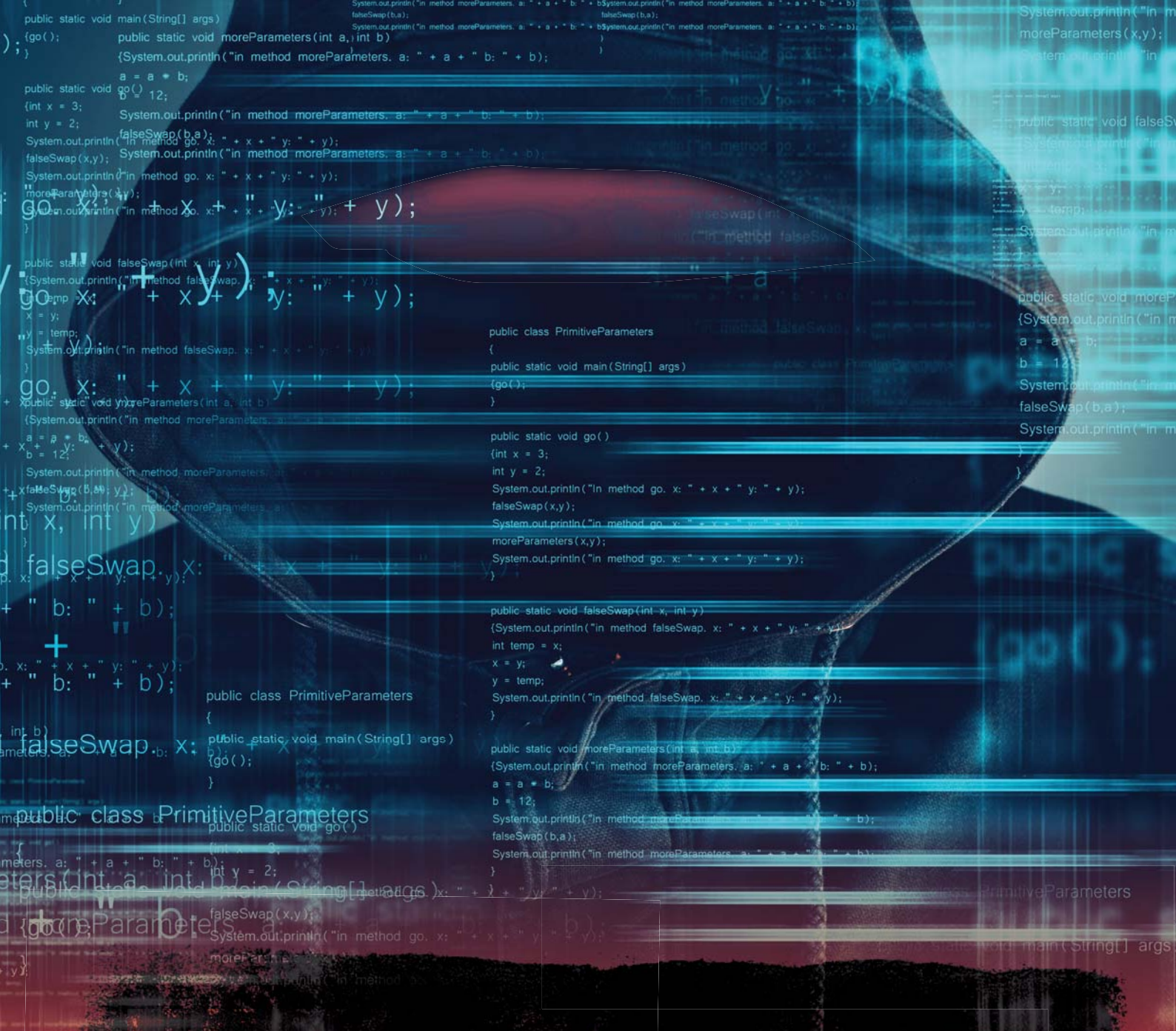


GROWING THREAT

CYBERSECURITY LANDSCAPE IN MALAYSIA 2024

CYBERSECURITY by PIKOM

exabytes | GROW Digital

One-Stop Cloud Solutions & Cybersecurity Managed Services

To Accelerate Business Growth

eSecure

Cybersecurity Services Enabling Highest Protection for Enterprises

eCloud | eBackup & DR | eCloudApp

Reach us at

exabytes.my/enterprise/secure

Arren
+6016-416 8286

Rae Von
+6016-421 7210

Published by:

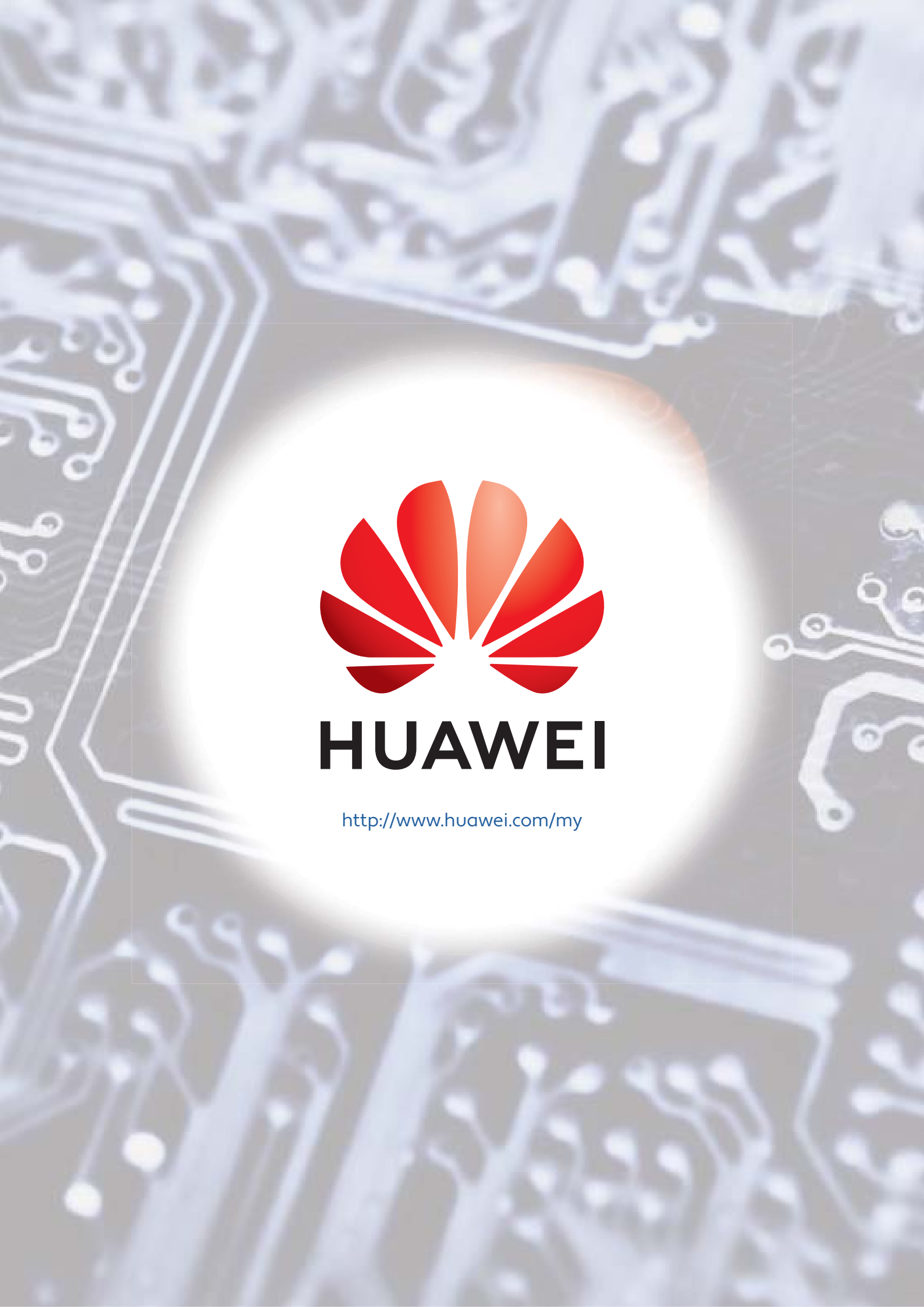
PIKOM

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: May, 2024

TABLE OF CONTENTS

- **Foreword by the Chairman of PIKOM** 7
- **Message from the Chair of PIKOM Cybersecurity Chapter** 8
- **Remarks by the Vice Chair of PIKOM Cybersecurity Chapter** 9
- **The Editorial & Design Team** 10
- **Executive Summary** 12
- **Qualitative Insights: CYBERSECURITY LANDSCAPE 2024** 15
- **Quantitative Results: CYBERSECURITY LANDSCAPE 2024** 21
- **CYBER ATTACKS: Comparative Analysis by Industry Sectors** 37
- **Recommendations** 43
- **Emerging Cyber Security Trends Shaping Malaysia's 2024 Outlook, by EY** 45
- **Cybersecurity Bill 2024** 51
- **References** 54



http://www.huawei.com/my

Trend Vision One™: A true cybersecurity platform

Trend Vision One delivers the full benefits of a platform approach to cybersecurity management, with comprehensive protection, prevention, detection, and response capabilities powered by AI and leading threat research and intelligence. It supports diverse hybrid IT environments, automates, and orchestrates workflows, and delivers expert cybersecurity services, so you can simplify and converge your security operations.

Customers' Choice: 2023 Gartner® Peer Insights™ 'Voice of the Customer': EPP

FOREWORD

ONG CHIN SEONG,
Chairman of PIKOM

Understanding Malaysia's cybersecurity landscape holds significant importance for several reasons. As Malaysia embraces digital technologies, it becomes increasingly vulnerable to cyber threats. With the proliferation of online platforms and transactions, cyber criminals exploit vulnerabilities, posing risks to digital assets.

Further, Malaysia's strategic position as a regional economic hub accentuates the necessity of cybersecurity. Its integration into global networks and cross-border transactions exposes it to both domestic and international cyber risks.

As Malaysia aims for high-income status, cybersecurity becomes essential for sustaining economic growth and investor trust. A robust cybersecurity framework is vital for safeguarding critical infrastructure, protecting sensitive data and ensuring the integrity of digital transactions, thereby securing Malaysia's digital economy.

I am proud and privileged to present this inaugural publication, which aims to provide insights into Malaysia's cybersecurity landscape, offering analysis, trends and best practices to empower stakeholders in navigating this evolving terrain. By comprehending the challenges and opportunities within Malaysia's cybersecurity ecosystem, we can collectively work towards building a safer digital future.

I would like to take this opportunity to extend PIKOM's appreciation to various parties for their invaluable contribution to this publication, including Sunway University and the University of Nottingham Malaysia for conducting qualitative interviews for the report. My appreciation also goes to EY for contributing a thought leadership article for this publication.

In addition, I would like to pay tribute to the PIKOM Cybersecurity Chapter led by Chair, Alex Loh and Vice Chair, Eric Foo as well as PIKOM Research Committee Chair Woon Tai Hai for helming this project and producing a report that will surely offer valuable insights to Malaysia and Malaysian companies.

Lastly, our appreciation also goes to the sponsors and advertisers who have always been supportive of our efforts to inform the digital community.

MESSAGE

ALEX LOH,
Chair of PIKOM Cybersecurity Chapter

It is with great pleasure and a profound sense of responsibility that I present to you the inaugural edition of our cybersecurity landscape report on behalf of the PIKOM Cybersecurity Chapter. This report marks a significant milestone in our continuous effort to strengthen the cybersecurity posture within our community and beyond.

In this comprehensive document, we look into the current state of our cybersecurity environment, examining priorities, breaches, frequency, resources, impacts and the response mechanisms employed by various industries. It is a reflection of our commitment to understanding the evolving threats and challenges that face us, with the aim of fostering a more secure digital ecosystem.

I would like to extend my heartfelt thanks to our generous sponsors. Your invaluable contributions and steadfast support have been instrumental in making this report a reality. Your commitment to cybersecurity excellence is truly appreciated and has not gone unnoticed.

Furthermore, I must also acknowledge the leadership of my Vice Chair, Eric Foo, who spearheaded this research initiative in close collaboration with the PIKOM Research Committee. His dedication has been pivotal to the successful completion of this important work.

This report is intended as a resource for you, offering insights and information critical to safeguarding your organisations against the ever-growing threat of cybersecurity breaches.

In the spirit of resilience, I encourage you to absorb its findings and recommendations and to integrate them into your strategies for cyber defence. Let this report serve as a reminder that staying resilient is not just a goal, but also a continuous journey.

Together, let us adopt resilience as our motto, ensuring that we are always prepared to face and overcome the cybersecurity challenges of today and tomorrow.

REMARKS

Eric Foo,
Vice Chair of PIKOM Cybersecurity Chapter

Welcome to the inaugural edition of our cybersecurity landscape report, a significant milestone for the PIKOM Cybersecurity Chapter.

This report represents our first foray into comprehensively analysing the cybersecurity environment catering to the local industry.

Initiated towards the end of 2023 and kicking off earnestly in February, this endeavour spanned approximately three months, during which we dedicated ourselves to meticulous surveys, in-depth interviews, thorough analysis and the production of this report.

Employing a dual approach, we balanced quantitative survey questions with qualitative interviews across a broad spectrum of industries, including Financial Services (FSI), Manufacturing, Food & Beverage (F&B), Technology, Services and Infrastructure, among others.

A pivotal element of our methodology was our collaboration with esteemed academic institutions, Sunway University and the University of Nottingham Malaysia. This partnership was instrumental, and I extend my heartfelt thanks to the professors and staff of these universities who contributed their expertise and insights to our study.

The primary aim of this research is to provide a clear, first-hand understanding of the current cybersecurity landscape and to offer insights into how our industries are responding to emerging challenges.

This report is crafted for a wide audience, including government agencies, vendors and users, offering valuable perspectives to all. Should this report prove beneficial to our readers, we are committed to producing an annual landscape report. We also recognise the dynamic nature of cybersecurity, where threats continually evolve in complexity and sophistication. It is our intention to keep the industry informed and prepared by tracking these changes through our ongoing and future studies.

I extend my profound gratitude to the PIKOM Research team, under the leadership of Woon Tai Hai, for their relentless effort and dedication in bringing this report to fruition.

On behalf of the Cybersecurity Chapter, thank you for everyone's commitment to excellence and your contribution to our collective cybersecurity resilience.

THE EDITORIAL & DESIGN TEAM

ERIC FOO

Eric Foo holds the position of Executive Vice President and Head of Enterprise Business for Exabytes Group. He is an experienced leader with more than 25 year's demonstrated history of expertise in the information technology and media industry. Eric is skilled in P&L and Sales Management, Product and Business Development, Cloud and Cybersecurity Solutions & Services. He has held various management positions in IBM, Astro, Mesiniaga and Hitachi Sunway. Presently, he leads Exabytes Group's cloud solutions and cybersecurity managed services business with a team of skilled and enthusiastic professionals supporting customers' digital transformation journey.

As a passionate leader, Eric is known as an innovative and inclusive business driver, supporting companies to grow their business by leveraging on digital technologies. He believes that digital transformation is a journey and not a destination, and enterprises can only achieve the desired business outcomes if they have a strong digital mindset using technologies as an enabler to continuously improve customer success and satisfaction.

WOON TAI HAI

Woon Tai Hai's illustrious career spans over 35 rich years across diverse sectors, imprinting his mark with notable expertise and dedication. He dedicated two fruitful decades to management consulting and risk management at renowned firms, KPMG and BDO Malaysia, drawing on deep insights and leadership to steer complex projects.

Since 2013, Woon has also been lending his expertise as an Advisor to PIKOM, Malaysia's national tech industry association, influencing the technology landscape significantly including leading the research committee for the past years.

Woon's academic path is equally impressive, holding a Master of Business Administration, a Postgraduate Diploma in Accounting and Finance, and a Bachelor of Science in Computer Science from prestigious Australian universities, UTS and UNSW.

ONG KIAN YEW

Ong Kian Yew serves as the devoted CEO of PIKOM, the National Tech Association of Malaysia, steering both the operations of the association and its chapters including the Pikom Cybersecurity Chaper.

Kian Yew is also a prominent figure on the international stage. He has represented PIKOM at significant global platforms such as the World IT and Services Alliance (WITSA) and the Asian Oceanian Computing Industry Organization (ASOCIO), even serving as Secretary General of ASOCIO in 2013.

Beyond these responsibilities, Kian Yew is a key player in PIKOM's government relations and his participation in numerous committees underscores his vital role in advocating for the ICT industry at the governmental level. Educated at the University of Strathclyde in Scotland, Kian Yew brings over two decades of experience to his role.

GRACE LEE

Grace Lee provides key secretariat support for the PIKOM Cybersecurity chapter, and she plays a central role in orchestrating key functions and events across multiple sectors within PIKOM, including the CIO, VIC, and CyberSecurity chapters as well as the Asia Pacific ICT Alliance (APICTA). She handles extensive duties ranging from local nominee coaching and international delegation management to overseeing the execution of PIKOM's flagship events such as the Leadership Summit and ICT Awards. Additionally, she also manages sales, marketing and operational logistics for major events. Her responsibilities extend to international travel coordination and event budget preparation, illustrating her integral involvement in advancing industry standards and connections globally.

NURUL ASYIQIN NASIR

Nurul Asyiqin Nasir is the dynamic force behind PIKOM's Media Relations, Government Affairs and is a member of the PIKOM Research Committee. With over two decades of experience in the Startup and Tech ecosystem, she is a seasoned professional in Training Content Development, Project Management and Management across various companies and associations.

Her expertise extends to Islamic Financing Planning. Nurul has spearheaded numerous national and international projects in Entrepreneurship, Education, CSR, Technology and Creative domains, enhancing her ability to analyse situations from diverse perspectives. She is instrumental in shaping PIKOM's research endeavours, including the annual Job Market report and other media publications, showcasing her unwavering dedication and passion for her work.

