KROLL

State of Incident Response:

Asia Pacific

October 2022

Contents

Executive Summary
Turning Pressure into Preparation

Global business has witnessed an unprecedented scale of cyberattacks in the past year, making it increasingly difficult for security teams to react.

A record number of vulnerabilities were brought to light in 2021, many of which threat actors continue to actively exploit in 2022. Ransomware continues to feature in our *Quarterly Threat Landscape Reports*; we also saw a number of supply chain vulnerabilities arise, such as Log4J. As businesses attempt to manage and mitigate cyber risk, security professionals are being pushed to their limits.

Kroll's Cyber Risk team investigates more than 3,200 incidents every year and works with companies on managing their cyber risk. Whether teams are transitioning to a new cloud environment, monitoring day-to-day risks or detecting and responding to incidents, Kroll provides extensive support using our expert team to protect, detect and respond to cyber threats.

This whitepaper sets out how the Asia Pacific (APAC) market has been impacted by vulnerabilities, highlights incident patterns for the region and proposes actionable priorities for the future.

Our research finds that businesses in APAC are feeling the impact of cyberattacks, but many are yet to build out appropriate response plans or have regular access to relevant cyber expertise. Building this "muscle memory" in response to cyber risk can go a long way in reducing the impact of cyberattacks and enabling businesses to recover more quickly.

We urge businesses in APAC to tap into those with extensive experience of dealing with a cyber incident and take a strategic and pragmatic approach to planning response. After all, the worst time to plan for an incident is during one.

Paul Jackson
Regional Managing Director, Asia Pacific
Cyber Risk, Kroll

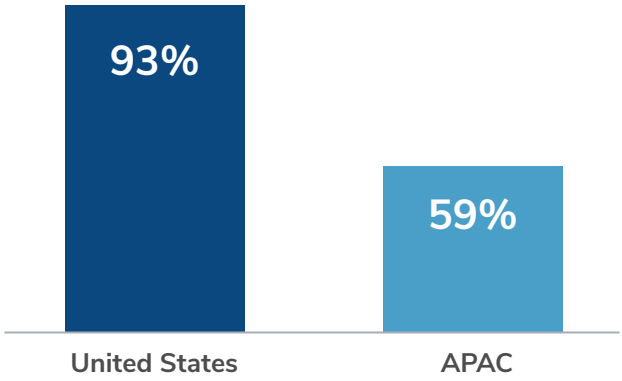
State of Play

Cyber Incidents are Numerous and Preparation is Lacking

Over half of all organizations interviewed in APAC (59%) have experienced a cyber incident, of which a third (32%) have suffered multiple incidents. This compares to 93% of organizations which had suffered a compromise of data in the U.S. during a 12-month period, according to a previous survey commissioned by Kroll.

