The primary objective of the Act is the protection of National Critical Information Infrastructure (NCII), defined as computer systems where disruption would have a detrimental impact on national security, public safety or government functions.

- **Designated NCII Sectors**: The Act specifically targets 11 critical sectors, including Financial Services, Telecommunications, Energy, Healthcare, Government and Transportation.
- **Sector Leads & Entities:** For each sector, an NCII Sector Lead has been appointed to oversee and enforce security standards. Organizations designated as NCII Entities are now legally obligated to provide information regarding their infrastructure, implement sector-pacific codes of practice, and conduct regular cybersecurity risk assessment and audits.
- **Mandatory Incident Reporting:** Under Section 23, NCII entities are required to notify both their Sector Lead the Chief Executive of NACSA of any cybersecurity incident within a strictly defined period.

Regulation of Cybersecurity Service Providers

The Act introduces a significant new regulatory pillar: the mandatory l**icensing of cybersecurity service providers (CSSPs)**.

- **Licensing Framework:** Starting from **October 1, 2024**, individuals and companies offering or advertising specific cybersecurity services must be licensed by NACSA.
- **Scope of Licensing:** This requirement applies to those providing services such as managed security monitoring, penetration testing, and incident response, ensuring a high standard of professional competence across the industry.
- **Exemptions:** Specific exemptions apply for services provided by government entitles, internal services within a corporate group (holding and subsidiaries), or services involving systems located entirely outside of Malaysia.

Enforcement and Penalties
The Cyber Security Act 2024 grants the National Cyber Security Agency (NACSA) broad enforcement powers, including the authority to investigate incidents and conduct searches and seizures.

- **Non-Compliance Risks:** Failure to comply with the Act's mandates – such as failing to report an incident or providing cybersecurity services without a license – can result in severe penalties
- **Financial and Criminal Penalties:** Fines for various offenses can reach up to **RM 500,000** and individuals may face imprisonment for terms up **10 years**.

2025 Implementation Crucible
The year 2025 served as the "Implementation Crucible" for Malaysia's cybersecurity landscape. While 2024 was defined by the passing of new laws, 2025 was the year those laws met the reality of a rapidly evolving, AI driven threat environment.

Specifically, three major shifts occurred 2025 that separate the 2024 "baseline" from the current 2026 findings:

1. **The "First Full Year" of the Cyber Security Act 2024**
   The Act came into force on August 26, 2024, meaning 2025 was the first full calendar year of mandatory compliance.
   - **Mandatory Audits:** 2025 marked the first cycle where National Critical Information Infrastructure (NCII) entities were required to complete their initial cybersecurity risk assessments and audits under the new regulations.
   - **The Licensing Boom:** On **October 1, 2024** the licensing of Cybersecurity Service Providers (CSSPs) began. Throughout 2025, the market saw massive "cleansing" effect as service providers (pen-testers, incident responders) rushed to meet NACSA's professional standards to remain legal.
   - **Enforcement Reality:** The "honeymoon period" ended in 2025 as Sector Leads began actively monitoring the 11 critical sectors for compliance, moving the conversation from policy to penalty.

"The Cyber Security Act 2024 has ended the era of 'voluntary' security for critical infrastructure."

2. **The AI "Great Leap Forward" (Threat Evolution)**
   In 2024, AI threats like "Deepfakes" were largely considered emerging curiosities.
   In 2025, they became a daily operational reality for Malaysian SOCs.
   - **The September Spike:** Threat reports from late 2025 show a massive surge in "escalated incidents", with **September 2025** recording the highest single-month volume of the year (over 3x the mid-year average). This indicated that attackers significantly ramped up operations in the second half of 2025.
   - **Operational Deepfakes:** 2025 saw the first widespread use of deepfake audio and video in Malaysian "CEO Fraud" cases, where AI was used to impersonate executives during virtual meetings to authorize fraudulent transactions.
   - **Agentic Phishing:** Attackers moved away from manual "copy-paste" phishing to using AI agents that could crawl Malaysian social media and LinkedIn to craft hyper-personalized spear-phishing messages in perfect local context.

3. Economic and Data Realities

2025 provided the first hard data on the cost of the "new" threat landscape:

- **The Cost of Breaches:** The average cost of a data breach in Malaysia climbed to RM 3.2 million based on 2025 data.
- **SME Crisis:** 2025 was a brutal year for smaller firms; ransomware attacks on Malaysian SMEs jumped from **48% in 2024 to 67% in 2025**.
- **Identify as the Perimeter:** 2025 data confirmed that Microsoft 365 (0365) became the dominant attack surface, generating nearly a third of all escalated incidents as attackers pivoted from hacking "networks" to hacking "identities".

In summary: The Strategic Impact on 2026 Operations

The Act has forced a re-evaluation of cybersecurity budgets and personnel requirements.

For many Malaysian firms, the journey from 2024 to 2026 has been defined by the need to align internal governance with these new legal requirements. Organizations are increasingly adopting international frameworks (such as ISO27001 or NIST) to demonstrate compliance with the mandatory codes of practice established by their respective Sector Leads.

If 2024 was about **legislation**, 2025 was about **confrontation** – where organizations had to balance the high costs of new compliance with the escalating technical sophistication of AI-driven adversaries.

"The Act forces a board-level shift, making security a mandatory operational pillar."

CHAPTER 4

The RoadMap Ahead (2026 & Beyond)

Strategic Recommendations

The findings from primary and secondary data in 2026 have confirmed that Malaysia has moved beyond the "compliance-seeking" phase of its digital journey. As we look forward to 2027 and beyond, the focus must shift from establishing frameworks to **operationalizing resilience**.

The following recommendations are designed to navigate a landscape defined by hyper-automation and the maturing regulatory environment.

For Organizations: Transitioning from Defense to Autonomous Resilience

As AI-driven attacks become the standard, the gap between "point-in-time" security and "real-time" threats is widening. Organizations must transition from manual security management to an automated, risk centric model.