MICHAEL LAI

Michael Lai has been a steadfast supporter and invaluable partner to PIKOM for over a decade, contributing significantly as one of the editors of the annual PIKOM Job Market Report. He is the driving force behind Mjlaikc Infoworks, a esteemed content and consultancy firm that specialises in business, industry, technology, corporate sustainability and related fields. With an impressive career spanning over 30 years across journalism, publication, advertising, public relations and event management, Michael's expertise has been pivotal in producing influential job market reports and digital economy reviews for PIKOM for the last 15 years. His unwavering dedication and profound impact on the industry are truly commendable.

HAWARUDIN RASANI

Hawarudin Rasani, known as Rudin, has been an integral part of PIKOM's publications, showcasing his remarkable design skills over the years. With nearly 25 years of expertise as a publication designer, Rudin has left an indelible mark on the industry. He is not only associated with Mjlaikc Infoworks, but also boasts a diverse portfolio of clients. His contribution to the transformation of PIKOM's job market outlook and digital economy review cannot be overstated. Through his creative vision and professional approach, Rudin has elevated these publications to new heights of aesthetic excellence and industry relevance.

EXECUTIVE SUMMARY

This cybersecurity report presents a review and analysis of the current cybersecurity landscape, leveraging a dual-method approach to gather data and insights across various industry sectors.

The study was conducted with the objective of obtaining a first-hand understanding of the cybersecurity challenges and responses within sectors such as Financial Services (FSI), Manufacturing, Food & Beverage (F&B), Technology, Services, Infrastructure and more.

This objective aligns with the overarching goal to equip government agencies, vendors, service providers, non-governmental organisations (NGOs) and users with relevant information to enhance cybersecurity measures. To achieve a balanced and in-depth perspective, the study employed a two-pronged methodological approach. Firstly, quantitative survey questions were designed and disseminated across the targeted industries to gather statistical data on cybersecurity practices, threat perceptions and mitigation strategies.

Secondly, qualitative interviews were conducted with key stakeholders and experts within these sectors to gain deeper insights into cybersecurity challenges and solutions. This blend of quantitative and qualitative data collection methods ensured a holistic view of the cybersecurity landscape, reflecting both measurable trends and nuanced industry insights.

Another crucial aspect of this research was the collaboration with academic institutions, specifically the University of Sunway and the University of Nottingham Malaysia. These collaborations were instrumental in refining the research methodology, enhancing the depth of the analysis and ensuring the academic rigour of the study. The involvement of academia not only contributed to the credibility of the research findings, but also facilitated a bridge between theoretical frameworks and practical industry applications.

The significance of this research lies in its aim to provide a detailed and nuanced understanding of the cybersecurity environment as it stands, including the challenges faced by diverse industry sectors and their responses to these threats. By offering an up-to-date snapshot of the cybersecurity landscape, this report serves as a vital resource for all stakeholders involved, encouraging informed decision-making and strategic planning in the fight against cybersecurity threats.

Findings and Recommendations

The report highlights the multifaceted nature of data breaches, influenced by system vulnerabilities, human error and lack of knowledge, compliance gaps and response shortcomings.

Accompanied by an analysis of the interviews and survey responses, the report also features unique and common experiences with cybersecurity breaches across sectors, emphasising the universal challenge of human error versus the effectiveness of preparedness and swift responses.

The findings clearly highlight continuous awareness training, strategic investment in security measures, solutions and collaborative knowledge sharing as crucial factors in enhancing cybersecurity resilience across all local industries.

While regulatory compliance is foundational, it alone cannot prevent breaches. Instead, a proactive approach encompassing technical solutions, employee training, incident response planning and stakeholder collaboration is imperative.

Effective cyber defence requires, among others: cybersecurity strategies tailored to the specific needs of each different industry sector - including addressing their respective unique vulnerabilities and compliance requirements - and maintaining a common foundation in employee awareness, training, data protection and incident response preparedness.

A constant and collective collaborative effort between the various industries and Government is also strongly emphasised and encouraged to protect the entire ecosystem.

In essence, integrating business dynamics into security planning is crucial. Ultimately, a holistic strategy merging technical solutions with human-centric practices, compliance efforts and business considerations is vital for robust cybersecurity resilience and data protection.

Conclusion

In summary, this research paper stands as a crucial contribution to the ongoing dialogue on cybersecurity, providing stakeholders with the knowledge needed to navigate the complexities of the digital age more effectively.

Through its comprehensive methodology, cross-sectoral analysis and collaborative efforts, the study aims to enhance the collective understanding of our local industries against an ever-evolving array of cybersecurity threats. Going forward, we will endeavour to carry out subsequent studies and their accompanying reports on a regular basis.

RAPID7

TAKE COMMAND OF THE ATTACK SURFACE

Breaches are officially "inevitable".
We disagree. It's time for new thinking.

One simple subscription to Managed Threat Complete and your environment is monitored end-to-end, 24/7, by an elite SOC that works transparently with your in-house team.
Your resources expand. Your proactivity goes up. And your risks and worries go down.

Learn more at rapid7.com or email apacsales@rapid7.com

Don't miss our keynote Wednesday 8th May;

Take Command Of Your Attack Surface

Denis Donnelly, Regional Director, Asia & India, Rapid7

In this presentation, Denis will discuss how Malaysian organisations can gain a better end-to-end view of their risk environment to deliver more accountable and effective monitoring.

Scan to register!

TAKE COMMAND
2024 Cybersecurity Summit

One Day Virtual Event | May 21 2024

If you are ready to take command of your attack surface, join us at Take Command for a one-day, global, virtual event featuring some of the most effective cybersecurity practitioners in the industry and the best research available.

QUALITATIVE INSIGHTS

Cybersecurity Landscape 2024

Cybersecurity has become a priority concern for companies in 2024 as they increasingly shift towards digital platforms, resulting in heightened risks of cyber attacks across various industries and sizes.

The digital expansion of businesses, alongside the growing use of connected devices and the Internet of Things (IoT), is expanding the target field for cyber criminals, whether they are hackers for gain or merely hackers for fun. The array of cyber threats is broadening, ranging from ransomware and phishing to social engineering and disruptions in the supply chain.

The fallout from a cyberattack can be severe, encompassing not just financial setbacks but also reputational harm and legal repercussions. This necessitates that enterprises constantly adapt to the latest trends and adhere to best practices to defend against cyber-attacks and thrive in the digital landscape.

This section of the report collates and curates insights from in-depth interviews with 14 organisations across different industries in order to paint a sweeping picture of the challenges and strategies in cybersecurity among Malaysian companies.

QUALITATIVE INSIGHTS

Types of Cyber Attacks

According to interviewees, organisations succumb to phishing and ransomware attacks due to weaknesses in email security, inadequate access restrictions and human error, including the mishandling of credentials or the inability to identify malicious emails.

Weaknesses that Cause Breaches

The interviews with selected industry representatives highlighted common weaknesses that have paved the way for cyber breaches at their companies. They include:

The human factor

Although compliance and policies lay the foundation, the human aspect within an organisation is crucial in either strengthening or compromising these measures. The risk of internal threats, whether deliberate or unintentional, underscores the vulnerabilities tied to human behaviour. This emphasises the importance of fostering a security-conscious culture throughout the organisation. Therefore, it is essential to prioritise employee awareness via ongoing education and thorough screening processes during recruitment.

Exploited vulnerabilities

A range of vulnerabilities, including flawed website coding, lax patch management and mistakes by third-party developers, create opportunities for unauthorised access to data and systems.

IoT and endpoint security gaps

Weaknesses in IoT device security and insufficient endpoint protection create pathways for network breaches, malware infiltrations and the compromise of data.

Internal system weaknesses and risky behaviour

Deficiencies in internal security protocols and procedures, along with risky employee habits such as utilising personal devices for work purposes, substantially elevate the risk of breaches.

Backup system targets

Cyber attackers leverage vulnerabilities in backup storage to impede recovery efforts, exploiting weaknesses within backup infrastructure.

Beyond the above weaknesses, interview respondents also highlighted other indirect root causes of cybersecurity breaches. They include:

- *Monitoring and awareness deficiencies:* Organisations become more susceptible to breaches due to the absence of real-time detection capabilities and a general lack of cybersecurity awareness among employees. Strengthening detection methods and implementing continuous educational initiatives is imperative.

- *Training and preparedness shortfalls:* Despite the presence of current programmes, continuous training and well-defined incident response protocols are indispensable for effective mitigation of breaches.

- *Misaligned management priorities:* Prioritising short-term financial gains over investments in cybersecurity compromises long-term security and resource allocation.

- *Compliance and responsibility gaps:* Difficulties in meeting standards such as ISO 27001, coupled with a fragmented approach to cybersecurity responsibilities, underscore the necessity for a more cohesive and dedicated security strategy across organisations.

Impact of Breaches

The hesitation to invest in cybersecurity often originates from concerns about return on investment (ROI). However, a failure to invest could result in major data breaches that incur severe financial losses and also other non-financial consequences such as damage to reputation, disruptions in operations, and the erosion of customer trust and loyalty over the long term.

Survey respondents listed some of the main financial and non-financial impact of cyber breaches they encountered over the past three years:

FINANCIAL

Revenue loss
Breaches can lead to significant revenue losses due to operational disruptions and affected customer trust.

Recovery and mitigation costs
The financial burden of data recovery, system restoration and the implementation of preventive measures is significant. Costs associated with deploying solutions such as endpoint detection and response (EDR), managed detection and response (MDR), data loss prevention (DLP) and data classification are essential for preventing and detecting breaches.

Investigation and response expenses
Financial resources must be allocated for forensic analysis, response teams and carrying out remediation efforts in the aftermath of a breach.

NON-FINANCIAL

Reputational damage
The loss of customer trust and market credibility following a breach can have long-lasting effects on an organisation.

Operational disruption
Breaches disrupt business operations, resulting in downtime, productivity losses and potentially substantial revenue declines.

Resource allocation and communication
A considerable amount of time and resources are dedicated to managing the breach, communicating with stakeholders and engaging cybersecurity vendors. These efforts impact normal operations.

Customer trust and loyalty erosion
Breaches can affect customer loyalty, leading to long-term revenue implications as customers migrate to competitors. Rebuilding trust requires significant investments in communication and security enhancements.

The extensive repercussions of data breaches highlight the importance of proactive cybersecurity investments to mitigate risks and effectively safeguard organisational assets.

CONCLUSION

The findings underscore the complexity of data breaches, influenced by a host of factors including system vulnerabilities, human error, compliance gaps and response inadequacies. While regulatory compliance provides a baseline, it is insufficient to guarantee immunity from breaches, necessitating continuous monitoring and proactive measures.

Proactive strategies involve a combination of technical solutions, employee training, incident response planning and stakeholder collaboration. In addition, the impact of business dynamics on cybersecurity highlights the importance of integrating business considerations into security planning.

The growing threat in cybersecurity protection is inevitable while the constraints of technical expertise and trained resources within the industries have accelerated the demand for service providers who specialise in cybersecurity consultancy, managed security services, incident response and forensics.

Overall, a holistic approach that blends technical solutions with human-centric practices, compliance efforts and business considerations is essential for effective cybersecurity resilience and data protection.

Forcepoint

Data Security Everywhere

Empowering people to work anywhere, with data everywhere.

Contact Us for a Demo:

QUANTITATIVE RESULTS

Cybersecurity Survey 2024

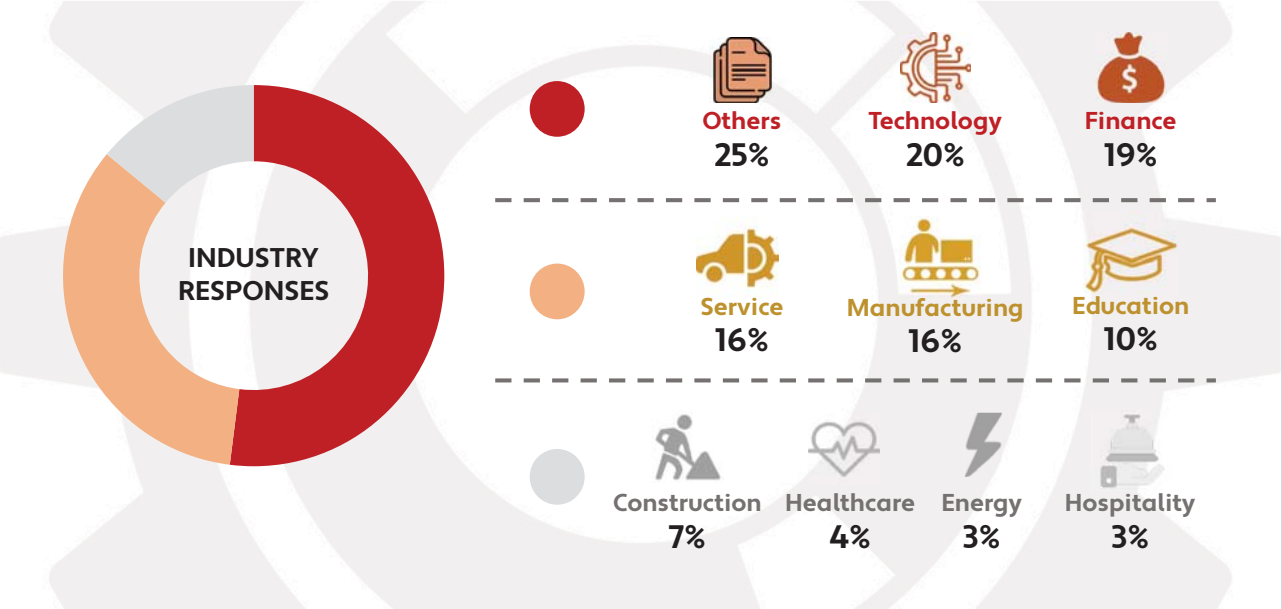
Survey respondents came from a diverse range of industries that form the bedrock of Malaysia's economy. Naturally, the technology, finance, manufacturing and services segments where cybersecurity is particularly critical, contributed the bulk of the respondents.

Others included industry leaders and representatives from various industries such as property, eCommerce, investment, utilities, waste management, chemicals, logistics, food and telecommunications.

Most survey participants were from the private sector with the balance from respondents answering as individuals or on behalf of non-governmental organisations (NGOs). A total of four respondents were from government agencies.

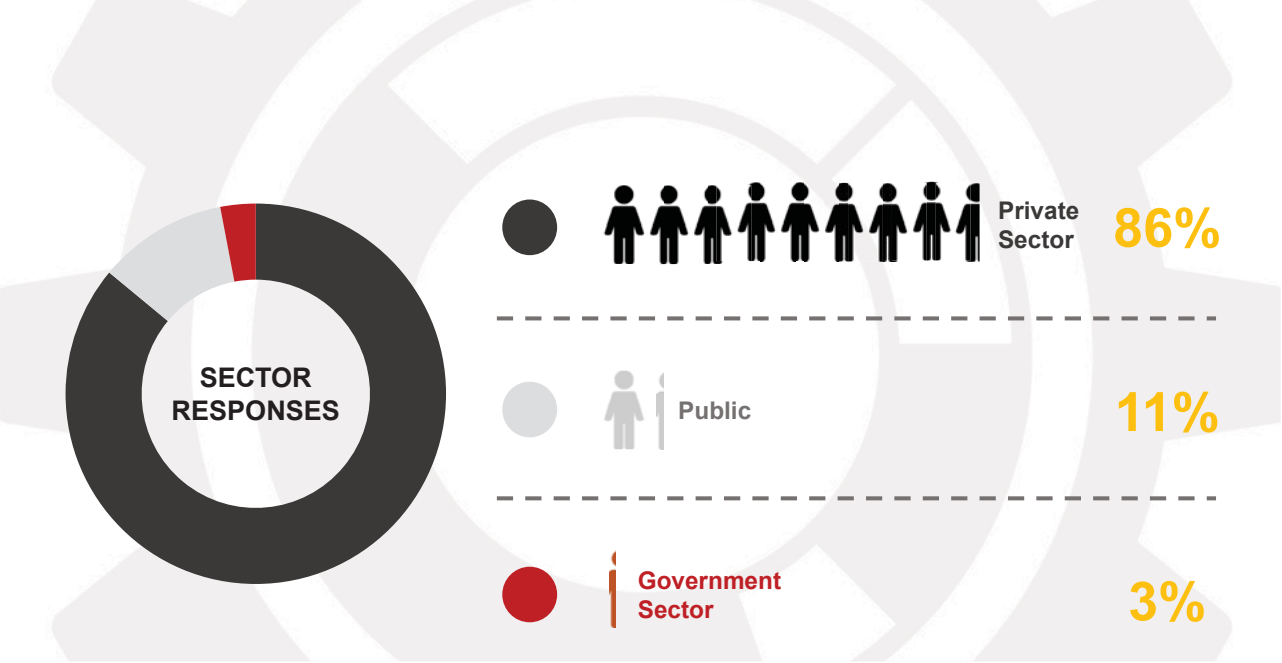
The analysis and reporting of the survey findings are supported and supplemented by external insights from desktop research to provide greater context and comparison with the responses from local organisations.

Survey Responses According to Industries



*Total of 149 responses from 122 individual respondents, some of whom selected more than one industry. Percentages are calculated from the absolute number of responses against 122.

Survey Responses According to Sector



According to respondents, almost 70% of companies were victims of cyber breaches in the past three years. However, only one in five reported an average of more than one successful attack per year during that period.