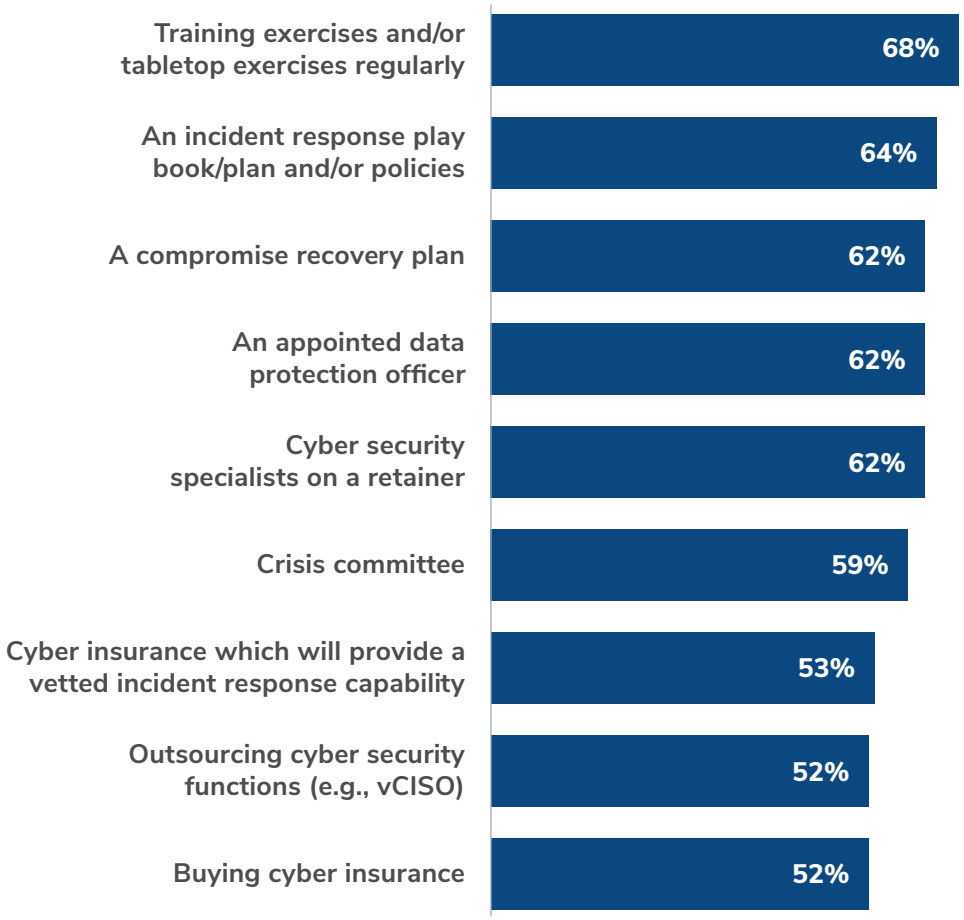
It is worth noting, however, that the regulatory landscape and data protection in APAC is generally less established than in developed markets such as the U.S. and thus this may understate the number of cyber incidents being reported.

Figure 1: Regional Breakdown of Businesses that Have Experienced a Cyber Incident



Despite the volume of cyber incidents, more than a third (36%) of organizations do not have a response plan if an incident were to occur, which leaves companies at the risk of being unable to handle an incident effectively and of being vulnerable to further attacks.