- **Maturing CTEM (Continuous Threat Exposure Management):** Move beyond the initial adoption of CTEM by integrating **AI-driven Red Teaming**. Organizations should automate the discovery of exploitable paths, focusing on business-critical assets rather than just technical vulnerability.
- **Governance of Autonomous Agents:** With the proliferation of "Agentic AI" in business workflows, organizations must establish an **AI Guardrail Registry**. This involves mapping every AI agent's permission to prevent "privilege escalation" by autonomous systems.
- **Identity as the New Perimeter:** With cloud adoption nearing 100% for many sectors, the focus must shift entirely to **Identity and Access Management (IAM) Resilience**. This includes implementing phishing-resistant MFA and moving toward "Just-In-Time" access to minimize the blast radius of credential theft.

"In 2026, resilience is the new currency of business trust in Malaysia."

For Government: Moving from Enforcement to "Cyber-Economic" Enablement

With the Cyber Security Act 2024 now fully operational, the government's focus should pivot toward streamlining the digital economy and preparing for the next frontier of computing.

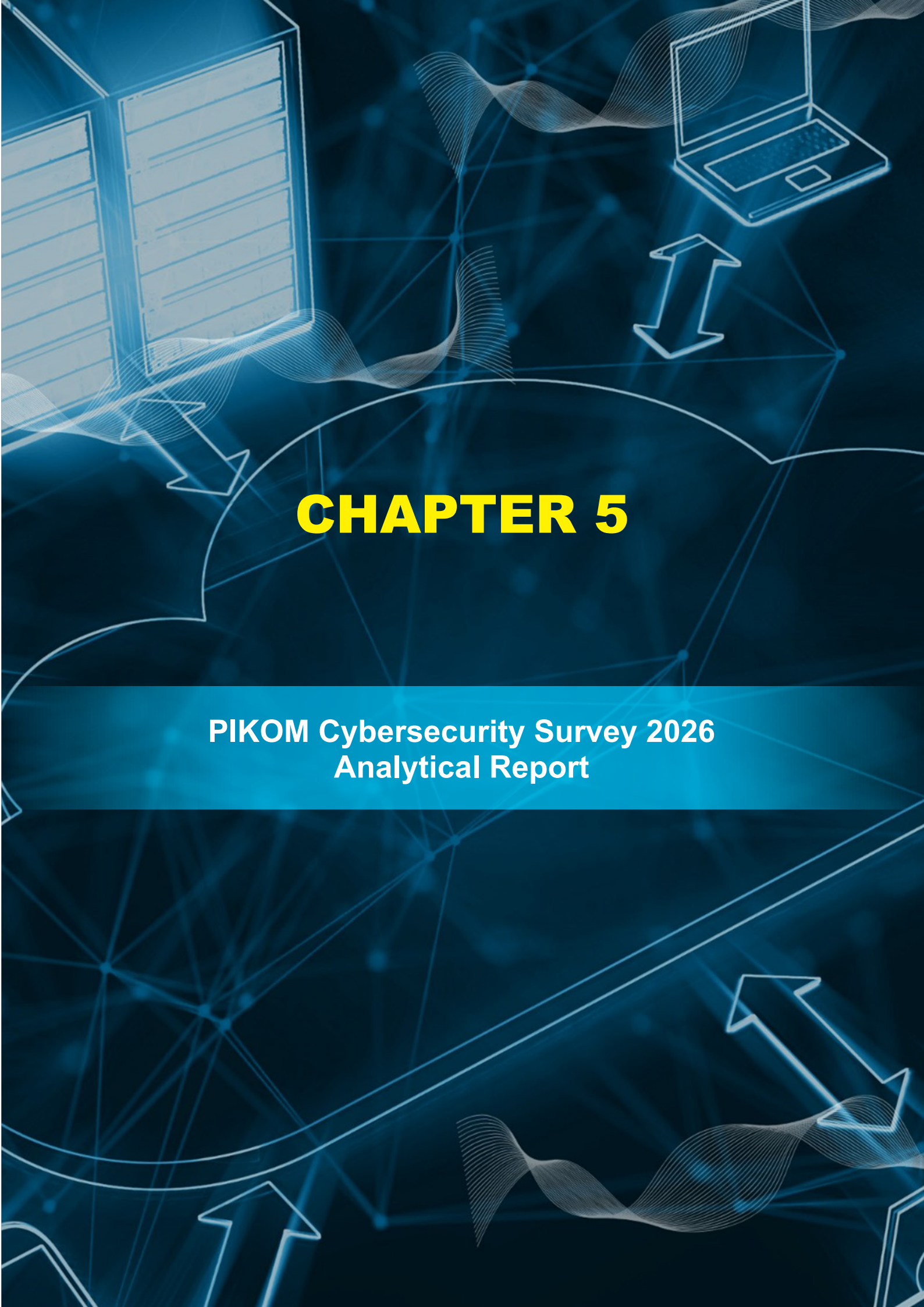
- **Regulatory Harmonization & Reciprocity:** To reduce the compliance burden on NCII sectors, NACSA should lead efforts to harmonize local licensing with international standards (e.g., ISO/IEC 27001:2022). Implementing **regulatory reciprocity** for licensed service providers will help Malaysian firms compete regionally while ensuring high domestic standards including implementation of AI governance and ethic (eg IS042001).
- **National Quantum-Safe Roadmap:** As we approach 2027, the government should mandate **Post-Quantum Cryptography (PQC)** Readiness Assessments for critical sectors. Incentivizing early migration to quantum-resistant algorithms will protect long-term data sovereignty.
- **Automated Regulatory Reporting:** Transition from manual audit submissions to **Continuous Regulatory Compliance (CRC)** platforms. By providing API-based reporting gateways, the government can gain real-time visibility into national resilience without increasing the administrative drain on private enterprises.

For PIKOM: Scaling the Talent Ecosystem and Supply Chain Integrity

As the voice of the industry, PIKOM must address the structural shortages in talent and the systemic risks within the ICT supply chain.