Malaysia was recently cited as the eighth most breached country in Q3 2023 by Netherlands-based cybersecurity company Surfshark. Citing a 144% increase in the breach rate in comparison to the previous quarter (Q2 2023), Surfshark also ranked Malaysia at number five in terms of breach density.

https://www.thestar.com.my/tech/tech-news/2023/12/06/cybersecurity-report-ranks-malaysia-as-eighth-most-breached-country-in-q3-2023

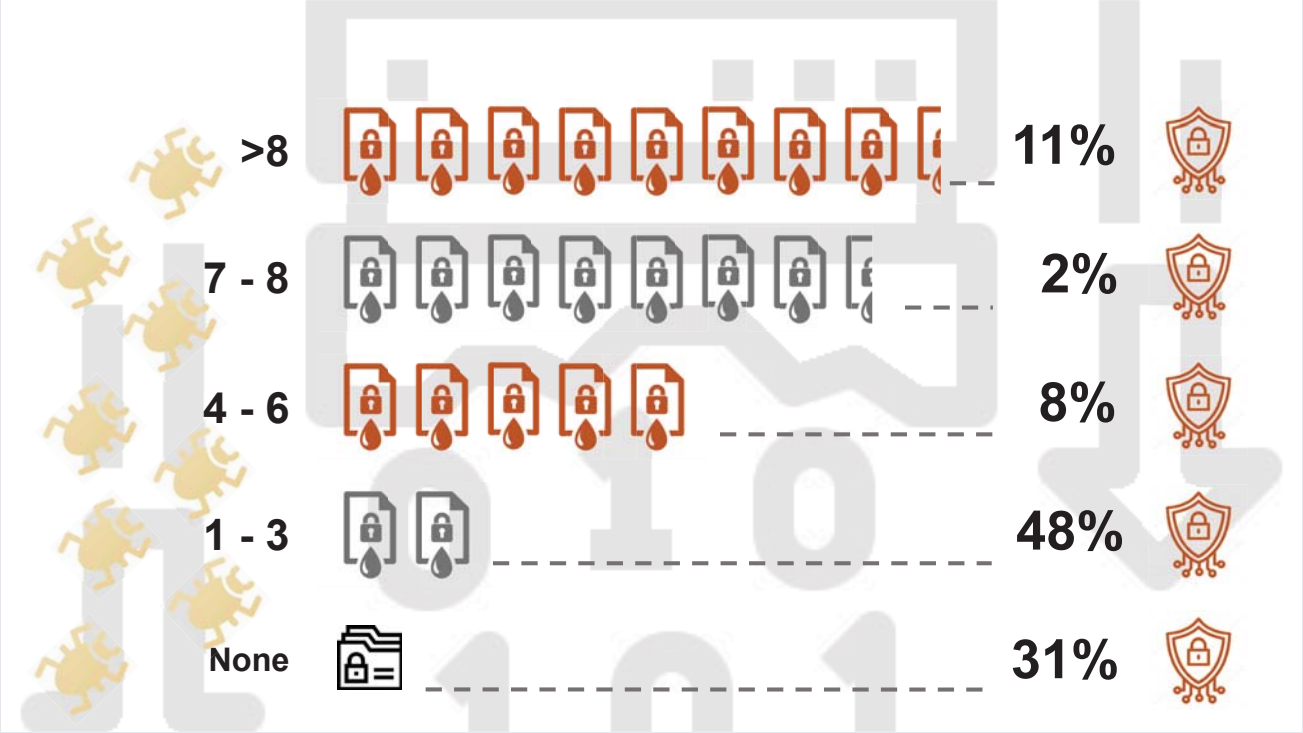
Another global cybersecurity firm, Kaspersky, pointed out that Malaysia was second in Southeast Asia for mobile malware attacks prevented by the company in 2022.

https://www.nst.com.my/news/nation/2023/07/935644/kaspersky-malaysia-ranks-second-southeast-asia-mobile-malware-attacks

On a broader perspective, a 2023 survey of 4,000 cybersecurity managers in 14 countries including Malaysia by American digital services provider, Cloudflare, found that 78% reported at least one incident in the previous 12 months with more than 60% indicating four or more attacks in that timeframe.

https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/

Q1: Number of Breaches and / or Attempts in Last Three Years



Survey participants also rated the severity of the cyber breaches and extensiveness of data compromised during the attacks. Less than a third categorised their breaches as serious (level 3 or higher) while 17% noted that data compromised were comparatively considerable (level 3 or higher).

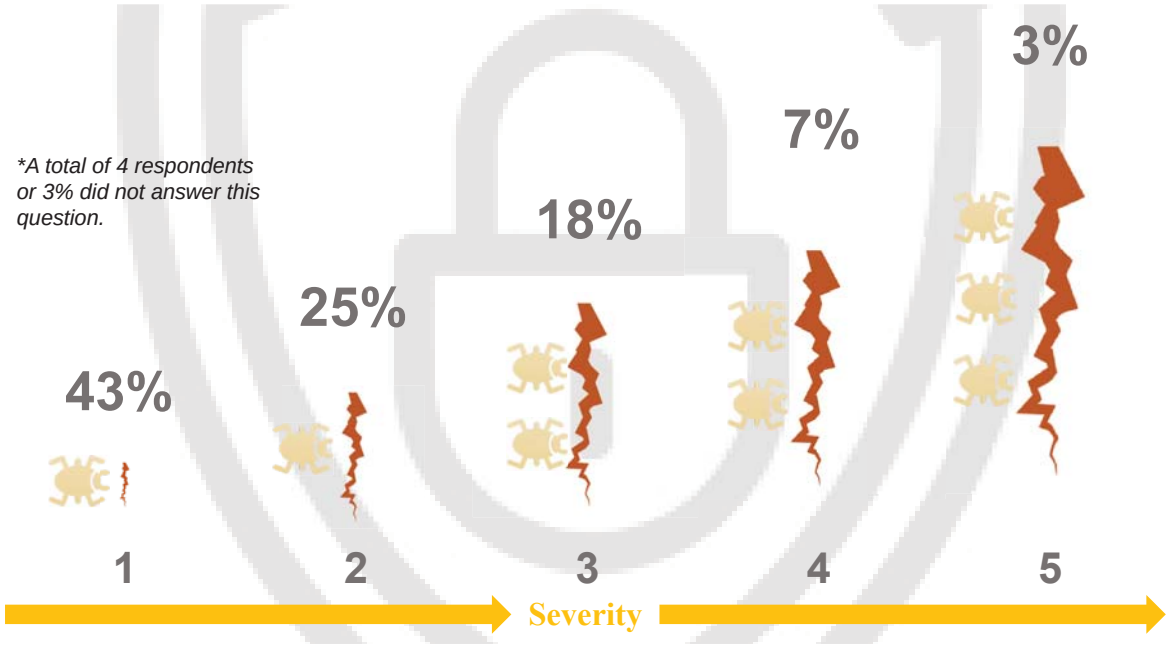
A Mid-Year Threat Landscape Report 2023 by Cybersecurity Malaysia gauged that more than 70% of the incidents were leaks associated with the administrator control interface (C Panel), customer data and sensitive data.

https://www.thestar.com.my/tech/tech-news/2023/10/25/cybersecurity-malaysia-report-government-sectors-suffered-most-data-breaches-while-telcos-spilled-over-400gb-of-data-in-h1-2023

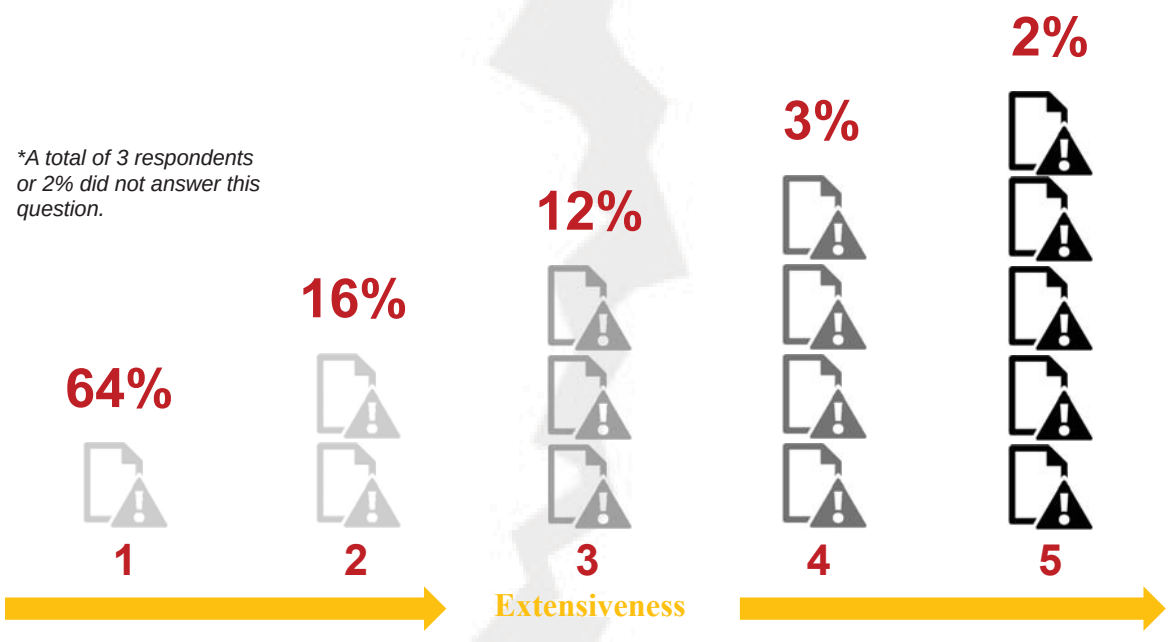
Although a significant number of these breaches were against government portals and websites, almost 80% of the attacks were on private sector domains in the telecommunications, education and retail industries, according to Cybersecurity Malaysia.

The cybersecurity sentinel formed by the Government also noted what it termed as a "staggering amount of 842.84gb" of data leaked in the attacks, with the telecommunications sector bearing the bulk of it at 424.92gb.

Q2: Severity of Breaches



Q3: Extensiveness of Data Compromised in Breach

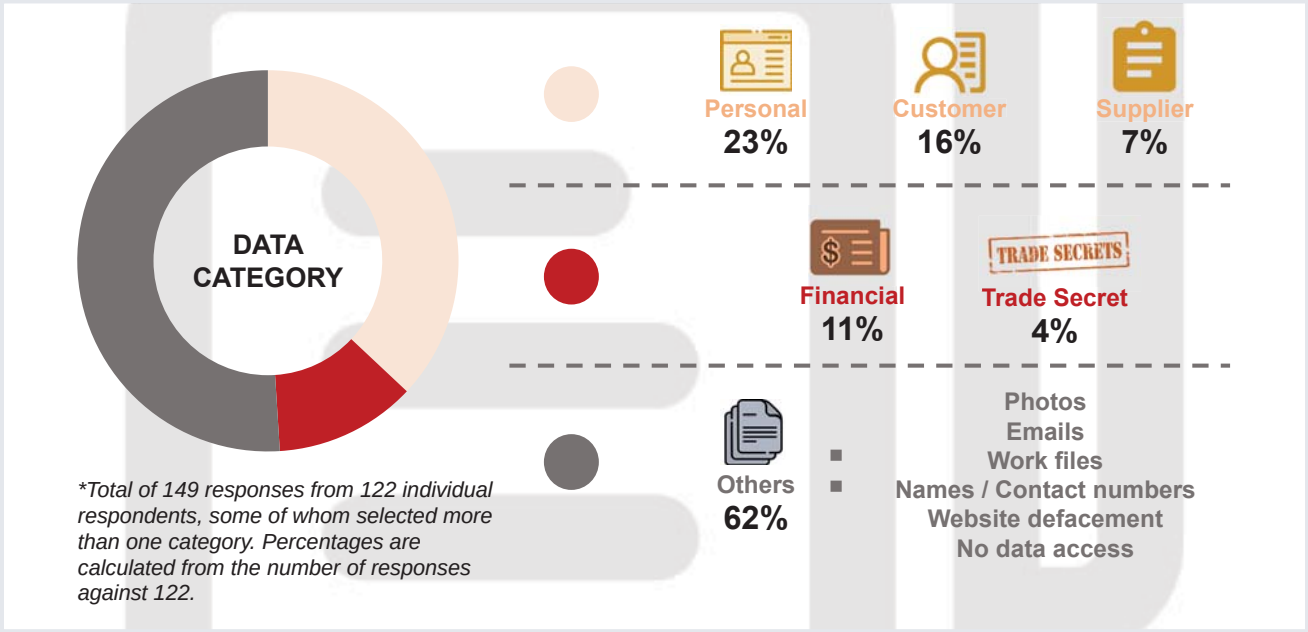


Some 15% of survey respondents indicated that data compromised during cyber breaches involved financial information and trade secrets, two categories that are extremely sensitive to organisational interests. Another 46% stated that compromised data included personal, customer and supplier, types of information normally considered sensitive.

This is consistent with the estimation by Russian information security specialist, Positive Technologies (Ptsecurity), whose survey in 2023 noted that 49% of successful cyber attacks resulted in the compromise of sensitive data. According to Ptsecurity, 27% of these breaches disrupted business operations.
https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/

Responding to a related question in the PIKOM survey, however, participants appeared to have a different benchmark for what they considered 'sensitive' data. Only 21% (level 3 or higher) deemed the compromised data to be sensitive with more than half appearing to be seemingly nonchalant over the impact.

Q4: Types of Data Compromised



**Total of 149 responses from 122 individual respondents, some of whom selected more than one category. Percentages are calculated from the number of responses against 122.*

Q5: Sensitivity of Compromised Data

**A total of 7 respondents or 6% did not answer this question.*

As expected, ransomware and malware topped the list for causes of breaches, with survey respondents also highlighting social engineering and misconfigured systems as weaknesses inviting cyber attacks.

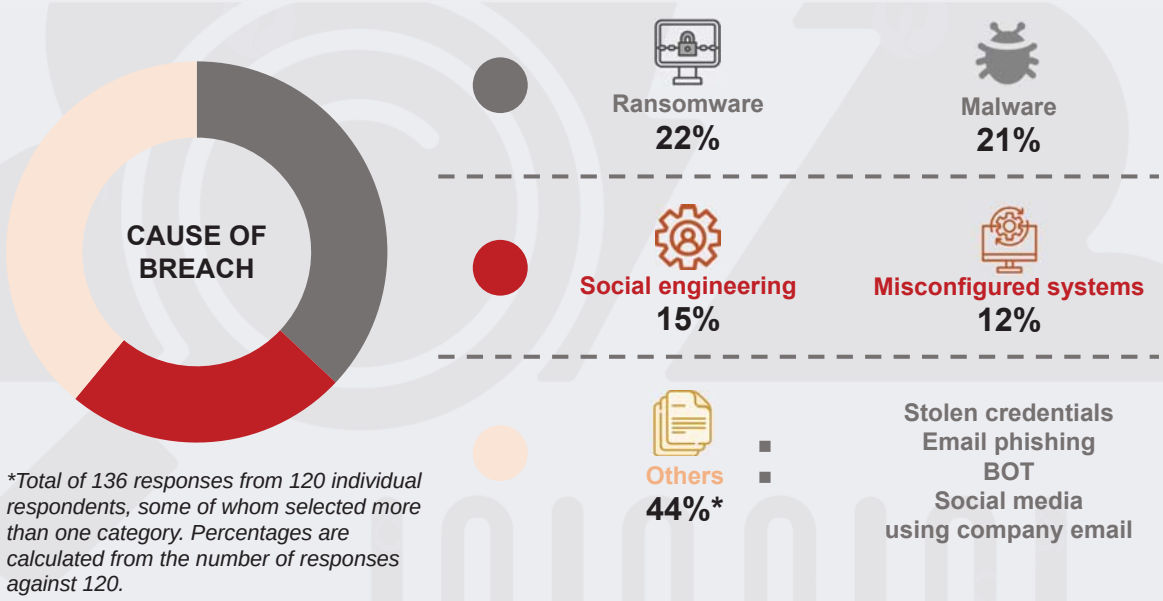
Overall, the main causes of breaches at the global level include misconfigured settings, social engineering, recycled passwords, theft of sensitive devices, software vulnerabilities and use of default passwords, according to third-party risk and attack surface management platform Upguard.

https://www.upguard.com/blog/common-data-leak-causes

In the case of data security firm Lepide, its list in order of most common causes was misuse of privileged access, weak and stolen passwords, unpatched applications, malware, social engineering and physical breaches.

https://www.lepide.com/blog/six-common-causes-of-data-breaches/

Q6: Cause of Breach



**Total of 136 responses from 120 individual respondents, some of whom selected more than one category. Percentages are calculated from the number of responses against 120.*

Almost three quarters of survey participants responded that they avoided any financial losses from the cyber attacks in 2023. Further, the remaining respondents quantified their losses at below RM500,000.