Figure 2: Measures Implemented to Respond to an Incident



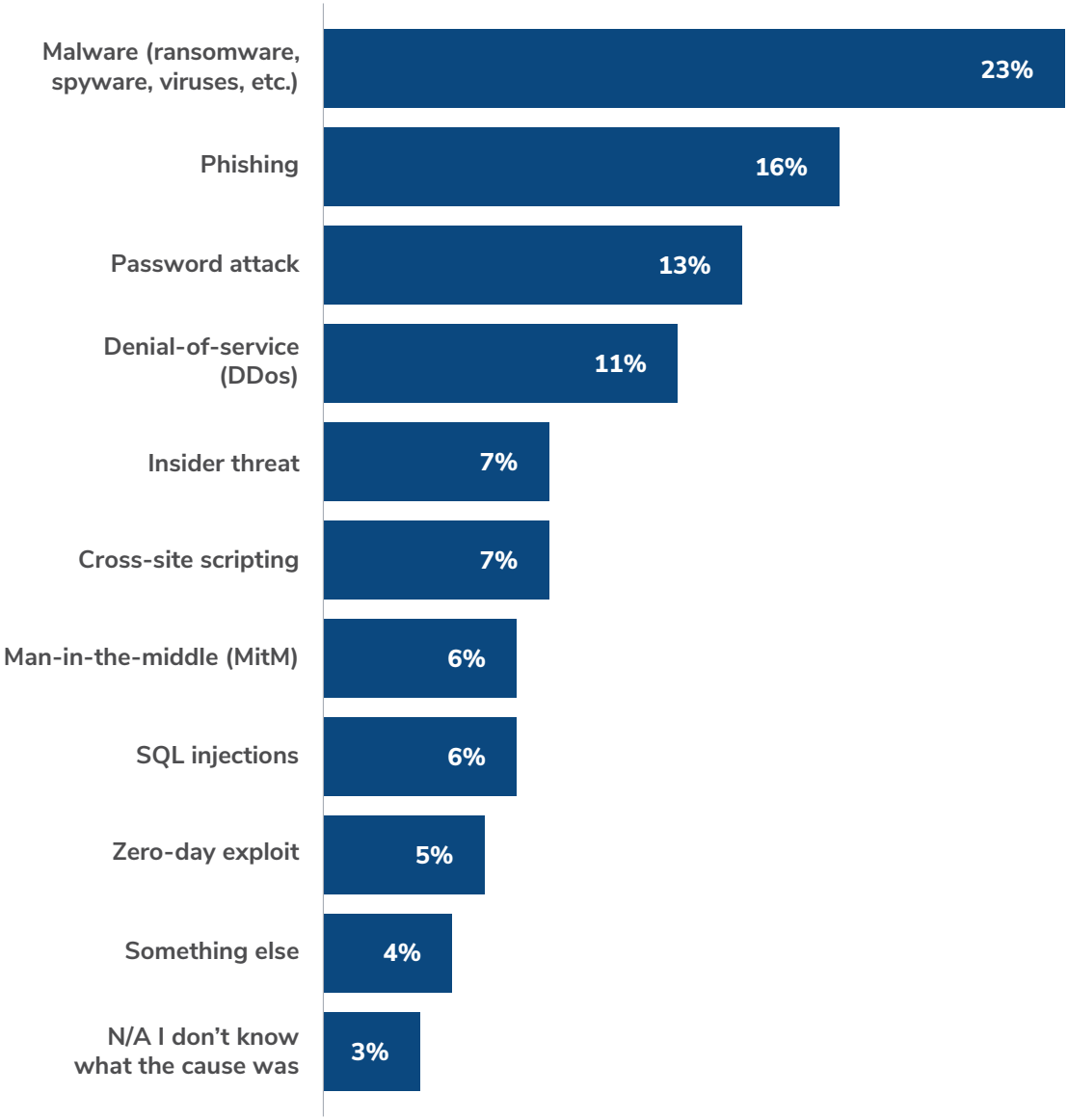
There is some measure of relevant representation of cyber expertise at senior levels across the companies surveyed, with 62% companies reported appointing a data protection officer and a similar percentage had cyber security specialists on a retainer. This, however, still leaves more than a third of companies in APAC (38%) without cyber security specialists to call in the event of an incident.