- **The "Cyber-Analyst to Architect" Upskilling Bridge:** To Address the hiring crisis, PIKOM should facilitate **Applied AI-Security Certifications**. The Focus must move from basic monitoring to high-level architecture - training professionals to design "Secure-by-Design" systems that incorporate AI safety ethical guardrails.
- **Supply Chain Trust Labels:** PIKOM can lead the development of a **Voluntary Vendor Security Rating** system. By standardizing the assessment of third-party SaaS and hardware providers, PIKOM helps SMEs and large firms alike navigate the "Difficult" hiring landscape by relying on vetted, high -trust ecosystem partners.
- **Cross-Regional Synergy:** Leveraging Malaysia's position in ASEAN, PIKOM should spearhead a **Regional Threat Intelligence Exchange**. Fostering "Collective Defense" beyond national will allow member companies to anticipate threats that have already hit neighbouring markets, turning regional synergy into a competitive advantage.

"The focus must shift from establishing frameworks to operationalizing resilience."



CHAPTER 5

PIKOM Cybersecurity Survey 2026
Analytical Report

Bottom Line
Resilience is improving at the surface, but attack methods are becoming more AI-enabled, more identity-focused, and more dependent on third-party exposure.

Executive Summary

The 2026 survey suggests that many Malaysian organisations have strengthened their baseline cyber posture, but resilience remains uneven. A majority of respondents reported no successful incident in the last 24 months, yet the organisations that were hit increasingly faced AI-assisted and identity-centric threats rather than only traditional malware patterns.

- Among the respondents to the incident question, 64.1% reported no successful incident in Jan 2024–Dec 2025, while 35.9% experienced at least one successful incident.
- Among affected organisations, the most reported attack types were AI-generated phishing/deepfake impersonation (32.6%), malware or RaaS (30.2%), and credential theft (25.6%).
- Security modernisation is underway: 55.9% of respondents operate more than 40% of IT/OT in cloud or hybrid environments, 61.9% have at least partial Zero-Trust adoption, and 51.7% are already piloting or actively using AI in cyber defence.
- Cost and capability constraints remain pronounced: 51.3% operate with annual cyber budgets below RM250,000, 78.8% have five or fewer dedicated cyber personnel, and 54.9% say hiring talent is difficult or very difficult.
- Third-party and future-readiness gaps are visible. 34.6% have no formal third-party cyber risk process, while only 10.8% are planning or implementing post-quantum measures.

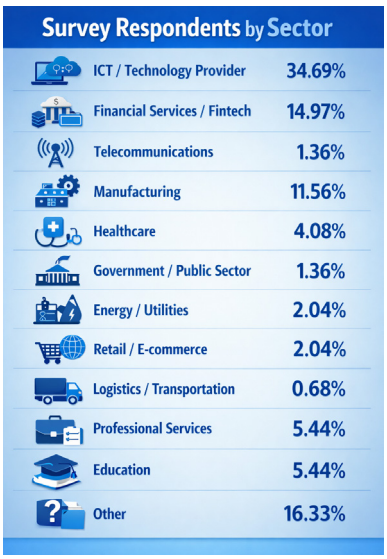
Compared with the 2024 report, the most important shift is not simply whether organisations are breached, but how they are being pressured. The earlier report highlighted human error, response planning and generic best practices. The 2026 responses show that the same human layer is now being targeted through AI-generated phishing, deepfake impersonation, shadow AI usage, and identity abuse. In short, resilience in 2026 is less about basic awareness alone and more about disciplined governance, modern controls, and sustained operating maturity.

"35.9% of surveyed organizations experienced at least one successful incident in the last 24 months.

1. Respondent Profile

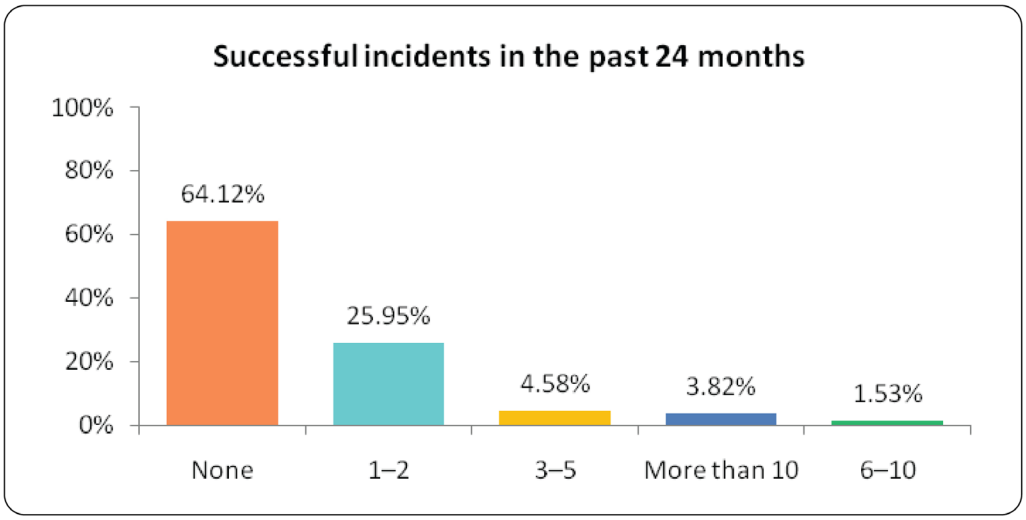
The respondent base is weighted toward ICT/technology providers, financial services, and manufacturing. This means the dataset is strongest as an indicator of cyber resilience among digitally mature or digitally exposed sectors, rather than a perfectly even economy-wide sample.

Organisation size is also meaningful. The largest groups came from organisations with 250–999 employees and 1000+ employees, giving the survey good visibility into mid-sized and larger enterprise practices, while still capturing small-company constraints through the SME segment