A Cost of Data Breach report by IBM estimated an average cost of US$3.05 million in Asean economies including Malaysia, which was an all-time high. The report also cited the financial and energy sectors as the most impacted across the region.

https://cybersecurityasean.com/news-press-releases/record-high-data-breach-costs-asean-malaysia-businesses-face-305m-impact

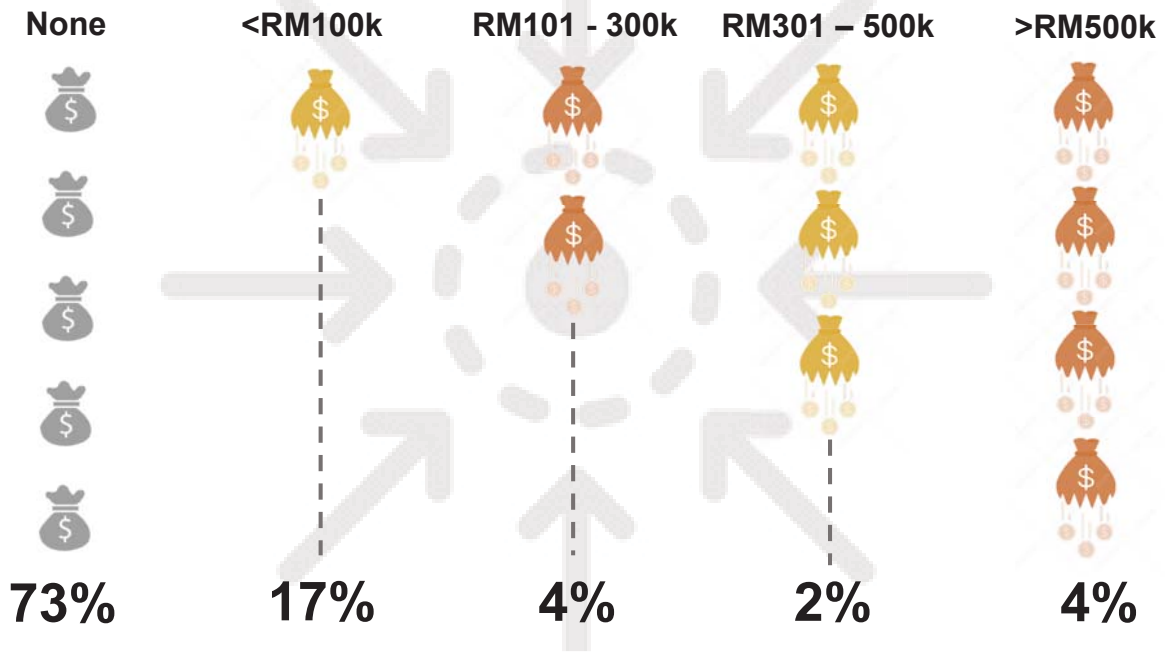
Last year, Cloudflare conducted a survey of 207 local companies and published the results in a Securing The Future: Asia Pacific Cybersecurity Readiness Survey report. According to the report, these intrusions were largely made via vectors such as web attacks (68%), phishing (60%) and BECs (46%). Overall, 48% of the affected companies report a financial impact of at least US$1 million, while 31% say they lost US$2 million.

https://www.thestar.com.my/tech/tech-news/2024/01/08/new-year-familiar-threats-cybersecurity-experts-warn-of-the-threats-to-come-for-2024

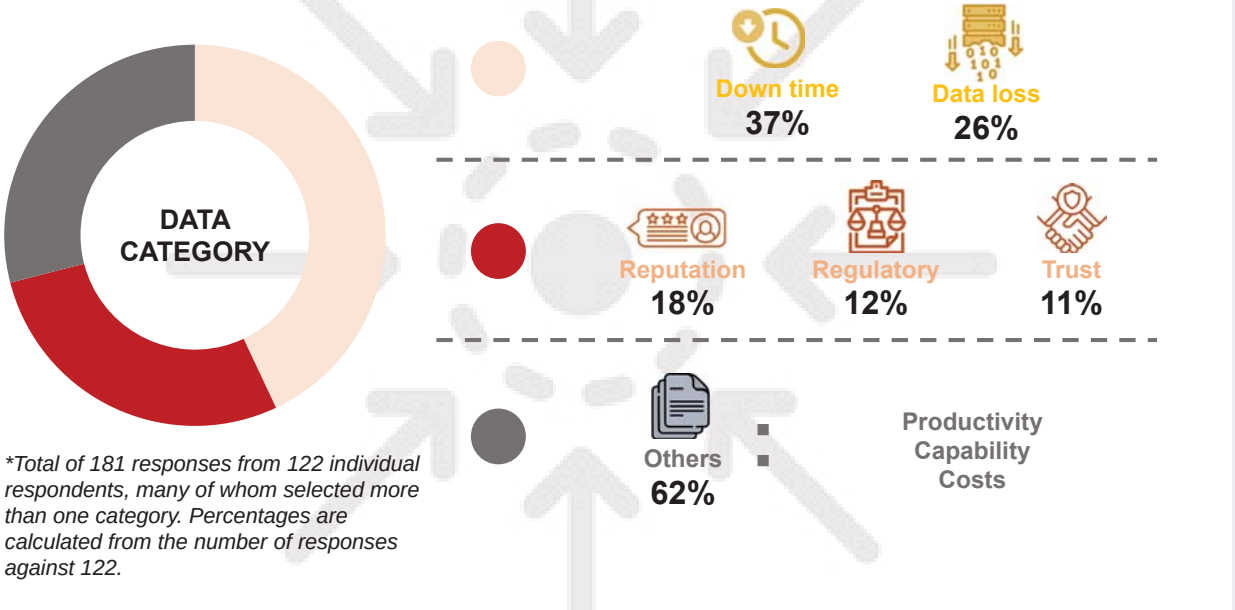
Meanwhile, Malaysia's National Scam Response Centre (NSRC) recorded a total loss of RM27 million from 456 cyber fraud cases flagged by Cybersecurity Malaysia in the first two months of 2023. This is about RM60,000 per case, supporting the contention of our survey participants.

https://themalaysianreserve.com/2023/07/26/alarming-rise-in-online-attacks-malaysias-cyber-security-landscape-in-2023/

Q7: Financial Impact



Q8: Non Financial Impact



**Total of 181 responses from 122 individual respondents, many of whom selected more than one category. Percentages are calculated from the number of responses against 122.*

The majority of survey participants pointed to down time and data loss as the most adverse non-financial impact of cyber breaches. Many also highlighted the implications to their company's reputation, trust and assurance, and potential legal consequences.

These findings are echoed by most cybersecurity firms. One such firm, MetaCompliance, disclosed the main impacts as reputation damage, legal actions, operational disruptions and nefarious use of sensitive personal data against individuals.

https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-data-breach

An overwhelming nine in 10 survey respondents stated their organisations have cybersecurity measures in place. Some 6% replied in the negative, which is surprising given the growing threat and ominous implications of current cyber breaches.

However, the high number of organisations with cyber protection is less relevant than the robustness of their existing measures against the increasingly strident and potent attacks these days, as pointed out by Cisco.

In its inaugural Cybersecurity Readiness Index, the global tech solutions provider noted that only 16% of Malaysian organisations have a 'mature' level of readiness to be resilient against modern cyber risks, which is marginally above the global figure of 15%.

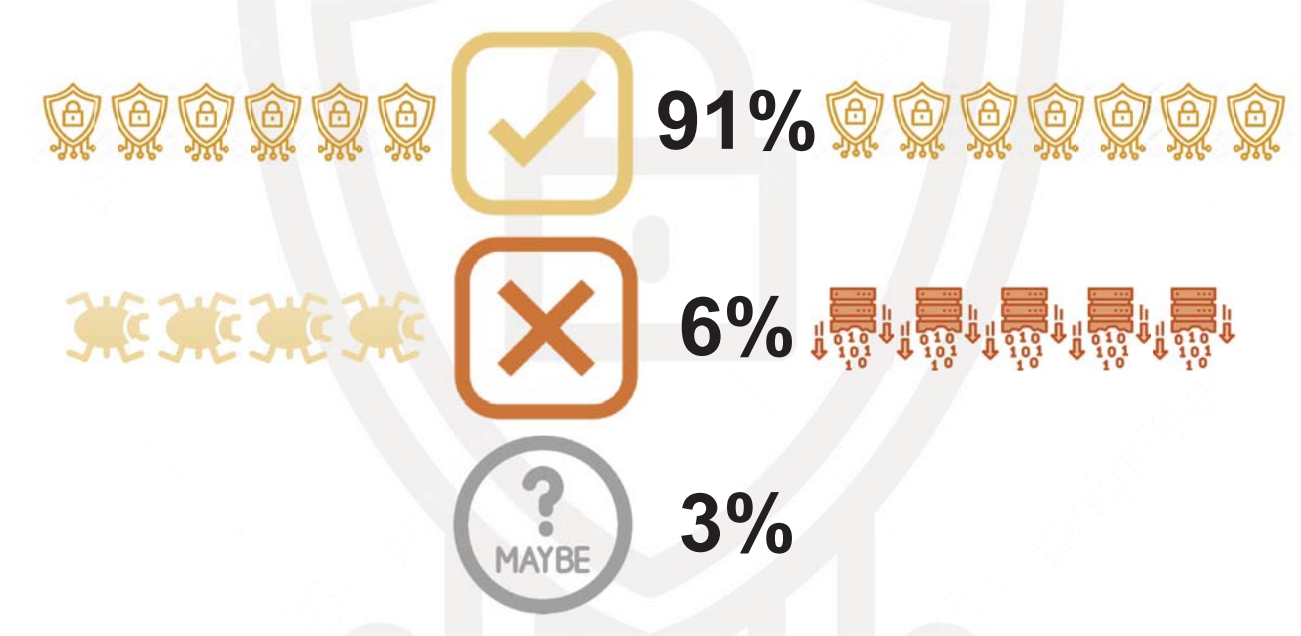
https://techwireasia.com/03/2023/cisco-most-organisations-in-malaysia-are-not-ready-to-defend-against-cyber-threats

Nevertheless, only about a quarter of survey participants cited shortcomings of cybersecurity measures as the reason for successful data breaches. It is interesting to note that Malaysia continues to suffer from a distinct lack of cybersecurity experts with only 15,000 out of the required number of 27,000.

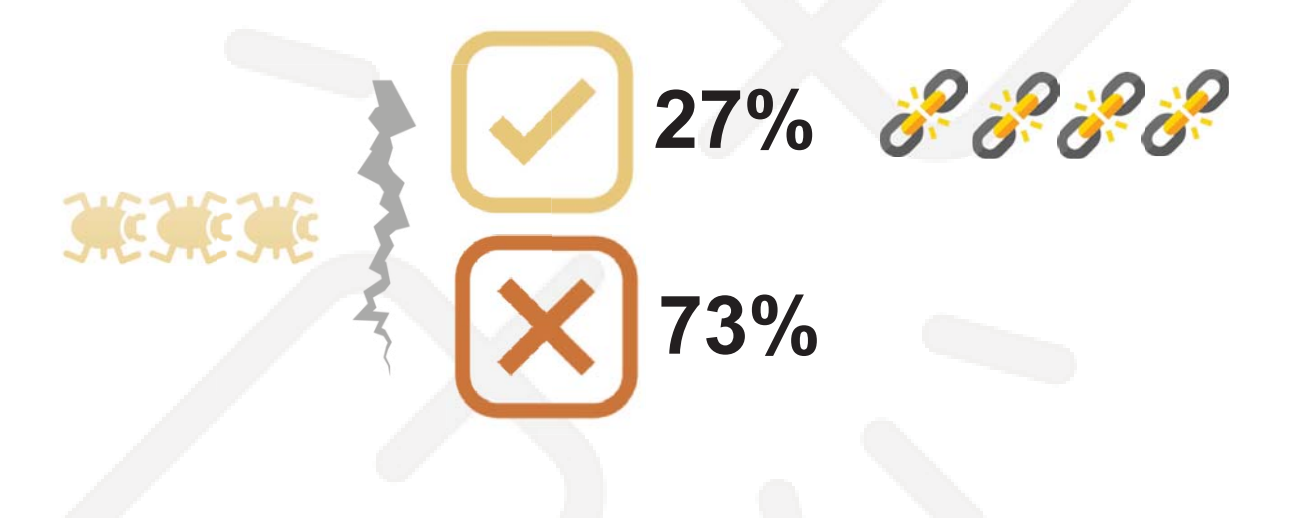
Communications and Digital Minister Fahmi Fadzil had pointed this out, adding that the shortfall of 12,000 experts was one of the main challenges hampering the implementation of the national digitalisation agenda.

https://www.nst.com.my/news/nation/2023/10/969613/malaysia-short-12000-experts-tackle-cyber-attacks-fahmi

Q9: Existence of Security Measures



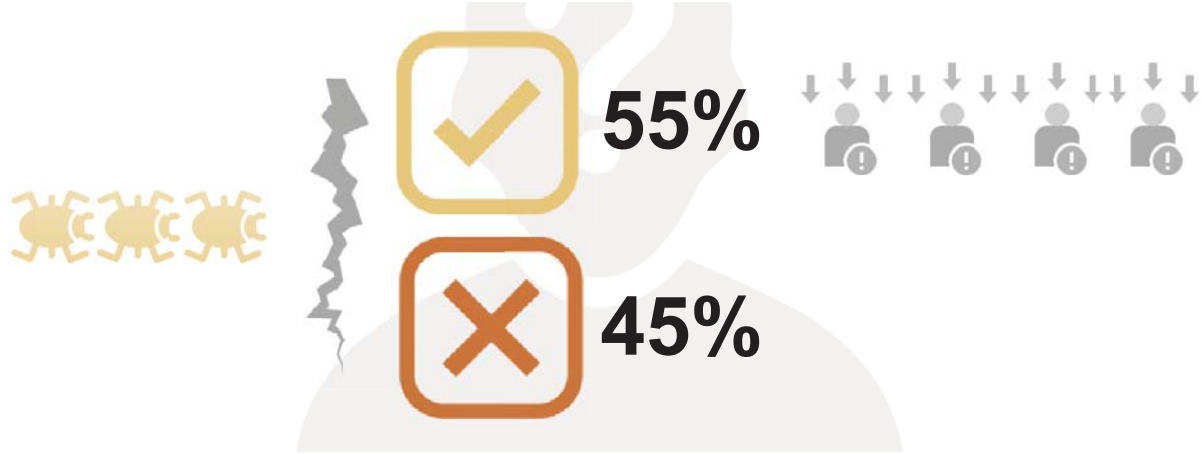
Q10: Breaches Due to Shortcomings of Security Measures



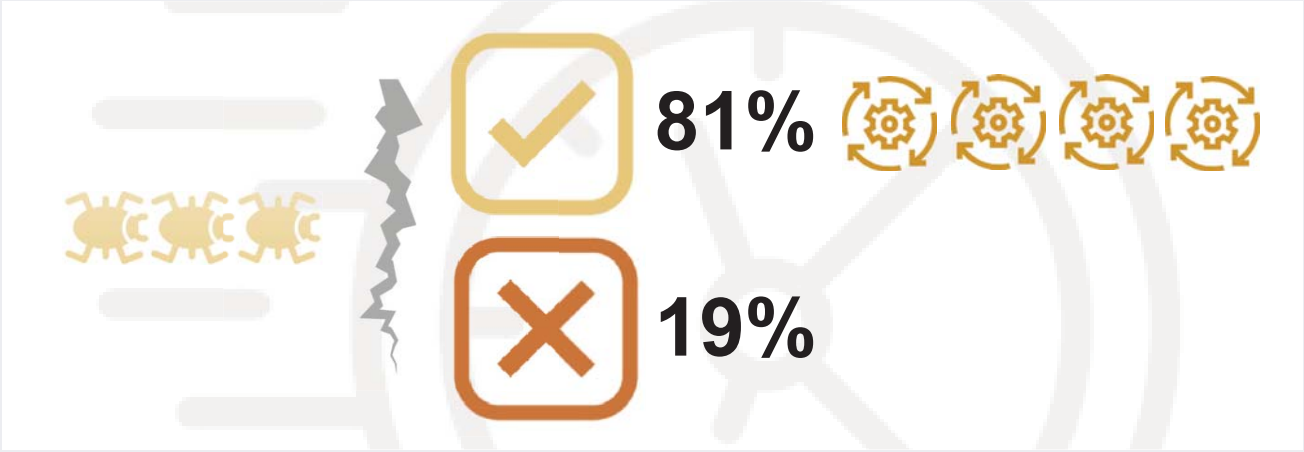
Instead of inadequate protection, more than half the survey respondents blamed human error or ignorance as the cause of the breaches. This finding is consistent with those from Verizon's 2023 Data Breach Investigations Report, which identified the human element as the most common threat vector at 74%.

https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020#

Q11: Breaches Due to Human Error or Ignorance



Q12: Existence of Response Strategy



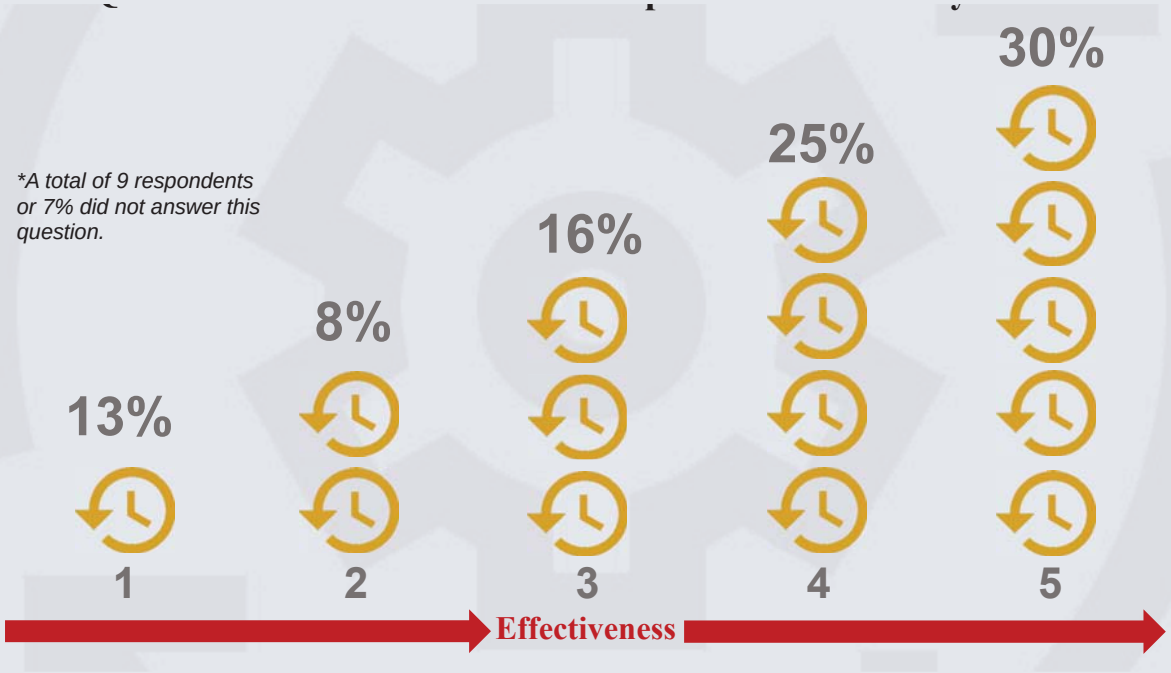
Prompt action taken in the event of a cyberattack is critical to contain the breach and mitigate the impact of the incident. According to IBM, companies can take up to 197 days to identify a breach and an average of 69 days for control and containment.

https://frsecure.com/blog/incident-response-statistics-how-do-you-compare/

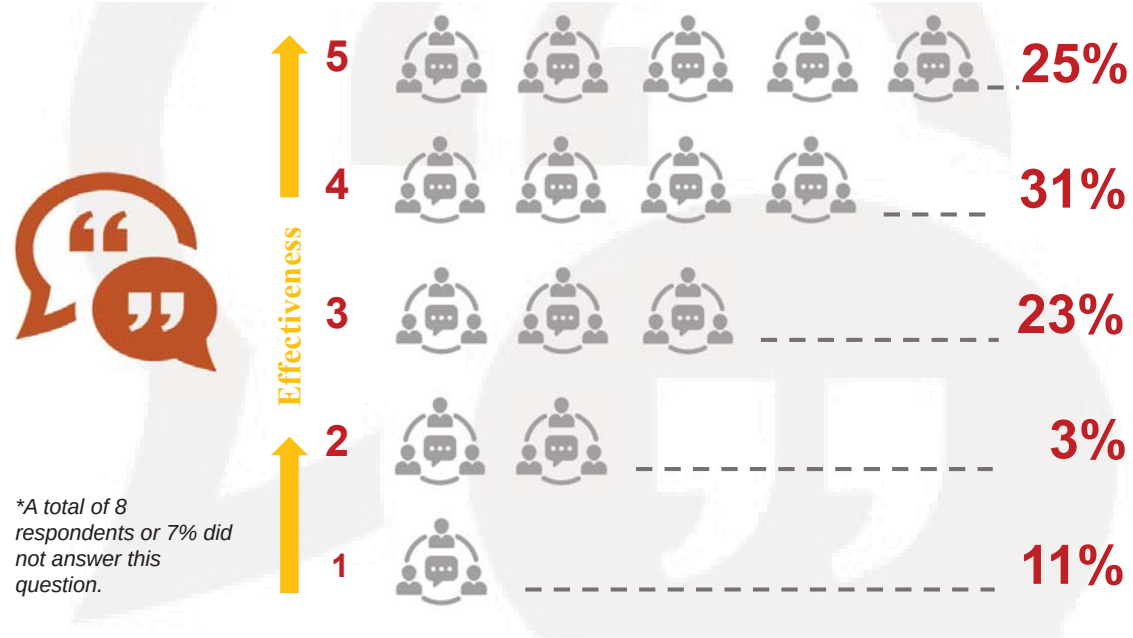
American cybersecurity solutions provider FRSecure found in a survey at the end of 2022 that an estimated 45% of US-based companies had established incident response plans. According to PIKOM's survey, four in five of the survey participants have a response strategy in place.