"The need for security expertise at senior levels within an organization is increasingly being recognized, with many chief information security officers (CISOs) now presenting cyber agenda directly to the board. Recently, the Securities and Exchange Commission (SEC) in the U.S. proposed mandatory cyber representation on boards subject to their regulation.

While the regulatory landscape in APAC may be less developed than the U.S., organizations would definitely benefit from having access to this expertise. Whether it is in-house, on retainer—for example, through a virtual chief information security officer (vCISO) program—or through third parties, having people who can assist management teams in navigating the requirements of an appropriate cyber risk posture can be invaluable to mitigate potential damage."

— **James McLeary**
Managing Director, Cyber Risk, Kroll

Figure 3: Cause of Reported Cyber Incidents



Common causes

The most cited cause of a cyber incident across APAC was malware, which includes ransomware, spyware, viruses, etc. The top three causes, which include phishing and password attacks, account for over half of all incidents reported.

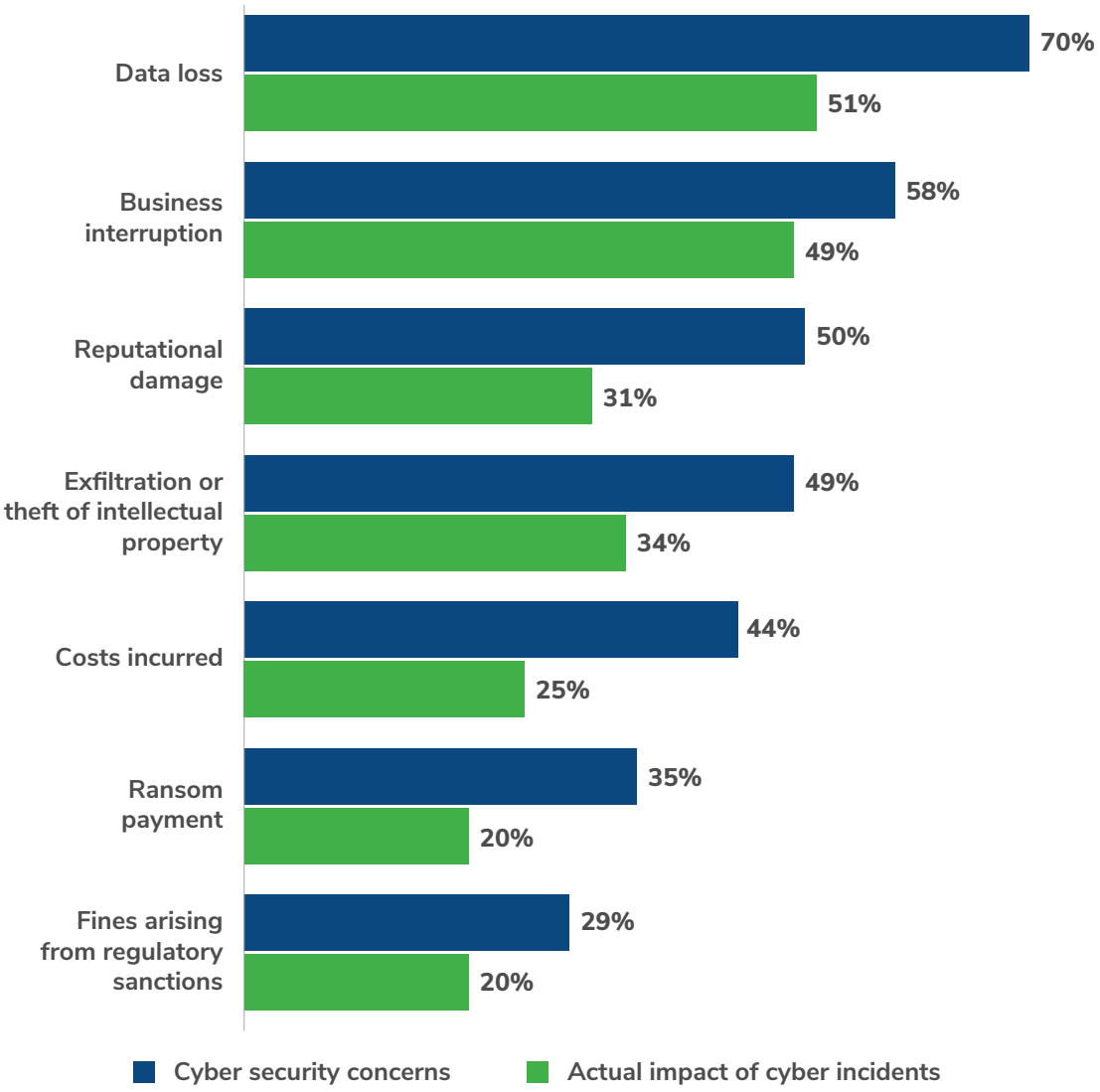
Focus is on Operational Impact: Data Loss and Business Interruption

Data loss (51%) and business interruption (49%) were the two most cited impacts of a cyber incident and, predictably, they are also the top cause of businesses' concern, with data loss being the primary worry (70%), followed by business interruption (58%).

Out of the types of impact reported from cyber incidents, these were arguably the most operational in nature. This could indicate a more tactical focus for now, rather than a strategic approach.

There are signs, however, that organizations are starting to understand the longer-term consequences of cyber incidents. Reputational damage, for example, is cited as a less common impact of an incident (31%), but half of the leaders who were surveyed (50%) are concerned about it.

Figure 4: Cyber Security Concerns are Aligned with the Impact of Actual Incidents