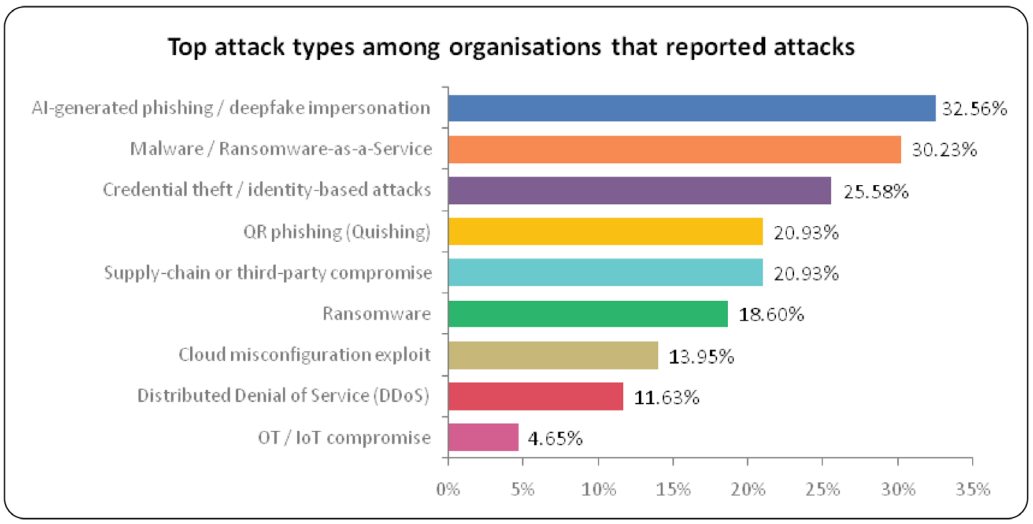


2. Incident Experience and Business Impact

On the core resilience question, 64.12% respondents reported no successful incident in the period Jan 2024–Dec 2025. That is a materially calmer picture than the inaugural 2024 report, although the question design is different and therefore should not be treated as a strict like-for-like reduction. More importantly, only 9.9% of respondents reported three or more incidents, indicating that repeated compromise is concentrated in a smaller at-risk group.



For organisations that were affected, the severity profile skews toward the manageable end but is not trivial. Just over half rated their most significant incident as minor, one-third as moderate, and a smaller but important minority as severe or catastrophic. Financial damage also shows a long tail: most affected respondents reported no direct financial loss or loss below RM100,000, but a few respondents reported losses above RM1 million, including one above RM5 million.



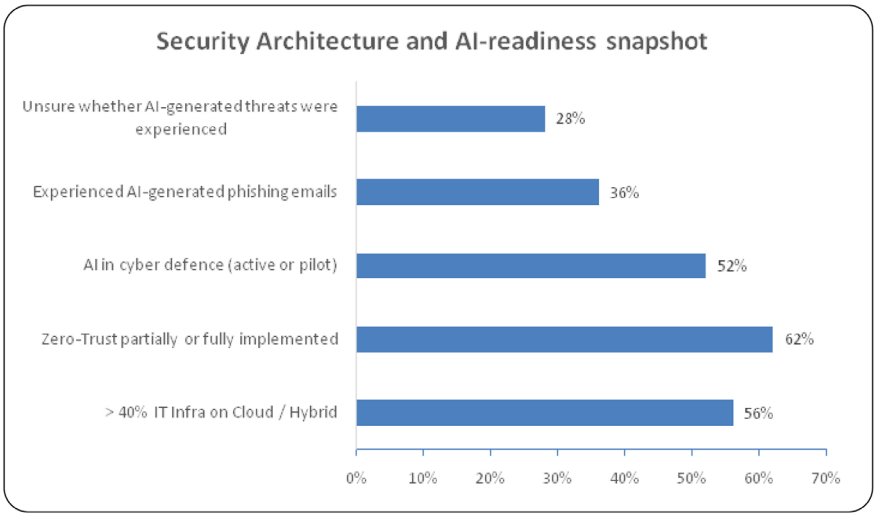
The pattern of attack exposure is notable. AI-generated phishing and deepfake impersonation were the most cited category among impacted organisations, ahead of traditional ransomware. Credential theft and quishing also ranked high. This suggests that the human attack surface remains central, but the tactics have become more convincing, faster, and harder to detect.

Observed impact themes from open-text responses

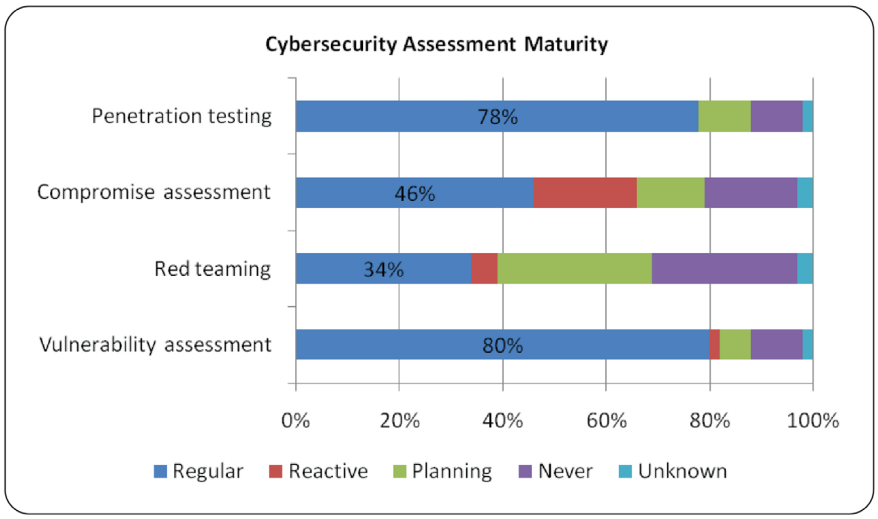
Theme	What respondents commonly described	Analytical implication
Operational disruption	Downtime, investigation workload, service interruption, internal process disruption.	Even when financial loss is limited, business continuity and recovery discipline remain critical.
Financial exposure	Recovery costs, containment work, and targeted spending after incidents.	The financial tail risk is real even if the median incident cost is still contained.
Reputational and trust concerns	Customer confidence and brand perception were repeatedly mentioned, though less often than operational effects.	Boards should treat cyber resilience as a trust and market issue, not only an IT issue.