Survey respondents were overwhelmingly positive over the effectiveness of their incident response and recovery as well as communication efforts during and in the aftermath of a breach. Almost four in five responses rated their response and recovery actions as effective (level 3 or higher) while 86% lauded their communication to stakeholders.

Q13: Effectiveness of Incident Response and Recovery Efforts



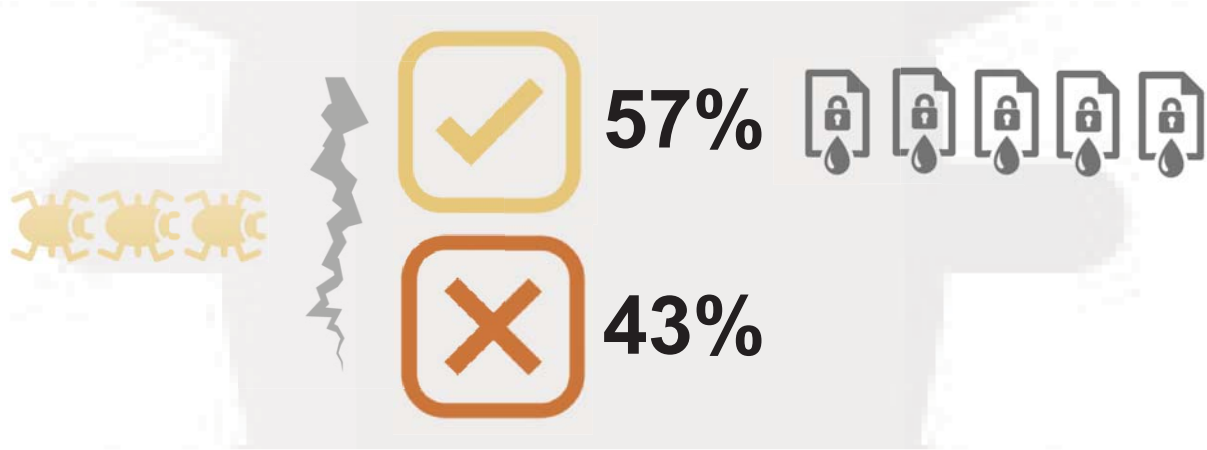
Q14: Effectiveness of Communication during and after Breach



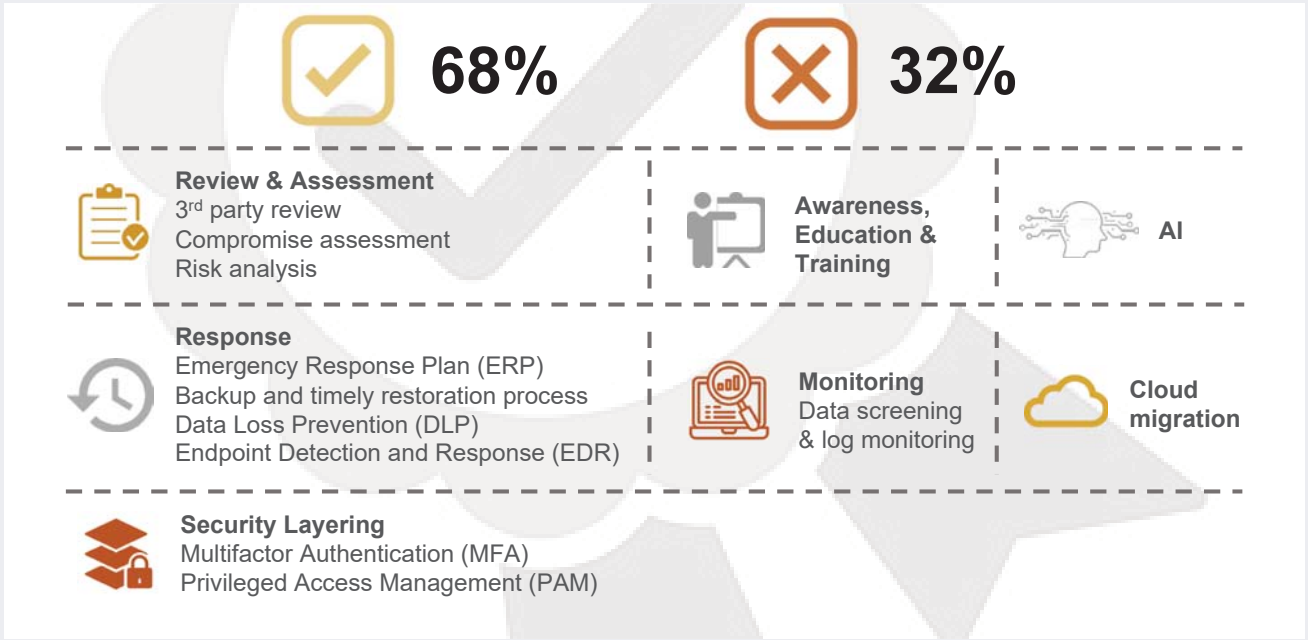
More than half the respondents expected further breaches in 2024 and beyond. This concern is echoed by most cybersecurity firms and experts who have warned of a rising wave in artificial intelligence (AI) powered cyberthreats, especially in phishing attacks.

https://www.thestar.com.my/tech/tech-news/2024/01/08/new-year-familiar-threats-cybersecurity-experts-warn-of-the-threats-to-come-for-2024

Q15: Likelihood of Further Breaches



Q16: Best Practices that could have Prevented or Mitigated Breach



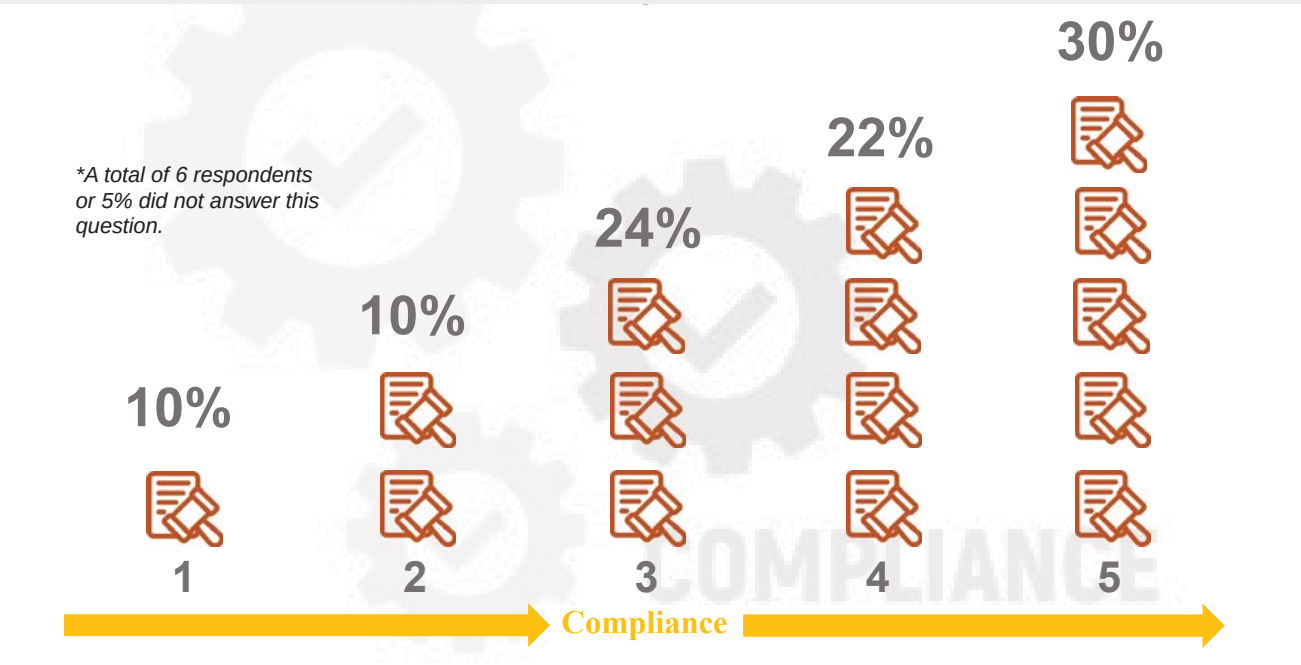
Almost seven in 10 respondents indicated they were aware of best practices in cybersecurity that could have prevented or mitigated breaches. The survey participants identified some of these practices as regular monitoring, periodic review and assessment, response plans and strategies, security layering, migration to cloud, deployment of AI as well as education and training.

Similarly, online learning platform Coursera listed nine practices as follows:

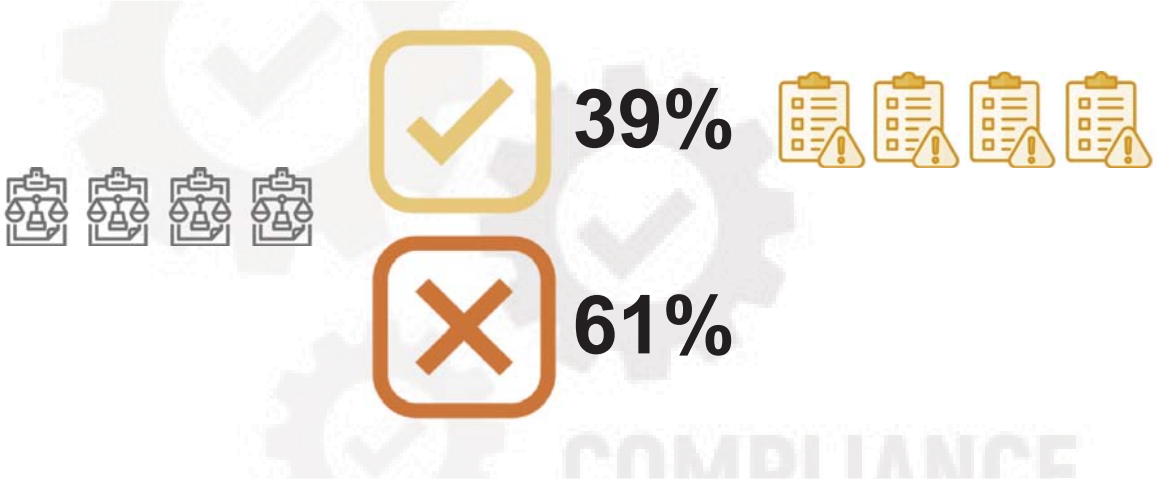
- Implement a robust cybersecurity strategy;
- Update and enforce security policies;
- Install security updates and backup data;
- Use strong passwords and multi-factor authentication;
- Collaborate with the IT department to prevent attacks;
- Conduct regular cybersecurity audits;
- Control access to sensitive information;
- Monitor third-party users and applications; and
- Embrace IT training and education.

https://www.coursera.org/articles/cybersecurity-best-practices

Q17: Compliance to Regulations prior to Breach



Q18: Impact of Compliance / Non-compliance to Regulations on Breach



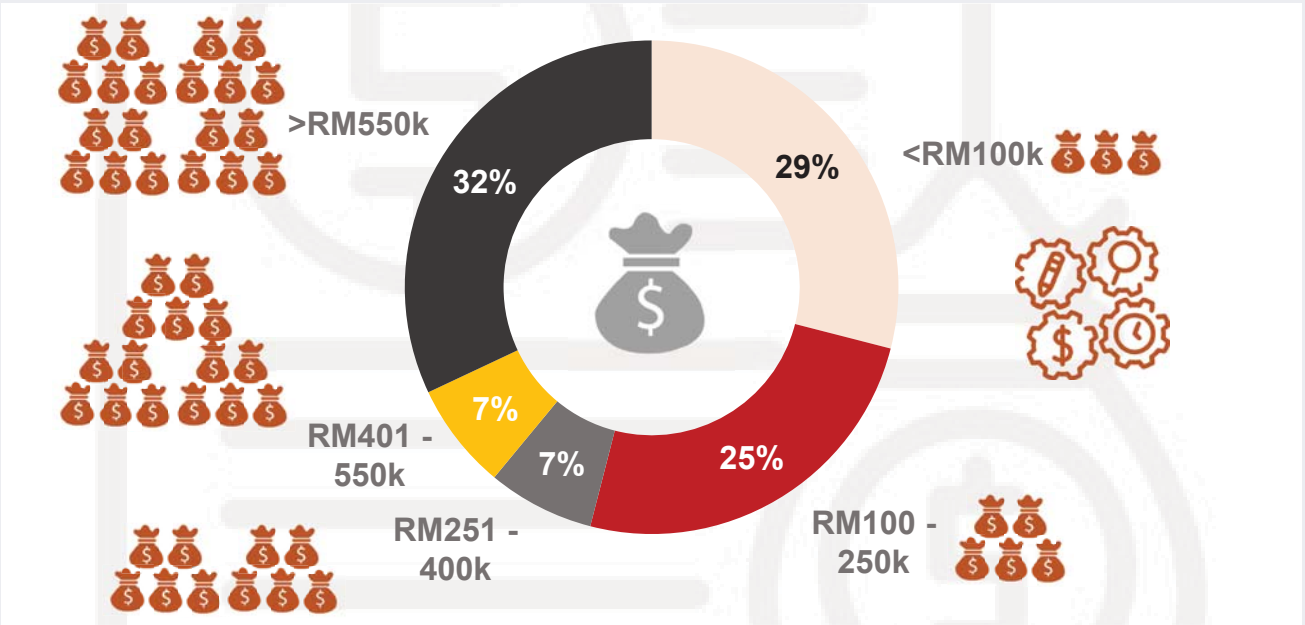
The majority of survey respondents (four in five) claimed the cyber breaches occurred despite their organisations' compliance with relevant regulations (level 3 or higher). An estimated two in five agreed that non-compliance to regulations contributed to the success of the cyber attack attempts.