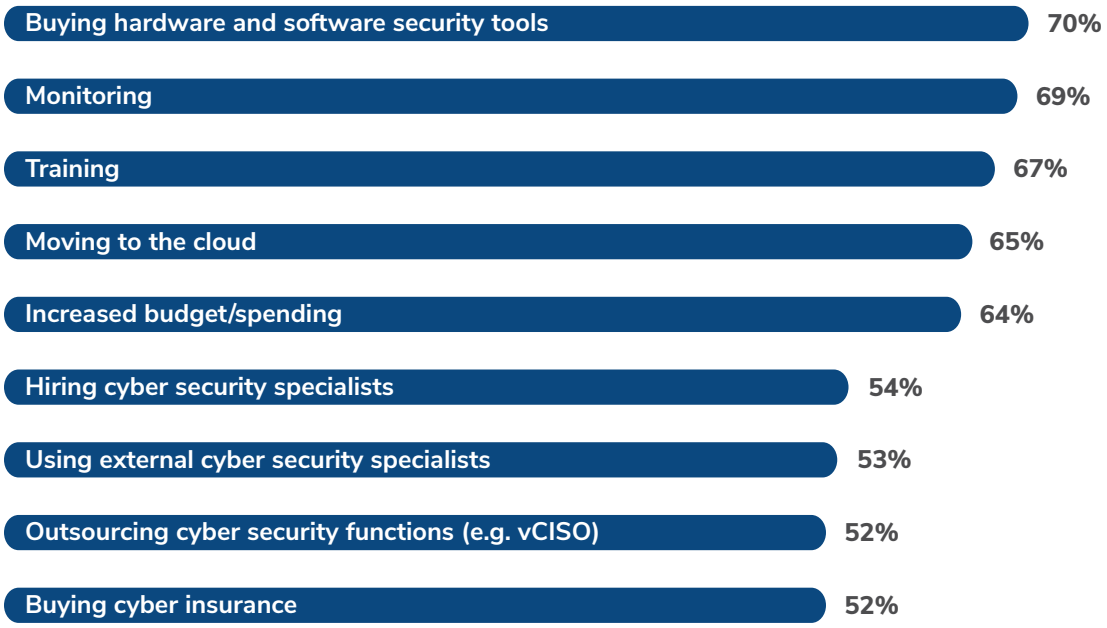


Cyber Security Efforts in APAC

To minimize the threat of a cyber incident, organizations are not only taking advantage of hardware and software security tools (70%) and monitoring the endpoints, network, systems and applications (69%) but also conducting regular training (67%) for the business to stay aware of potential threats.

In addition, nearly two-thirds (64%) of organizations interviewed are increasing their budgets or spending to address cyber security threats. Overall, more than half of the companies in this region are willing to invest resources to prevent operational disruption from cyber incidents.

Figure 5: Measures Implemented to Address Cyber Security Threats



Future Investment Priorities

Cyber security professionals in multinational organizations said that they expect to prioritize incident management in the coming two years, with a growth in investment priority increasing from 26% to 39%. By comparison, the largest growth area for Pan-Asian companies is mobile working policy, increasing from 20% two years ago to 34% in two years' time.

This survey was conducted in March and April 2022, during a period when many Asian countries were still experiencing strict COVID-19 measures. The difference in investment focus could perhaps indicate a broader trend where Pan-Asian companies are still recovering from the operational impact of the pandemic, such as a material shift to remote working. Conversely, multinational organizations were possibly more able to adapt to a new paradigm in working conditions—and the security requirements needed to support it—and thus could prioritize incident response management.

> **"We have seen a shift in attitude in recent years relating to incident response. More than ever before, organizations with a more developed perspective on cyber risk are preparing for when an attack might happen, rather than whether it might happen. This could be the reason for an increasing interest in incident response retainers and managed detection and response (MDR). There is a palpable benefit to having a qualified, experienced incident response team on retainer—and, therefore, on call. MDR adds another level of assurance by having experts monitor your entire fleet of computers and respond to any incident on a 24x7 basis. Pan-Asian companies may still be getting to grips with a distributed infrastructure brought about by working conditions imposed by the pandemic, but there is a clear appetite to be better prepared."**

— **Rob Phillips,**
Managing Director, Cyber Risk, Kroll

Figure 6: Incident Management as a Priority (Four-year Evolution)