3. Security Architecture and Operating Maturity

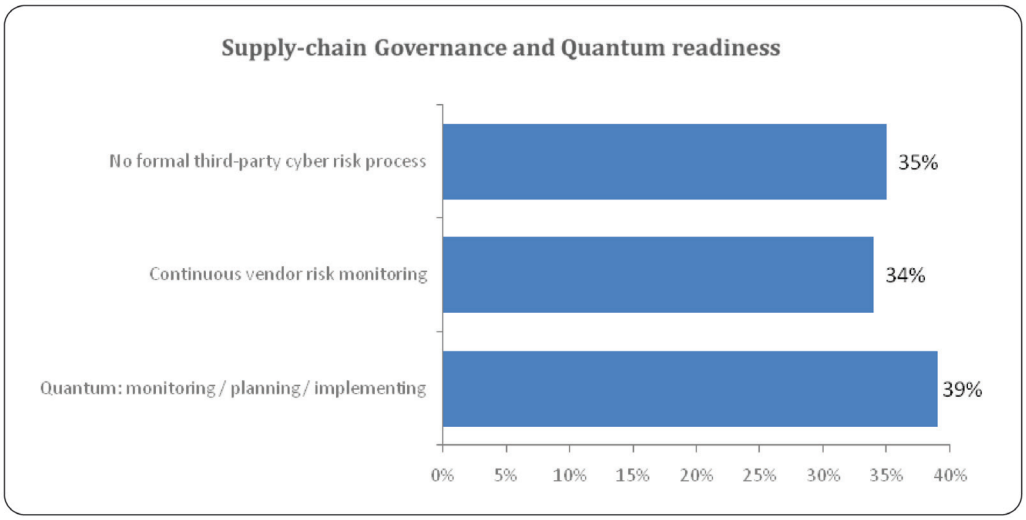
The 2026 responses show a sector that is moving beyond perimeter thinking. Cloud and hybrid environments are now mainstream in the sample, Zero-Trust adoption is gaining traction, and AI is no longer only a threat topic but also a defence enabler.



However, architecture maturity is not evenly matched by operational maturity. Partial implementation dominates Zero-Trust, and nearly one in three respondents are already using AI defensively while another 42.4% are still only planning. This means the market is in transition: intent is high, but execution maturity still varies sharply by budget, skills, and governance discipline.



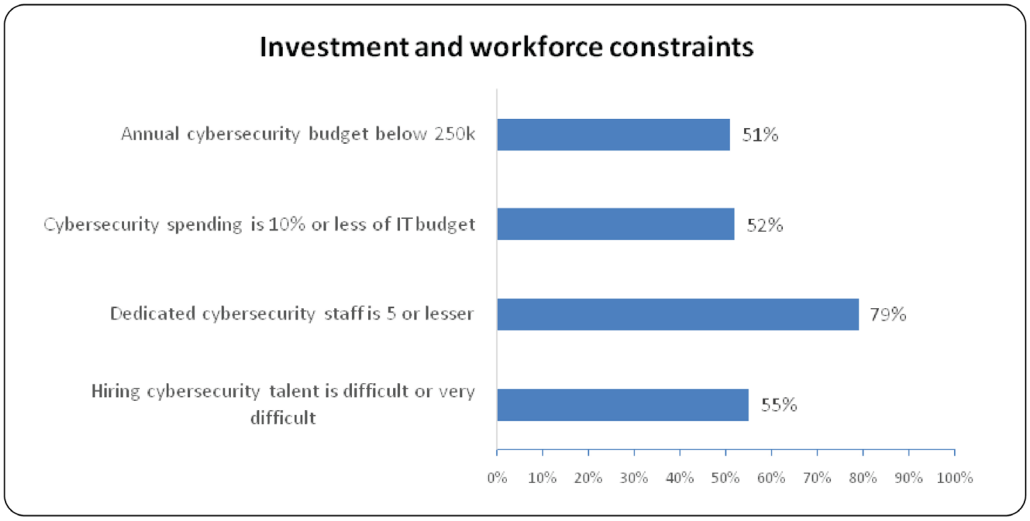
Two findings stand out. First, penetration testing and vulnerability assessment are now established baseline practices, with roughly four in five respondents performing them on a regular cadence. Second, more advanced assurance practices lag badly: only one-third conduct red teaming on a regular basis, while nearly one-third never do it. Compromise assessments also remain underused relative to the current threat environment.



Third-party cyber risk management remains one of the report's clearest red flags. More than one-third of respondents said they have no formal process. That is especially concerning given the prominence of supply-chain and third-party compromise in the threat landscape. Quantum readiness is even earlier-stage: most respondents are either only aware or not yet aware, which is understandable in the short term, but it highlights the need for monitoring and roadmap discipline now rather than later

4. Investment and Workforce Constraints

Resilience gaps in 2026 are shaped as much by economics and workforce capacity as by technology choice. Many organisations are attempting to modernise, but they are doing so with relatively modest budgets and very lean internal teams



This is a structurally important result. When over half of respondents operate with cyber budgets below RM250,000 and more than three-quarters have five or fewer dedicated cyber staff, resilience becomes highly dependent on prioritisation, managed services, and good governance rather than on building large in-house specialist teams. The hiring picture reinforces this: difficulty recruiting talent is now a persistent operational drag, not a temporary inconvenience.

For SMEs and mid-market organisations, this means the path to resilience will often depend on pragmatic control choices: identity security first, disciplined vulnerability management, tested incident response, strong third-party onboarding, and selective use of managed detection, threat monitoring, and specialist assurance services.

5. Regulatory Impact and Qualitative Findings

Open-text responses show that the Cyber Security Act 2024 and related NCII / MCSS expectations are already influencing organisational behaviour, even where implementation is still maturing. The responses do not indicate a uniform industry reaction; rather, they show three broad patterns.

- **A governance lift:** respondents described stronger compliance attention, policy reviews, clearer board or management visibility, and more structured control expectations.
- **A resourcing challenge:** some respondents linked the Act to higher investment needs, heavier documentation or reporting effort, and practical difficulty translating policy intent into execution.
- **An uneven maturity curve:** a meaningful subset reported limited change so far, suggesting that the regulatory effect is real but still diffusing across the market.

Most common themes from open-text responses

Question area	Most common themes	Interpretation
Emerging 2026 challenges	AI-enabled threats, talent shortage, supply-chain risk, OT/IoT and cloud exposure.	The threat agenda has expanded beyond traditional malware into operational, identity, and ecosystem risk.
AI-related concerns	Deepfake social engineering, shadow AI, governance gaps, adversarial misuse, and data leakage.	AI is now both an attack amplifier and a governance challenge inside the enterprise
Actions started or planned	Roadmaps, awareness programmes, policy updates, monitoring, and early post-quantum exploration.	Most organisations are responding, but often at planning stage rather than full deployment.
National resilience recommendations	Government support for SMEs, more awareness, better threat sharing, clearer guidance, and talent development.	Respondents want resilience to be treated as a shared ecosystem issue, not only an internal company task.