More than 70% of organisations surveyed employed fewer than six dedicated security personnel with a mere 7% having cybersecurity teams larger than 20 talents. According to management consultant Avasant, the average number of cybersecurity personnel in companies amounted to 4.2% of employee headcounts in 2023. This works out to at least two dedicated personnel for companies with 50 employees and at least 20 for those with 500.

https://avasant.com/report/it-security-staffing-ratios-2024/#

Q19: Number of Dedicated Security Personnel in Organisation

Q20: Annual Budget for Cybersecurity



About two thirds of organisations participating in the survey allocate less than RM550,000 for their annual cybersecurity budget with slightly more than half spending less than RM250,000 for protection. From a benchmarking perspective, the IANS & Artico Security Budget Benchmark Summary Report 2022 noted that US-based companies spent an average of 9.9% of their IT budgets on cybersecurity in 2022.

https://venturebeat.com/security/benchmarking-your-cybersecurity-budget-in-2023/

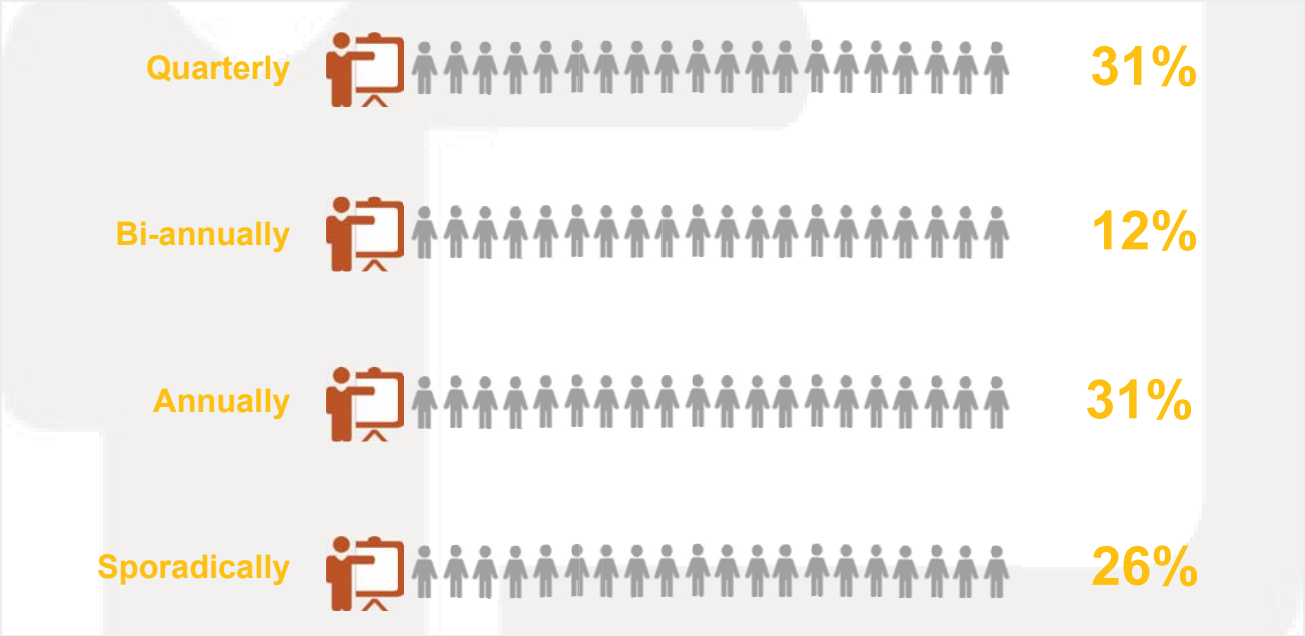
It is worth noting that one third of Malaysian organisations have increased their cybersecurity budget by 50% in 2023, according to the Palo Alto Networks' 2023 State of Cybersecurity ASEAN report. The report stated that Malaysian organisations have the highest percentage of spending across the ASEAN region.

https://techwireasia.com/09/2023/businesses-in-malaysia-increase-cybersecurity-budget-allocation-in-2023/

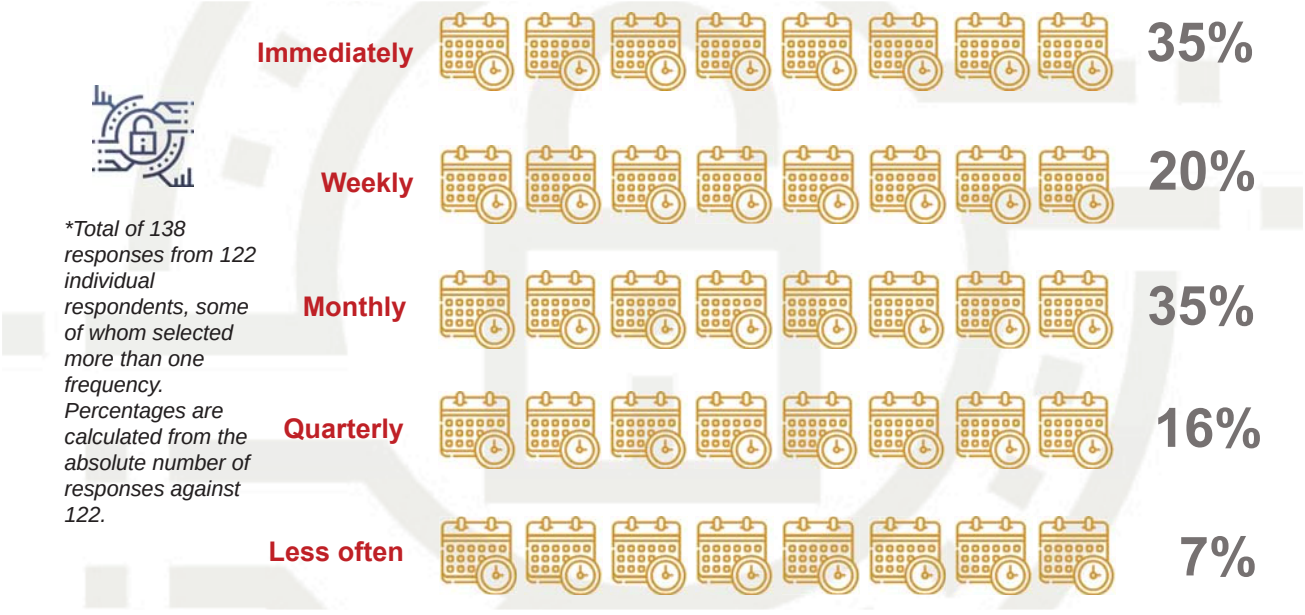
Less than half of organisations provide training on cybersecurity awareness at least once every six months, according to survey respondents. About three quarters of these organisations ensure training is conducted every year. ISACA, the international professional association focused on IT governance, has recommended that training be held every four to six months.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training#

Q21: Frequency of Training on Cybersecurity Awareness



Q22: Frequency of Security Patches and Updates to Software and Systems



Slightly more than half the organisations in the survey performed daily or weekly patching or upgrades to their cybersecurity software and systems. Another 35% of respondents stated their organisations carried out such tasks at least once a month.

According to US-based cybersecurity service provider RSI Security, patch management for software and systems should be conducted daily with detailed assessments weekly or monthly if organisations are businesses that process payments via credit and debit cards, or are in the healthcare, energy and finance industries.

https://blog.rsisecurity.com/how-often-should-you-perform-patch-management/

An overwhelming number of survey participants responded that their organisations were able to detect cybersecurity breaches within days with about 60% attesting to having discovered the incidents on the same day.

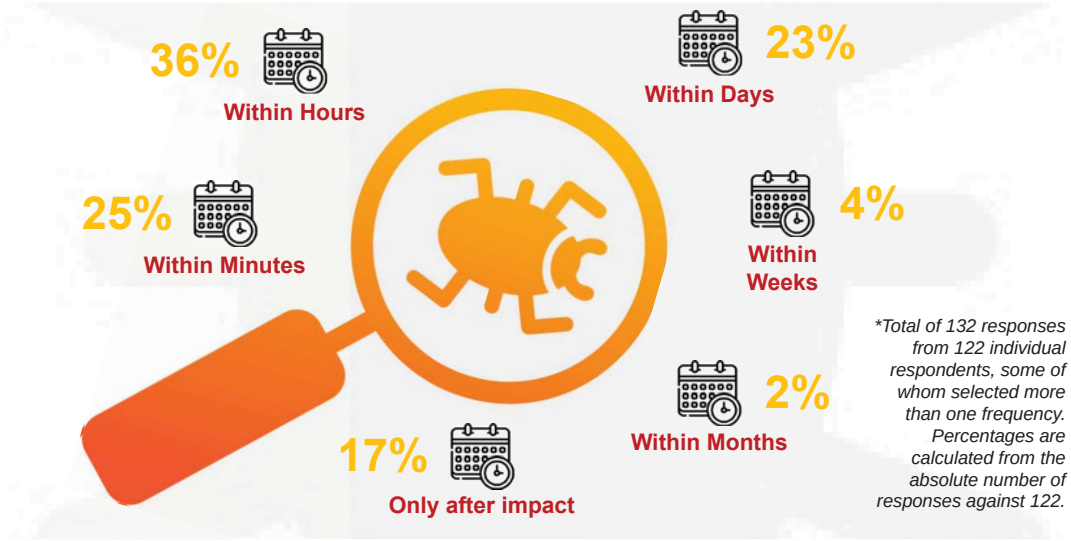
Such timeframes are substantially better that the mean number of 204 days to identify data breaches around the world, according to statista.com. The statistics platform stated that the time taken in 2023 is marginally lower than in previous years.

https://www.statista.com/statistics/1417455/worldwide-data-breaches-identify-and-contain/

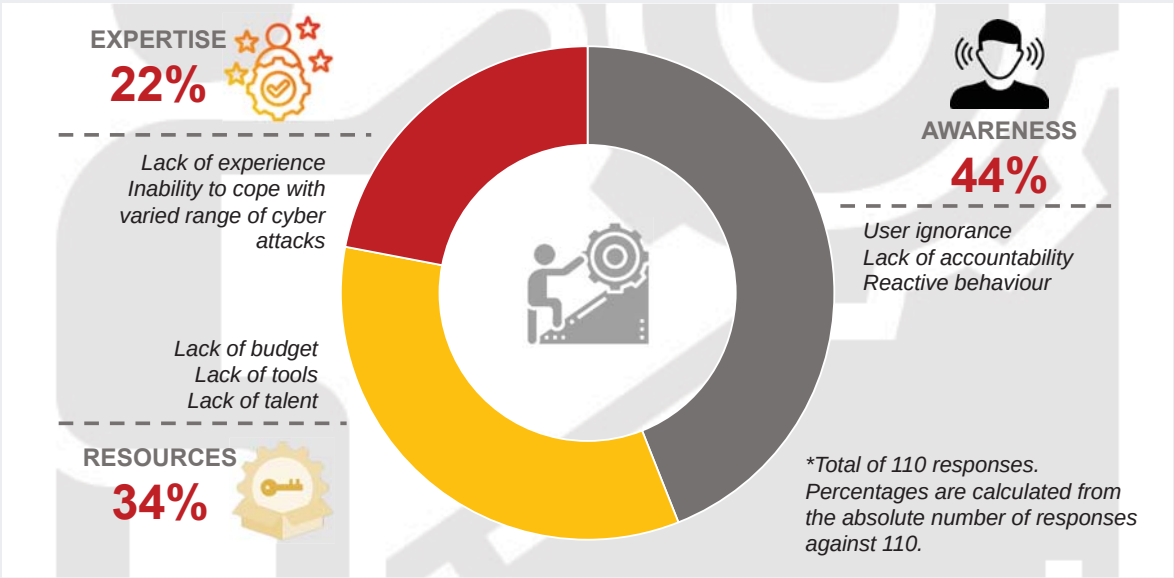
The IBM 2022 data security report had painted an even more dire situation, reporting an average of 277 days or about nine months for businesses to identify breaches and 327 days in the case of stolen or compromised credentials.

https://cyforsecure.co.uk/how-long-does-it-take-to-detect-a-cyber-attack/#

Q23: Time Taken for Breach Detection



Q24: Biggest Challenges in Cybersecurity

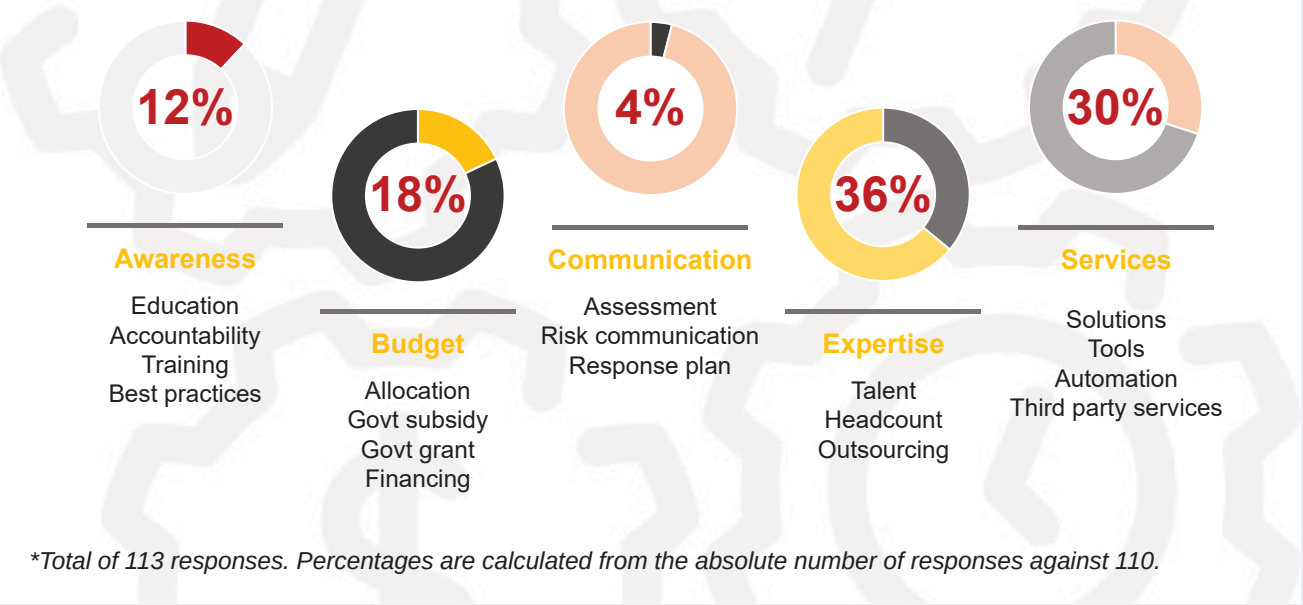


Survey respondents identified awareness, resources and expertise as the major cybersecurity challenges faced by their organisations. In the case of awareness, Malaysian employees continue to display ignorance and a lack of accountability.

Resources and expertise are among the main challenges cited by Tech Target. The American data marketing specialist pointed to slashed budgets, skills gap and staffing issues, and cybersecurity weaknesses in the supply chain as among the main cybersecurity concerns in 2024.

https://www.techtarget.com/searchsecurity/tip/Cybersecurity-challenges-and-how-to-address-them

Q25: Resources Required to Improve Cybersecurity



**Total of 113 responses. Percentages are calculated from the absolute number of responses against 110.*

Two thirds of survey participants identified expertise in the form of capability as well as headcount and third party services including tools and solutions as the resources most needed to improve cybersecurity in their organisations.

Q26: Suggestions & Recommendations

CYBER ATTACKS

Comparative Analysis by Industry Sectors

This section provides a comparative analysis of cyber threats faced by 10 industry sectors including Agriculture, Construction, Education, Energy, Electronics, Financial Services (FSI), Healthcare, Manufacturing, Retail and Telecommunications as well as an overlapping Critical Infrastructure category covering government, banking, transportation, healthcare and energy.

The analysis dives into the common threats, sector-specific threats and the tech sophistication of each sector. The threats are categorised according to the following:

- Phishing Attacks;
- Ransomware;
- Data Breaches;
- Insider Threats;
- Advanced Persistent Threats (APTs);
- Payment Card Fraud;
- Supply Chain Attacks;
- Distributed Denial of Service (DDoS) Attacks;
- Credential Stuffing; and
- Regulatory Compliance Challenges.

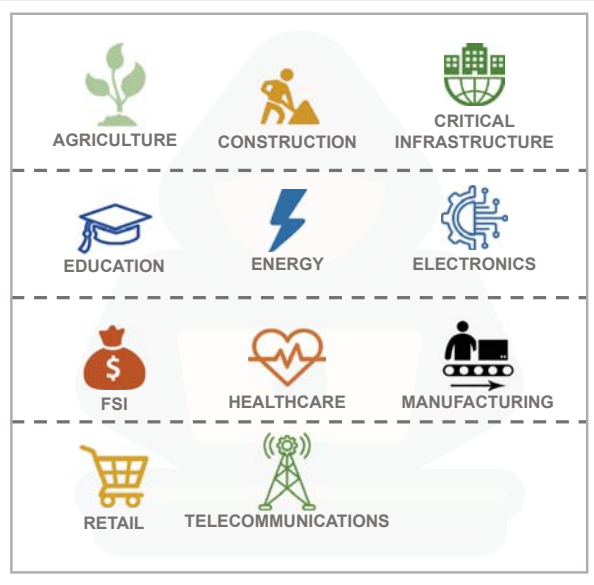
The data and information in this section were sourced via desktop research to support and supplement the findings from our cybersecurity survey. This not only ensures a balance of perspectives, but also offers greater insights and clarity into the many issues revolving around cyber threats and cybersecurity.

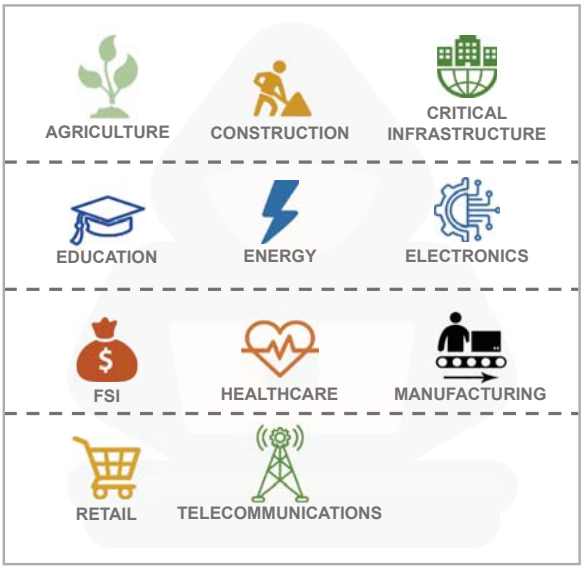
PHISHING

Commonality
Universal across all sectors, exploiting human error rather than technical vulnerabilities.

Sector-Centric Threats
Particularly severe on FSI, Healthcare and Retail, where sensitive personal data is frequently handled.

Tech Sophistication
Low to moderate. Defences require regular staff training and advanced email filtering.





RANSOMWARE

Commonality
A significant threat across all sectors, especially where operational continuity is critical (Healthcare, FSI, Manufacturing).

Sector-Centric Threats
Healthcare and FSI are often targeted due to the critical nature of their services and data.

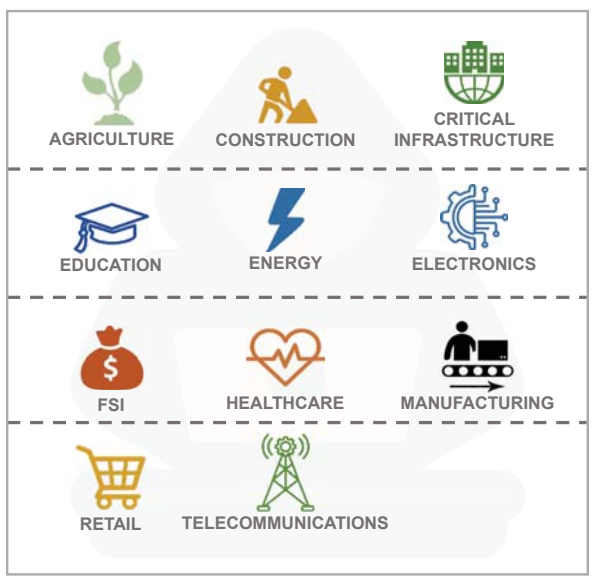
Tech Sophistication
Low to moderate. Defences require regular staff training and advanced email filtering.