6. What Has Changed Since the 2024 Report

The 2024 report established five strong messages: cyber incidents were widespread, human error was central, response planning mattered, organisations expected more breaches, and awareness of best practices was meaningful but uneven. The 2026 dataset does not replace those findings; it sharpens them.

The most important analytical conclusion is that Malaysia's cyber resilience conversation has moved from awareness to execution. In 2024 the system was still heavily describing the problem. In 2026 the problem is more clearly defined: organisations are modernising, but unevenly; attack methods are more AI-enabled; and ecosystem dependencies now matter as much as endpoint or email hygiene.

7. Strategic Recommendations

Based on the quantitative and qualitative responses, the strongest recommendations for 2026–2027 are as follows.

For organisations

- Prioritise identity resilience: strengthen phishing-resistant MFA, privileged access controls, credential monitoring, and deepfake/social-engineering verification workflows.
- Move from annual hygiene to operating discipline: regular vulnerability assessment, scheduled penetration testing, tested incident response, and selective compromise assessment should become standard.
- Treat third-party cyber risk as a board-level dependency issue. Formalise onboarding checks, monitoring, and minimum control expectations for critical vendors.
- Establish AI governance that covers approved tools, data handling, shadow AI, and the use of AI in both de fence and business operations.
- For smaller teams, simplify ruthlessly. Focus on the handful of controls that reduce the most risk rather than spreading scarce resources too thinly.

For government

- Support SME uplift through incentives, co-funding, shared services models, or practical implementation toolkits linked to national requirements.
- Continue to translate regulatory intent into operational guidance, especially for organisations that are not NCII operators but still need stronger resilience baselines.
- Strengthen trusted information-sharing channels and sector-specific threat visibility, especially for AI-enabled fraud, supply-chain compromise, and critical infrastructure risk.

For PIKOM and industry associations

- Use the 2026 findings to build targeted awareness programmes on AI-enabled threats, third-party governance, and practical cyber operating models for SMEs and mid-market members.
- Develop benchmarking content that helps members understand what 'good' looks like for budget mix, staffing models, assessment cadence, and Zero-Trust adoption.
- Facilitate ecosystem collaboration between technology providers, end-user organisations, academia, and government so that resilience becomes a shared capability rather than a fragmented effort.

"Resilience in 2026 is less about awareness and more about disciplined governance."

GLOSSARY / ACT

Glossary or Acronyms list to include more granular terms found in the text, as well as several industry-standard terms that are contextually relevant to the “Continuing Saga” of Malaysia’s landscape.

EXPANDED CYBERSECURITY GLOSSARY

Technological & Offensive Terms

- **Agentic AI:** A transition from “content” to “action,” where AI systems act as autonomous agents capable of planning and executing tasks to reach a goal, including potential paths toward Artificial General Intelligence (AGI).
- **Defensive AI:** The deployment of AI and Machine Learning (ML) tools by defenders to automate threat detection and enhance SIEM capabilities.
- **Deepfake Impersonation:** The use of AI-generated synthetic media to mimic the voice or appearance of executives or employees to facilitate fraud.
- **Embodied Intelligence:** AI that is integrated into physical systems or environments, requiring specialized security awareness as these systems interact with the physical world.
- **Quishing:** A portmanteau of “QR” and “phishing”; an attack vector where malicious QR codes are used to lead users to credential-harvesting sites.
- **Ransomware:** A type of malware that encrypts an organization’s data, demanding payment for its release; currently the #1 threat to Malaysian businesses.
- **Red Teaming:** An adversarial testing methodology that mimics real-world attackers through both technical hacks and social engineering to test an organization’s detection limits.

Architectural & Strategic Terms

- **Compromise Assessment:** Forensic investigations aimed at discovering hidden threats or “dwellers” that have already bypassed perimeter defenses undetected.
- **Hybrid Infrastructure:** An IT environment that combines on-premises data centers with public or private cloud services; many Malaysian firms now operate 60% to 100% of their stacks in the cloud.
- **PQC (Post-Quantum Cryptography):** Cryptographic methods researched and implemented to remain secure against the massive computing power of future quantum computers.
- **SIEM (Security Information and Event Management):** A solution that provides real-time analysis of security alerts. In 2026, these are increasingly “augmented” by AI.
- **Supply-Chain Security:** A 2026–2027 focus area aimed at securing the network of third-party vendors and software providers to prevent collateral breaches.
- **Zero-Trust Architecture (ZTA):** A security model based on the principle of “never trust, always verify,” treating every user and device as a potential threat regardless of their location.

MALAYSIAN AND GLOBAL ACTS

1. Malaysia's Primary Cybersecurity Framework

- **Cyber Security Act 2024 (Act 854):** The most critical legislation for your report. Enforced on **August 26, 2024**, it mandates that National Critical Information Infrastructure (NCII) entities comply with specific codes of practice, perform regular audits, and report incidents within strict timelines.
- **Personal Data Protection (Amendment) Act 2024:** A major update to the 2010 Act, implemented in phases throughout **2025**. Key changes include:
- **Mandatory Breach Notification:** Organizations must notify the Commissioner within 72 hours of a data breach.
- **Data Protection Officers (DPO):** Mandatory appointment of DPOs for certain organizations (as of June 2025).
- **Increased Penalties:** Fines increased up to **RM 1 million** and/or 3 years imprisonment.
- **Data Portability:** New rights for individuals to move their data between service providers.

2. Regional & Global Regulations

Malaysian firms with international operations or digital exports must track these, as they often dictate "standard of care."

- **ASEAN Cybersecurity Cooperation Strategy (2026–2030):** Following the 2021–2025 plan, the new 2026 strategy focuses on regional incident response (ASEAN CERT) and cross-border protection of critical infrastructure.
- **EU General Data Protection Regulation (GDPR):** The gold standard for global privacy. Any Malaysian company serving EU citizens must comply. The 2024 Malaysian PDPA amendments were specifically de signed to align closer to GDPR standards.
- **Singapore Cybersecurity (Amendment) Act 2024**: Given the close economic ties, Singapore's update to include "Foundational Digital Infrastructure" (like Cloud services and Data Centers) often mirrors or influences Malaysian policy trends for 2026.
- **EU AI Act (2024/2026):** As your report mentions Agentic AI and Deepfakes, this is the world's first comprehensive AI law. It categorizes AI systems by risk level and will likely serve as a template for Malaysia's upcoming AI governance frameworks in 2026.

3. Sector-Specific Standards (Malaysia)

- **BNM Risk Management in Technology (RMIT):** The definitive standard for the Malaysian financial sector, emphasizing resilience against the "Breach Epidemic" and secure cloud adoption.
- **National Cybersecurity Strategy (NCSS) 2024–2028:** While a policy framework rather than an act, it sets the strategic pillars for cyber resilience and workforce development that the current 2026 report measures.

APPENDIX

BEYOND COMPLIANCE: THE STATE OF CYBER RESILIENCE IN MALAYSIA 2026 SURVEY FORM

INTRODUCTION

This survey forms part of the **PIKOM Cybersecurity Landscape Report 2026** which will be launched during the **Future of Cybersecurity Summit (FCOS) 2026.**

These are designed as a direct follow-up to the 2024 mini-survey (which covered branches, impacts, preparedness, budgets, human error, compliance, and sector comparisons) while incorporating the latest 2025-2026 cybersecurity trends relevant to Malaysia and globally.

- AI-powered attacks (deepfakes, agentic AI, AI-driven, phishing/quishing)
- Ransomware evolution @ extortion
- Supply -chain/third-party risks
- OT/IoT security (especially critical infrastructure)
- Regulatory development (Cyber Security Act 2024, Malaysia Cyber Security Strategy, NCII resilience)
- Quantum readiness awareness
- Cyber resilience & AI governance

The survey results will provide valuable **industry insights and benchmarks** for **Malaysian organisations**.

All responses will be **aggregated and anonymised**. Individual organizations will not be identified without consent.

Estimated completion time: **7-10 minutes**

ORGANISATION PROFILE

1. Which sector best describes your organization?

☐ ICT/Technology Provider	☐ Retail/E-Commerce
☐ Financial Services/Fintech	☐ Logistics/Transportation
☐ Telecommunications	☐ Professional Services
☐ Manufacturing	☐ Data Centre/Cloud Provider
☐ Healthcare	☐ Education
☐ Government/Public Sector	☐ Other (please specify)
☐ Energy/Utilities	_____

2. How many employees does your organization have?

☐ Fewer than 10	☐ 250-999
☐ 10-49	☐ 1000+
☐ 50-249	

3. Name of Organisation (optional) _____

CYBERSECURITY INCIDENTS & THREAT LANDSCAPE

4. In the past 24 months (Jan 2024-Dec 2025), how many successful cybersecurity breaches or incident has your organisation experienced?

- ☐ None (if answer is none go to QB)
- ☐ 1-2
- ☐ More than 10
- ☐ 3-5
- ☐ 6-10

5. Which of the following cyberattacks has your organisation encountered in the past 24 months? (You can select multiple answers)

- ☐ Ransomware
- ☐ AI-generated phishing/deepfake impersonation
- ☐ QR phishing (Quishing)
- ☐ Supply-chain or third party compromise
- ☐ Malware/Ransomware-as-a Service
- ☐ Credential theft/identify-based attacks
- ☐ OT/Iot compromise
- ☐ Cloud misconfiguration exploit
- ☐ Distributed Denial of Service (DDoS)
- ☐ Other (please specify) _____

6. On a scale of 1-5, how would you rate the severity of the most significant cybersecurity incident:

1 - Negligible 2 - Minor 3 - Moderate 4 - Severe 5 - Catastrophic

7. Estimated financial loss from your most significant cybersecurity incident:

- ☐ None
- ☐ Less than RM100,000
- ☐ RM100,000 – RM500,000
- ☐ RM500,000 – RM1 milion
- ☐ RM1 milion – RM 5 milion
- ☐ More than RM 5 milion

SECURITY ARCHITECTURE & TECHNOLOGY ADOPTION

8. What percentage of your organisation's IT/OT infrastructure is clou-based or hybrid?

- ☐ 0-20%
- ☐ 21-40%
- ☐ 41-60%
- ☐ 61-80%
- ☐ 81-100%
- ☐

9. To what extent has your organization adopted Zero-Trust architecture?

- ☐ Not started
- ☐ Planning Stage
- ☐ Partially implemented
- ☐ Fully implemented
- ☐ Not applicable
- ☐

10. Does your organisation use AI or machine learning tools for cybersecurity defence? (e.g. threat detection, automated response, SIEM augmentation)

- ☐ Yes-actively deployed
- ☐ Yes-pilot testing
- ☐ No-but planning
- ☐ No-not considering

11. Has your organisation experienced AI-generated cyber threats?

- ☐ Deepfake impersonation attacks
- ☐ AI-generated phishing emails
- ☐ AI-assisted malware
- ☐ Automated vulnerability scanning by AI
- ☐ None detected
- ☐ Unsure

CYBERSECURITY INVESTMENT & WORKFORCE

12. Approximate annual cybersecurity budget for 2026:

- ☐ Less than RM100,000
- ☐ RM100,000 – RM250,000
- ☐ RM251,100 – RM500,00
- ☐ RM501,000 – RM5 milion
- ☐ More than RM5 milion

13. Cybersecurity spending as percentage of IT budget:

- ☐ Less than 5%
- ☐ 5-10%
- ☐ 11-15%
- ☐ 16-20%
- ☐ More than 20%
- ☐

14. How many dedicated cybersecurity personnel (full-time equivalent) does your organisation employ?

- ☐ 0-2
- ☐ 3-5
- ☐ 6-10
- ☐ 11-20
- ☐ More than 20
- ☐

15. How difficult is it your organisation to hire cybersecurity professionals?

___ Very difficult ___ Difficult ___Neutral ___ Easy ___ Very easy

CYBERSECURITY PRACTICES & RESILIENCE
Q16-Q19: Which cybersecurity assessments does your organisation conduct?