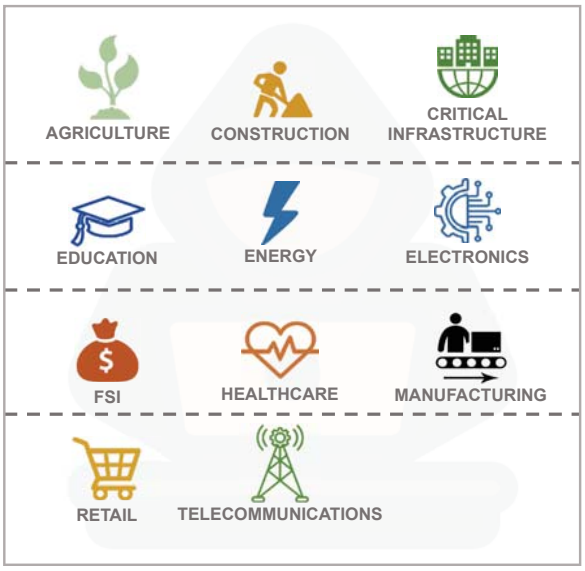
DATA BREACHES

Commonality
A risk for all sectors, with varying impact depending on the sensitivity of the data held.

Sector-Centric Threats
FSI and Healthcare have the most to lose due to the highly sensitive nature of the data.

Tech Sophistication
High, both for attackers and defenders. Requires comprehensive security measures including encryption and access control.





INSIDER THREATS

Commonality
Relevant to all sectors, but varies based on access controls and sensitivity of internal data.

Sector-Centric Threats
Particularly concerning in sectors with high-value IP (Manufacturing, Electronics) and sensitive data (FSI, Healthcare).

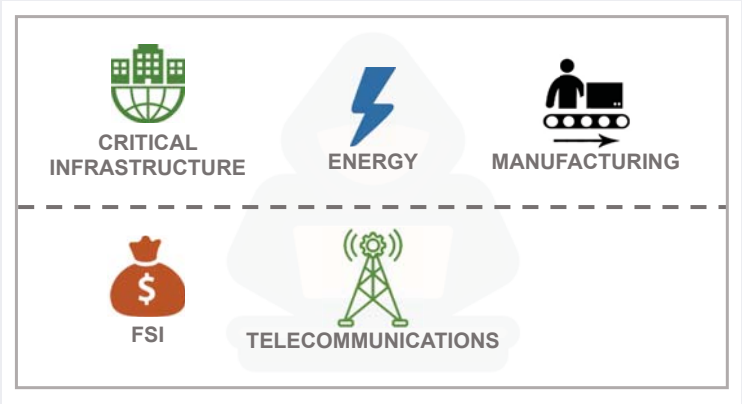
Tech Sophistication
Low to high. Prevention strategies include employee monitoring and strict access controls.

APT (Advanced Persistent Threats)

Commonality
A concern for sectors that are strategically important or have high-value assets (FSI, Telcos, Government and Defence-related Manufacturing).

Sector-Centric Threats
FSI and Telcos are prime targets due to the infrastructure and data they control.

Tech Sophistication
Very high. Defences involve sophisticated threat detection and response strategies.



PAYMENT CARD FRAUD

Commonality
Primarily affects Retail, FSI and any sector that processes payment transactions.

Sector-Centric Threats
Retail and FSI bear the brunt due to direct handling of payment transactions.

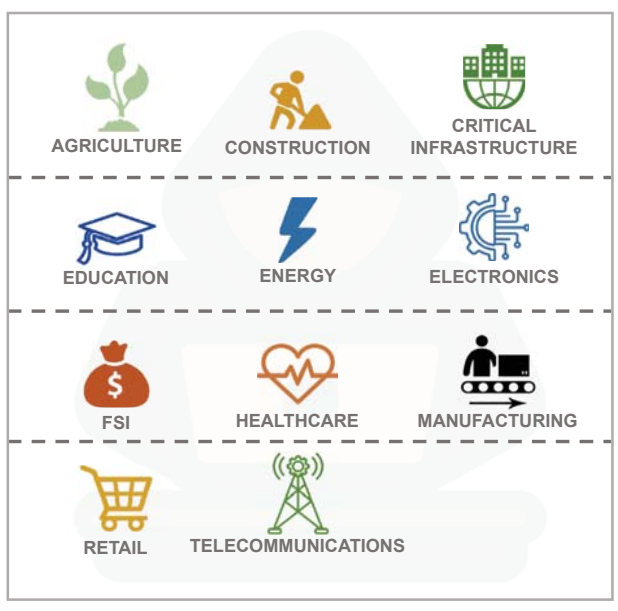
Tech Sophistication
Moderate. Requires secure payment processing systems and fraud detection mechanisms.

SUPPLY CHAIN ATTACKS

Commonality
A risk for all sectors, especially those dependent on complex supply chains (Manufacturing, Electronics, Construction).

Sector-Centric Threats
Manufacturing and Electronics are particularly vulnerable due to their reliance on global supply chains.

Tech Sophistication
High. Protection requires securing all nodes of the supply chain and conducting regular audits.



DDOS ATTACKS
Distributed Denial of Service

Commonality
Threatens sectors reliant on online operations (FSI, Retail, Telcos).

Sector-Centric Threats
Telcos and FSI are highly targeted with intention to disrupt services or as a smokescreen for other attacks.

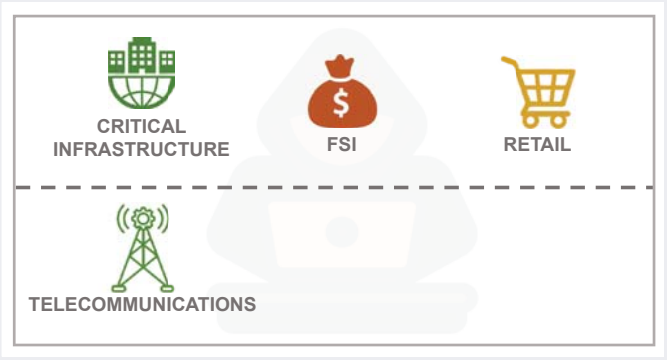
Tech Sophistication
Moderate to high. Defences include anti-DDoS solutions and traffic management strategies.

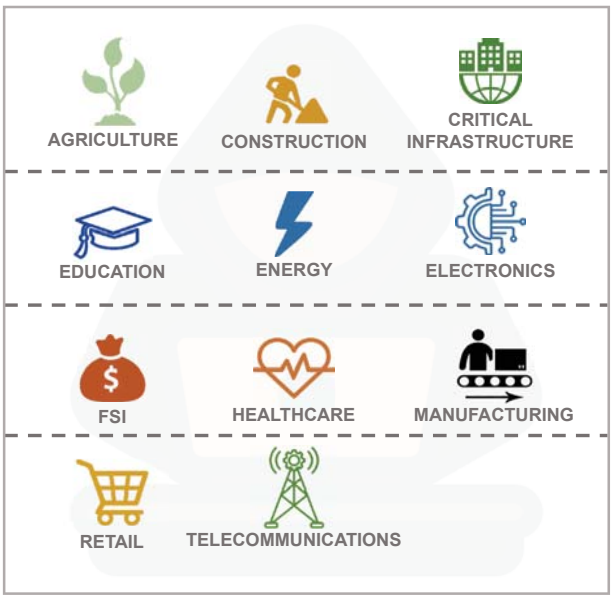
CREDENTIAL STUFFING

Commonality
A concern for any sector with online customer accounts (FSI, Retail, Education).

Sector-Centric Threats
Retail and FSI, where customer accounts are prevalent and often linked to financial information.

Tech Sophistication
Low to moderate. Requires multi-factor authentication and monitoring of access patterns.





REGULATORY COMPLIANCE CHALLENGES

Commonality
Impacts all sectors, with the degree varying by the specific regulatory environment.

Sector-Centric Threats
FSI and Healthcare are heavily regulated due to the sensitivity and importance of the data they handle.

Tech Sophistication
High. Compliance requires a comprehensive understanding of relevant regulations and the implementation of complex controls.

Overview of cybersecurity measures and recommended measures by Sector

Financial services
Financial institutions continually invest in cybersecurity measures, including threat intelligence, employee training, network security and incident response capabilities, to mitigate cyber threats and safeguard their operations, customers and reputation.

Education
Educational institutions must prioritise cybersecurity measures such as implementing robust network security protocols, conducting regular security awareness training, performing system audits and vulnerability assessments, and establishing incident response plans to mitigate the risks posed by these cyber threats.

Healthcare
Healthcare organisations should prioritise the same cybersecurity measures as the education sector. In addition, collaboration with industry stakeholders, government agencies and cybersecurity experts is essential to enhance the resilience of the healthcare sector against evolving cyber threats.

Telcommunications
Telcos must implement robust cybersecurity strategies, including network segmentation, access controls, encryption, intrusion detection systems, security monitoring, incident response planning and employee training, Similar to the healthcare sector, collaboration with the same parties is essential to enhance the resilience and security posture of the telco sector.

Manufacturing
To address cyber threats, manufacturing companies should prioritise cybersecurity measures such as implementing network security protocols, conducting regular cybersecurity assessments and audits, educating employees about cybersecurity best practices, and investing in threat detection and incident response capabilities. Collaboration with all stakeholders is also imperative.

Retail
Among the measures retail businesses should take include encryption of sensitive data, implementation of multi-factor authentication for employee and customer accounts, regular security assessments and penetration testing, employee training on cybersecurity best practices and adherence to regulatory compliance standards such as the Personal Data Protection Act (PDPA). Collaboration is also highly recommended.

Energy
Beyond implementing many of the measures already outlined for the other industry sectors, energy players should strictly adhere to regulatory requirements and standards such as those set forth by the Malaysian Communications and Multimedia Commission (MCMC) to ensure the security and reliability of energy infrastructure in Malaysia.

Critical Infrastructure
Critical infrastructure organisations should implement robust cybersecurity measures such as network segmentation, intrusion detection systems, employee training on cybersecurity best practices, regular security assessments and penetration testing, incident response plans, and collaboration with government agencies, industry partners and cybersecurity experts to enhance resilience against cyber attacks. Similar to the energy sector, compliance with relevant regulatory requirements and standards is essential.

Agriculture
Agricultural businesses should adopt best practices such as regular software updates, employee training on cybersecurity awareness, secure data storage and transmission practices and collaboration with cybersecurity experts or industry organisations.

Construction
Over and above many of the measures highlighted for various other sectors, it is vital to foster a cybersecurity culture and promote information sharing about cyber threats within the construction sector to improve resilience against cyber attacks.

Electronics
The electronics sector in Malaysia faces a diverse array of cybersecurity threats that demand a high level of technical sophistication to mitigate. Given its pivotal role in the global supply chain and the high value of its intellectual property, the sector is a prime target for a variety of cybercriminal activities. Combating these threats effectively requires a multifaceted approach that combines advanced technological solutions, rigorous employee training and strict regulatory compliance measures.

Summary of Findings

High-Risk Sectors (FSI, Healthcare, Critical Infrastructure, Energy)
These sectors face the greatest diversity and sophistication of threats due to the sensitive nature of their data and the criticality of their services. They require the highest levels of security investment and regulatory compliance.

Intermediate-Risk Sectors (Telcos, Manufacturing, Retail, Electronics)
These sectors face significant risks, especially from APTs, supply chain attacks and DDoS attacks, due to their infrastructure, economic value and customer base.

Lower-Risk Sectors (Education, Agriculture, Construction)
While not immune, these sectors may not be targeted as frequently or require slightly less sophisticated defences due to the nature of their data and services. However, they still face risks from phishing, insider threats and compliance challenges.

Each sector needs a tailored cybersecurity strategy that addresses its unique vulnerabilities and compliance requirements, with a common foundation in employee training, data protection and incident response preparedness.

RECOMMENDATIONS

Cybersecurity has surged to the forefront of companies' concerns as they increasingly embrace digital platforms. This transition exposes them to heightened risks of cyber attacks spanning various industries and company sizes.

As businesses expand digitally and integrate more connected devices and Internet of Things (IoT) technologies, cybercriminals find a broader scope for exploitation. Whether driven by financial gain or sheer mischief, hackers employ a wide array of tactics, including ransomware, phishing, social engineering and disruptions in supply chains.

The aftermath of a cyberattack can be profound, encompassing not only financial losses but also reputational damage and legal repercussions. Hence, it is essential for enterprises to continually adapt to evolving threats and adhere to cybersecurity best practices to protect their operations and flourish in the digital landscape..

Based on the Interviews across various industries, a number of recommendations to prevent and mitigate cyber attacks were suggested.

The following are a snapshot of ideas and suggestions offered by them:

Cybersecurity strategy and policy framework

A robust cybersecurity policy and framework are essential for any organisation. This framework should encompass data governance, IT standardisation and regular strategic discussions on cybersecurity.

The policy and framework serve as the cornerstone on which all other cybersecurity measures are constructed. In addition, a comprehensive cybersecurity policy and framework establish the foundation for effective incident response and management. This framework is critical for setting a baseline for security measures and protocols, guiding the organisation in its cybersecurity endeavours and compliance with regulations.

However, mere compliance is not sufficient to address cybersecurity threats. It serves as the minimum requirement, prompting ongoing efforts to not only meet, but also surpass these standards to strengthen security postures against evolving threats.

Identifying and addressing vulnerabilities

A swift response to breach incidents is imperative, emphasising the necessity for robust protocols to tackle both internal and external vulnerabilities. The varied nature of these threats underscores the importance of adopting a proactive and comprehensive security approach.

Beyond compliance

Meeting standards such as ISO 27001 serves as a foundational step. However, organisations must foster a culture of vigilance and preparedness that goes beyond basic regulatory compliance to effectively protect against cyber threats.

Incident response and management post-breach

A well-defined incident response strategy is crucial. This involves implementing internal communication protocols, involving stakeholders and managing legal complexities while also maintaining a stance of continuous adaptation to emerging threats.

Technological defences and infrastructure

Implementing robust security measures such as access controls, audit trails and network segmentation is vital, particularly in the context of IoT and other emerging technologies, to uphold a strong defensive posture.

Collaborative defence

Cybersecurity extends beyond the IT or security department, constituting a shared responsibility. across the entire organisation. Collaborative efforts across different departments ensure a unified and comprehensive approach to addressing cybersecurity challenges. This collaboration cultivates a security-focused culture that strengthens the organisation's resilience against cyber threats through collective vigilance and shared responsibility.

User engagement and responsibility

Fostering a security-conscious culture within an organisation entails engaging end-users in cybersecurity initiatives and emphasising their responsibility in data asset ownership. Cybersecurity solutions should prioritise user-friendliness to enhance usability and mitigate the risk of human error.

Navigating change

Changes in company ownership can introduce vulnerabilities, particularly regarding software licence renewal and support for existing security solutions.

Learning from incidents

The insights obtained from past breach incidents are invaluable for refining and strengthening cybersecurity practices. These lessons inform the development of best practices, highlighting the significance of vigilance, simulation exercises for preparedness, and clear and effective communication within the organisation to enhance incident response capabilities.

Technological evolution and strategy

The rapid evolution of technology, including the widespread adoption of IoT devices and the integration of AI capabilities, introduces new challenges and vulnerabilities. This technological progress requires adaptive and forward-thinking strategies, such as network segmentation and advanced threat detection methodologies, to mitigate sophisticated threats. It emphasises the importance of a dynamic cybersecurity strategy that evolves alongside technological advancements.

Resource allocation

Implementing effective monitoring and response strategies can be resource intensive. Financial constraints may hinder an organisation's ability to deploy sufficient monitoring tools and response mechanisms, thereby affecting its capability to detect and respond to threats promptly. Strategic resource allocation is crucial for striking a balance between operational efficiency and cybersecurity imperatives.

EXTRACT

Emerging Cyber Security Trends Shaping Malaysia's 2024 Outlook

Contributed by

In Malaysia, the digital landscape is rapidly changing due to evolving technology trends, offering both opportunities and challenges. The shift towards a cashless society, coupled with advancements in Artificial Intelligence (AI), quantum computing, and cloud computing, as well as regulatory updates, is driving innovation and economic growth.

The rising number of cyberattacks is a clear indication of the increasing cyber threat landscape associated with these technological trends. It is crucial for organizations to recognize and understand the challenges that come with these advancements. By doing so, organizations can develop comprehensive strategies to effectively manage and mitigate potential risks while embracing and leveraging the opportunities that these emerging technologies offer.

Unveiling the Future with Emerging Technologies

Rising Tide of AI and ML in Malaysian Cybersecurity

ESET's latest research unveils a notable trend among Malaysian organisations: a significant investment in advanced machine learning to bolster their cybersecurity defenses. In addition to that, the Malaysian government has established Malaysia Artificial Intelligence (AI) Roadmap (2021-2025) describes how Malaysia's AI capabilities will be harnessed, catalysed and propelled within the next 5 years, from 2021 until 2025.

ESET. (2023). Enhance cybersecurity with advanced machine learning

An evident use of AI in Malaysia is the adoption of ChatGPT, with businesses increasingly leveraging its capabilities for innovative applications. According to a recent EY survey, 62% of consumers trust AI-generated responses for their queries, highlighting a growing acceptance of AI-driven solutions such as chatbots or automated responses. Additionally, there is burgeoning potential for GenAI, which combines AI capabilities with customer data and human insights to enhance personalization and foster engagement through next-generation hybrid distribution models.
EY (2023) Reframing Asset Management Report

Embracing the Rise of Quantum Computing

With the escalating threat landscape, organisations are increasingly turning to quantum computing to enhance encryption methods and fortify cybersecurity defenses. Quantum-resistant cryptography and quantum key distribution are poised to revolutionize data protection, safeguarding sensitive information from sophisticated cyber threats.