16. Penetration Testing (Pen Testing)

A controlled cybersecurity test where security experts simulate attacks on systems, applications or networks to identify technical vulnerabilities that could be exploited by attackers.

- ☐ Monthly
- ☐ Quarterly
- ☐ Twice a year
- ☐ Annually
- ☐ Planning
- ☐ Never
- ☐ I don’t know what this is

17. Compromise Assessment

A forensic security investigation conducted to determine whether a system or network has already b een breached or contains hidden threats, even if no breach has yet been detected.

- ☐ Quarterly
- ☐ Twice a year
- ☐ Annually
- ☐ Occasionally after incidents
- ☐ Planning
- ☐ Never
- ☐ I don't know what this is.

18. Red Teaming

An advanced, goal-based adversarial simulation where a team mimics real attackers using multiple tactics (technical, physical and social engineering) to test an organization's overall ability to detect and respond to a full-scale attack

- ☐ Every 6 months
- ☐ Annually
- ☐ Every 2 years
- ☐ After incidents
- ☐ Never
- ☐ Planning
- ☐ I don't know what this is

19. Vulnerability Assessment

A systematic, proactive process of identifying, quantifying and prioritizing security weaknesses in an organization's IT systems, application, and network infrastructure. It uses automated scanning tools and manual analysis to find vulnerabilities such missing patches or misconfigurations and provides recommendations for remediation

- ☐ Continuously
- ☐ Monthly
- ☐ Quarterly
- ☐ Annually
- ☐ After incidents
- ☐ Planning
- ☐ Never
- ☐ I don't know what this is

20. Which practices does your organisation use to manage third-party cyber risk?

- ☐ Vendor cybersecurity questionnaires
- ☐ Mandatory ISO27001 certification. An international standard that helps organisations establish, implement, maintain and continually improve an Information Security Management System.
- ☐ SOC2 or equivalent assurance. Service Organisation Control 2 is an auditing standard developed by the American Institute of Certified Public Accountants (AICPA) that focuses on five Trust Services Criteria (TCSc): security, availability, processing integrity, confidentiality and privacy.
- ☐ Security audits before onboarding vendors
- ☐ Continuous vendor risk monitoring
- ☐ No formal process
- ☐ Other (please specify)

_____

REGULATORY IMPACT & EMERGING RISKS

21. Please describe the primary impacts (financial, operational, reputational, regulatory) of any cybersecurity incidents your organisation experienced in the past 24 months, and whether the impacts have change compared with 2023-2024.

22. How has the Cyber Security Act 2024 (or related NCII and MCSS requirements) affected your organisation's cybersecurity strategy, investment decisions, or compliance efforts? What improvements or difficulties have you observed?

23. What are the biggest new or emerging cybersecurity challenges your organisation expects to face in 2026? Please elaborate.(e.g, AI threats, supply-chain attacks, talent shortage, OY/Iot security)

24. What AI-related risks is your organisation concerned about or actively managing? (e.g, shadow AI a gents, deepfake social engineering, adversarial AI attacks, or governance of AI security tools)

25. How prepared is your organisation for quantum computing threats and the transition to post-quantum cryptography?

- ☐ No awareness
- ☐ Awareness only
- ☐ Monitoring development
- ☐ Planning post-quantum cryptography transition
- ☐ Already implementing quantum-safe cryptography

26. Based on Question 22; What action (if any) have you started or planned?

STRATEGIC RECOMMENDATIONS

27. Recommendation to Improve National Cyber Resilience

What recommendations would you give to:

- Malaysian organisations
- Government
- Industry associations such as PIKOM

to strengthen national cyber resilience in 2026-2027?

Thank you for participating in the PIKOM Cybersecurity Landscape Survey 2026.
Your input will contribute to the national cybersecurity conversation and industry benchmarking.

REFERENCES

Cyber Incident Statistics
https://mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=5d6330b4-971e-44b9-b62b-be713eab55c5

Cyber Security Act, Regulations And Directives
https://www.nacsa.gov.my/legal.php

Cyber Security Act 2024
https://www.nacsa.gov.my/act854.php

BigBand. (2026, March 17). RM3.2 Million
The real cost of a data breach in Malaysia (2025).BigBand Cybersecurity Insights.
Retrieved from
https://bigband.net.my/index.php/2026/03/17/rm3-2-million-the-real-cost-of-a-data-breach-in-malaysia-2025/

IBM Security. (2025). Cost of a data breach report 2025. IBM Corporation.
Retrieved from
https://www.ibm.com/security/data-breach

Palo Alto Networks Unit 42. (2026). Global incident response report 2026. Palo Alto Networks
https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

https://www.thestar.com.my/news/nation/2025/07/26/malaysia-faces-rising-cyber-threats-as-incidents-increase

https://www.thestar.com.my/tech/tech-news/2026/03/23/cyber-incidents-rise-as-malaysians-lag-on-online-safety

https://linkaxia.com/news-event/cybersecurity-awareness-month-2025-alarming-surge-in-cyberattacks-across-southeast-asia

https://securitybrief.asia/story/microsoft-365-behind-32-of-escalated-security-incidents

FUTURE OF CYBERSECURITY SUMMIT 2026 PARTNERS

GOLD PARTNERS

veeam

SANGFOR

SILVER PARTNERS

HUAWEI

ManageEngine

TECHLAB SECURITY

IBM Gold Partner

SUPPORTING PARTNER

COMPLETE HUMAN NETWORK
Enabling Enterprise Mobility

NETWORKING LUNCH PARTNER

Raddish Technology

EXHIBITION PARTNERS

AI MSP 365

AMIYA

armourzero
Simplifying Cybersecurity

BLACKPANDA

CloudEngine Digital

CloudMile

Comstor

CSC
CYBER SECURITY CLOUD

CTC
Challenging Tomorrow's Changes

CYNCLAIR

ENZOPLUS

FIRMUS

glocomp
a Keppel company

KPINTAR
enhancing capability

mimecast

NETASSIST

xcitium
The Power of Zero. Unleashed.

VECTRA

WIKI LABS

REGISTRATION SYSTEM PARTNER

SOUR

PIKOM

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

E : info@pikom.org.my W : www.pikom.org.my