According to recent data from the Malaysian government, it is recognised that quantum computing will bring a significant impact on cybersecurity landscape in 2023.

MCMC (2023) 2023 Cybersecurity Trends

As Malaysia embraces the rise of quantum computing, it signals a strategic shift towards cutting-edge technology adoption and innovation-driven growth. By harnessing the potential of quantum computing backed by robust data, Malaysia aims to unlock new opportunities across various sectors, including finance, healthcare, and telecommunications.

Unveiling the Cloud Revolution

Malaysia's business landscape is witnessing a profound revolution driven by the widespread integration of cloud computing technology. The government's greenlight for new data center construction in February 2021, aligned with Malaysia's cloud-first strategy and the Malaysia Digital Economy Blueprint, marks a pivotal moment in the nation's journey toward digital eminence. This strategic move underscores the government's commitment to fostering innovation and accelerating economic growth by leveraging advanced digital infrastructure.

Major industry players like Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and Telekom Malaysia are seizing the opportunity, investing in cutting-edge data center infrastructure within Malaysian borders. This influx of investment not only reinforces Malaysia's position as a regional leader in cloud computing but also opens doors for businesses to harness state-of-the-art technology to streamline operations and fuel expansion.

Notably, Bank Negara Malaysia's updates to the RMiT Guideline have introduced additional cloud-related requirements, reinforcing the importance of cloud security and compliance in the financial sector. This alignment underscores the pivotal role of cloud computing in reshaping business dynamics and driving Malaysia's digital transformation journey forward.

Navigating the Regulatory Landscape

Some 63% of Malaysian CEOs identify regulatory changes as the leading factor in potential industry disruption.

The Edge Malaysia (2023). Malaysian CEOs see regulation changes as top concern

While regulatory change may impose limitations on the flexibility of technology companies to experiment, develop new solutions, a significant portion of respondents believe that regulations can simultaneously enhance security, foster innovation, and promote competitiveness.

Malaysian government has notably intensified its focus on cybersecurity over the recent years, aiming to bolster the country's resilience against cyber threats. As cyber data breaches continue to rise, the Malaysian government is prioritizing on strengthening of data protection and cybersecurity measures. This commitment is underscored by the upcoming rollout of an updated Personal Data Protection Act (PDPA) in 2024 with five major changes:

1. Mandatory appointment of a Data Protection Office (DPO)
2. Making Personally Identifiably Information (PII) Portable
3. Mandatory Data Breach Notification
4. Extension of the Security Principle to Data Processors
5. Cross-Border Data Transfers and the "Black-list"

As the increasing trends on the adoption of cloud in Malaysia's organization, Bank Negara has issued an updated Risk Management in Technology (RMiT) policy document in June 2023 to provide additional guidance in Appendix 10 to strengthen financial institution's cloud risk management capabilities and it embodies a shift to a risk-based approach in cloud consultation and notification process.

Risk Management in Technology (RMiT) Policy Document Appendix 10, pg52 –pg67

The key advantage from this update is the potential for standardization in the cloud consultation and notification process. By establishing clear guidelines and procedures, it promotes consistency and uniformity across financial institutions, facilitating smoother compliance efforts and reducing administrative burdens.

The guidance provided in Appendix 10 serves to elevate the overall maturity of cloud risk management practices within financial institutions. By offering insights, frameworks and best practices, the policy equips organisations with the tools and knowledge necessary to navigate the complexities of cloud adoption securely and confidently.

What are the challenges?

As Malaysia embraces digital transformation, evolving technology trends reshape the digital landscape, offering both opportunities and challenges. The surge in a cashless society, alongside advancements in artificial intelligence, quantum computing, and cloud computing, as well as regulatory updates, fuels innovation and economic growth. However, these advancements also pose cybersecurity challenges and is your organization ready to address it?

Is your organization prepared and aware of actions in case of a breach?

As cybersecurity evolves, organisations face increasingly complex challenges in incident response readiness. With the emergence of new technologies, organisations require more robust mechanisms to address potential breaches effectively.

This includes combating fraudulent activities in digital transactions, defending against AI-specific attacks, and developing rapid response strategies to counter quantum-enabled cyber threats.

The updated PDPA 2024 introduces mandatory data breach notifications to authorities, encompassing compromised, hacked, or unauthorized sharing of private data.

In light ofthese changes, organisations must expand their incident response drills and simulations to encompass newly emerging technology trends. This proactive approach ensures readiness to address potential breaches promptly and effectively, safeguarding data security and privacy in the digital landscape.

Has your organization met all the requirement in the updated rules & regulations?

Ensuring compliance with updated regulations, such as the revised PDPA and RMiTguidelines, is imperative in today's regulatory landscape. These changes demand thorough examination and proactive measures to meet the new standards effectively.

Conducting a comprehensive assessment of current compliance status is essential to pinpoint any shortcomings or areas of non-compliance with the revised regulations. Organisations must then develop and execute action plans to rectify identified gaps or deficiencies, ensuring alignment with updated requirements.

Maintaining compliance is a continuous effort with ongoing monitoring and refinement. Organisations must establish mechanisms for regular oversight and improvement, ensuring sustained adherence to regulatory mandates and mitigating associated risks.

Are privacy matters and data security being considered and addressed?

The shift towards cashless societies raises significant concerns surrounding data breaches and identity theft. As digital transactions surge, the vulnerability of sensitive financial information and personal data to unauthorized access escalates.

Similarly, the adoption of AI systems necessitates access to vast datasets for training and operation, intensifying worries about potential unauthorized access and misuse of sensitive information. The immense computational capabilities of quantum computers pose a threat to the security of encrypted data, potentially rendering current encryption algorithms ineffective.

Additionally, the growing dependence on cloud services introduces fresh security challenges concerning data protection and privacy. Organisations face risks such as unauthorized access to cloud-stored data, concerns about data sovereignty, and the looming threat of data breaches.

The evolving landscape of privacy and data security extends beyond conventional controls. This expansion reflects the growing complexity of cybersecurity threats and the need for organisations to adopt a holistic approach to safeguarding sensitive information.

Is your organization prepared for the use of AI and ML?

With legacy systems existing in some organization, a seamless integration of emerging cybersecurity trends may be a challenge. For example, the integration AI systems with existing cybersecurity infrastructure while maintaining security and interoperability presents significant challenges as current controls may not be ready to address the security controls.

Organization may need to allocate resources to assess legacy systems to ensure compatibility with emerging cybersecurity trends. This may involve investing in software updates, hardware upgrades, or adopting interoperability solutions to bridge the gap between legacy and modern systems.

Does your organization have the right skillset and people?

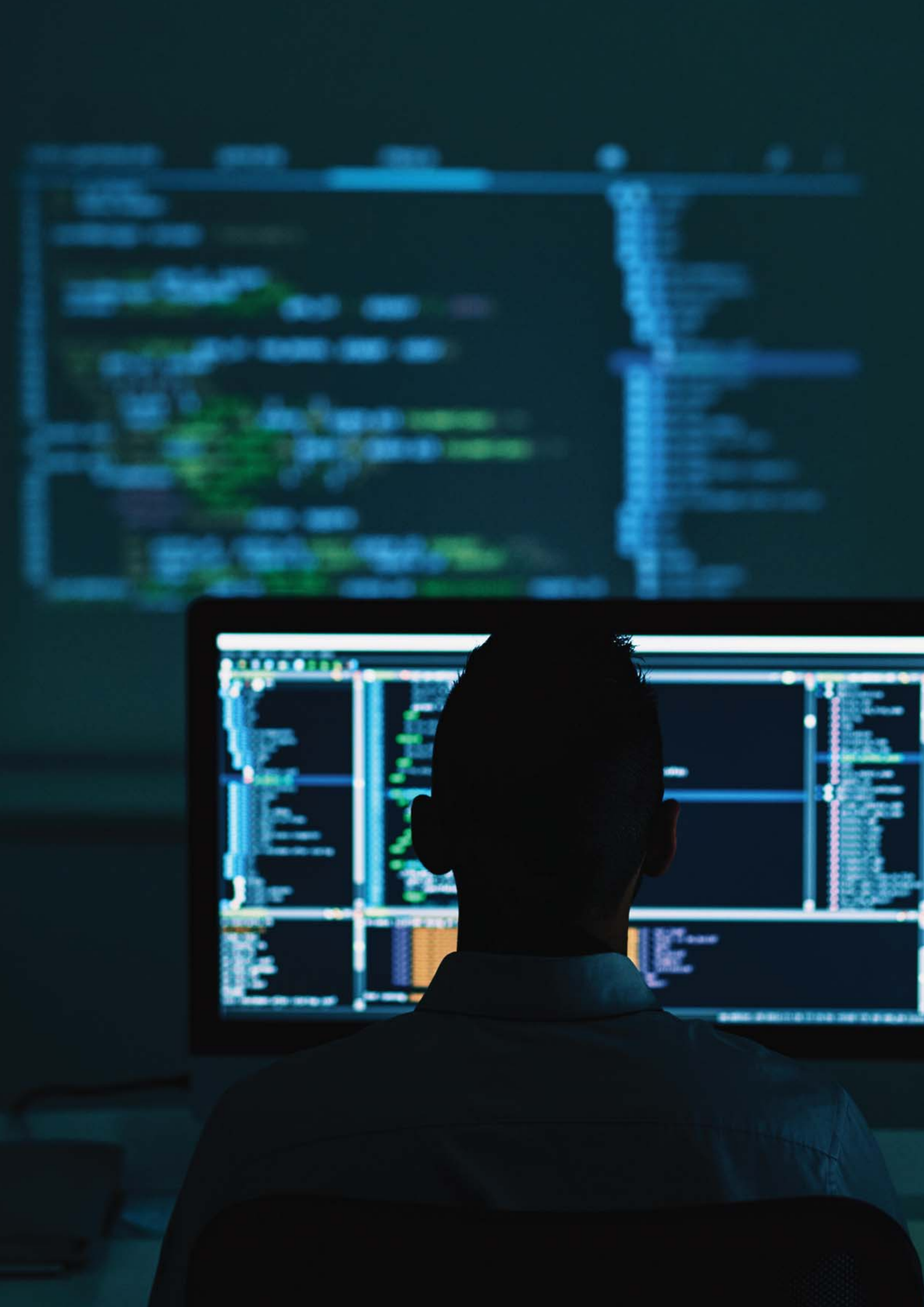
In tandem with these technological shifts and changes in regulatory requirements, having the right skill personnel persist across various cybersecurity trends, requiring organisations to address knowledge and expertise gaps effectively.

Allocation of sufficient budget to provide ongoing training and professional development opportunities for cybersecurity professionals can help bridge the skills gap.

Importantly, fostering a culture of cybersecurity awareness among employees through regular training sessions and awareness campaigns can empower individuals to recognise and mitigate cybersecurity risks proactively.

Comstor

If it’s connected, you’re protected.




CYBERSECURITY BILL 2024

Malaysia's Cyber Security Bill 2024 is poised to become law following its successful passage through both houses of Parliament: Dewan Rakyat on 27 March and Dewan Negara on 3 April. Once royal assent is given, the Bill will become the Cyber Security Act 2024.

The bill is designed to apply extra-territorially, affecting individuals irrespective of nationality or citizenship, and also extends to both Federal and State Governments. The National Cyber Security Committee, chaired by the Prime Minister, will play a pivotal role in advising the Government, overseeing implementation and issuing directives to ensure compliance with the bill.

In protecting critical national information infrastructure (CNII), the bill outlines specific requirements for entities operating within CNII sectors. These sectors encompass various vital domains such as government, banking, transportation, healthcare, energy and more. Each CNII sector is assigned a sector lead responsible for designating CNII entities and formulating Codes of Practice to ensure cyber security within their respective sectors.

CNII entities are obligated to adhere to the prescribed measures, conduct cyber security risk assessments, and report incidents to the Chief Executive and their sector leads. Additionally, the bill mandates licensing for cyber security service providers.

In essence, the bill entails the introduction of roles such as the Chief Executive and CNII Sector Leads to focus on industry-specific cyber security governance. The bill signifies Malaysia's commitment to protecting its critical information infrastructure amidst rising cyber threats.

PIKOM's Perspective

The points below represent PIKOM's take on the Bill:

- The bill impacts both individuals and businesses by mandating compliance with cybersecurity standards. It is noted that many cybersecurity incidents in Malaysia go unreported due to the lack of disclosure requirements, which the bill seeks to change.

- It will impact individuals and businesses, especially those within the CNII. However, what is not comprehensively covered is the criteria that would be used to determine which entities are considered CNII. According to the Bill, the chief executive has the power to appoint the CNII leads, who will then further define the CNII scope. The Bill repeatedly mentions that the chief executive would have immense power in this issue.

- The bill emphasises the roles of the security committee and chief executive. It mandates the management of cybersecurity threats and incidents. Businesses within CNII must prepare for and respond to cybersecurity incidents.

- There are concerns over the broad powers granted to the chief executive, including the ability to conduct enforcement actions without a warrant and the potential implications for privacy and legal rights. For example, action can be taken by any authorised police officer appointed by the chief executive irrespective of rank. This is not common as other laws specify that authorised officers must be of inspector rank and above.

- The bill is expected to create opportunities for cybersecurity service providers and stimulate sector growth due to increased demand for cybersecurity measures.

- The bill is anticipated to boost the cyber insurance market as businesses seek coverage for potential cybersecurity incidents.

- The bill introduces licensing requirements for individuals providing cybersecurity services, with further details to be prescribed by the minister. This raises questions about the scope of cybersecurity services and the impact on companies providing these services.

- Details to be prescribed by the Ministry on the types of cyber security services have yet to be revealed.
- Although the bill references the National Cyber Security Agency (NACSA), it does not define it, leading to questions about its role and the chief executive's appointment.
- The bill's impact on small businesses and their role in the supply chain for CNII sectors is unclear, necessitating further clarification.
- The bill is seen as an enhancement of the PDPA, aiming to protect personal data and hold entities accountable for cybersecurity breaches.
- Companies need to adhere to new regulations to strengthen their cybersecurity measures. As an example, in the case of healthcare, there is currently no clear framework on how patient data should be regulated.
- The bill is expected to impact on cybersecurity education and training due to heightened compliance standards.
- The bill's operation in the context of cyber warfare is not explicitly defined, leaving its applicability in such situations open to interpretation.
- The bill has extra-territorial application, meaning it applies to offenses committed outside Malaysia that affect Malaysian entities. This is crucial in dealing with cybercrimes originating from abroad.
- The bill applies to foreign entities operating in Malaysia, ensuring that they comply with the same cybersecurity standards as local entities. This includes Malaysian entities operating overseas, highlighting the bill's broad scope.
- There are potential contradictions between the Bill and existing legislation like the PDPA and the Communications and Multimedia Act. The bill's broad scope may overlap with these existing laws, raising questions about enforcement and compliance.
- The Bill does not explicitly state that the chief executive would be immune from prosecution, suggesting that they could be held accountable under certain circumstances.
- Directors may face personal liability for company offenses under the Bill, emphasising the need for cybersecurity risk assessments and audits.

REFERENCES

Surfshark: *https://www.thestar.com.my/tech/tech-news/2023/12/06/cybersecurity-report-ranks-malaysia-as-eighth-most-breached-country-in-q3-2023*

Kaspersky: *https://www.nst.com.my/news/nation/2023/07/935644/kaspersky-malaysia-ranks-second-southeast-asia-mobile-malware-attacks*

Cloudflare: *https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/*

Cybersecurity Malaysia: *https://www.thestar.com.my/tech/tech-news/2023/10/25/cybersecurity-malaysia-report-government-sectors-suffered-most-data-breaches-while-telcos-spilled-over-400gb-of-data-in-h1-2023*

PT Security: *https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/*

Upguard: *https://www.upguard.com/blog/common-data-leak-causes*

Lepide: *https://www.lepide.com/blog/six-common-causes-of-data-breaches/*

IBM: *https://cybersecurityasean.com/news-press-releases/record-high-data-breach-costs asean-malaysia-businesses-face-305m-impact*

Cloudflare: *https://www.thestar.com.my/tech/tech-news/2024/01/08/new-year-familiar-threats-cybersecurity-experts-warn-of-the-threats-to-come-for-2024*

NSRC: *https://themalaysianreserve.com/2023/07/26/alarming-rise-in-online-attacks-malaysias-cyber-security-landscape-in-2023/*

MetaCompliance: *https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-data-breach*

Cisco: *https://techwireasia.com/03/2023/cisco-most-organisations-in-malaysia-are-not-ready-to-defend-against-cyber-threats*

https://www.nst.com.my/news/nation/2023/10/969613/malaysia-short-12000-experts-tackle-cyber-attacks-fahmi

Verizon: *https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020#*

IBM / FRSecure: *https://frsecure.com/blog/incident-response-statistics-how-do-you-compare/*

https://www.thestar.com.my/tech/tech-news/2024/01/08/new-year-familiar-threats-cybersecurity-experts-warn-of-the-threats-to-come-for-2024.

Coursera: *https://www.coursera.org/articles/cybersecurity-best-practices*

Avasant: *https://avasant.com/report/it-security-staffing-ratios-2024/#*

IANS & Artico: *https://venturebeat.com/security/benchmarking-your-cybersecurity-budget-in-2023/*

Palo Alto Network: *https://techwireasia.com/09/2023/businesses-in-malaysia-increase-cybersecurity-budget-allocation-in-2023/*

ISACA: *https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training#*

RSI Security: *https://blog.rsisecurity.com/how-often-should-you-perform-patch-management/*

Statista: *https://www.statista.com/statistics/1417455/worldwide-data-breaches-identify-and-contain/*

IBM: *https://cyforsecure.co.uk/how-long-does-it-take-to-detect-a-cyber-attack/#*

Tech Target: *https://www.techtarget.com/searchsecurity/tip/Cybersecurity-challenges-and-how-to-address-them*

http://www.mcmc.gov.my

CYBERSECURITY 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