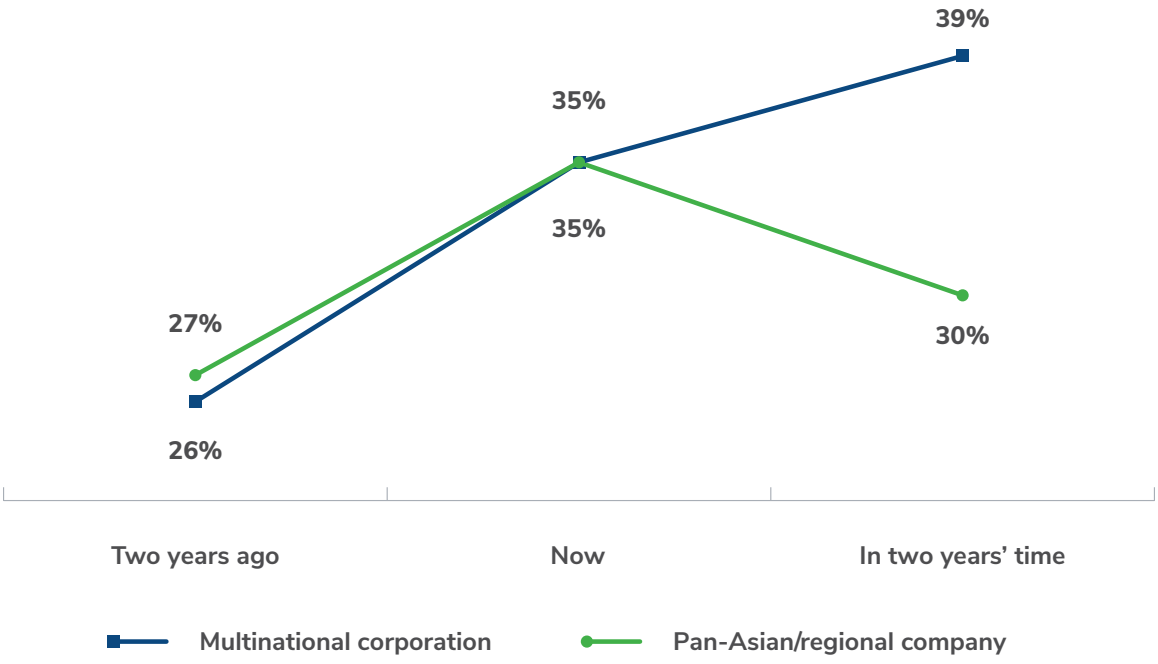
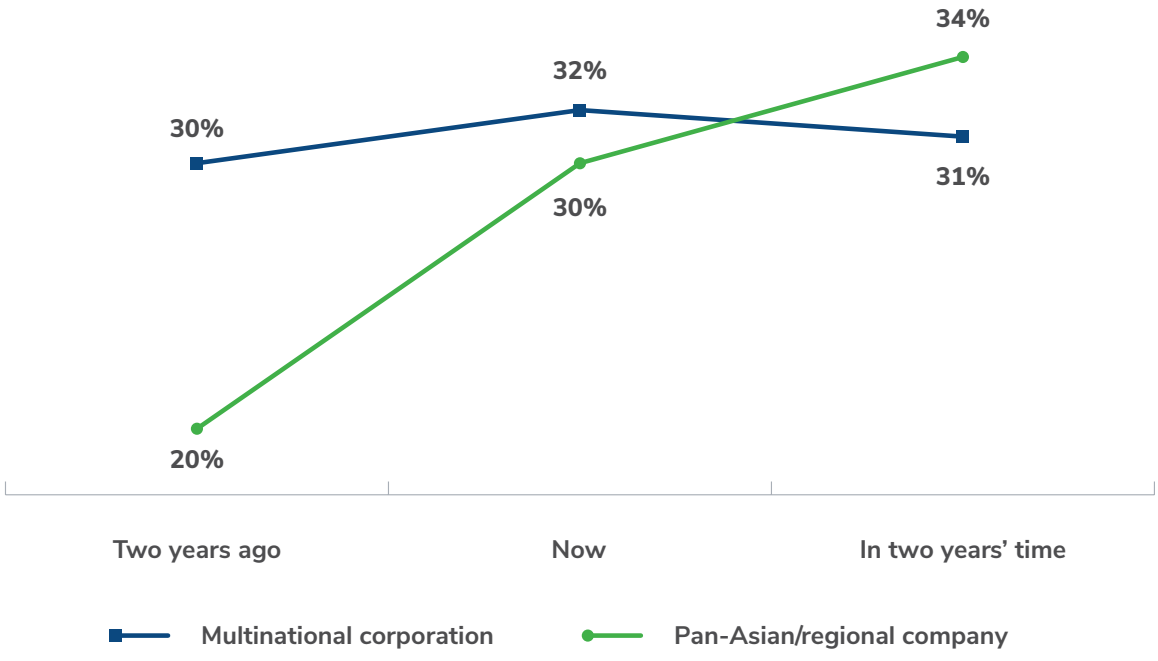


Figure 7: Mobile Working Policy (Four-year Evolution)



Cloud Conundrum

Companies around the world have been moving to the cloud for some time now. The ability to manage a more effective remote workforce thanks to the collaboration advantages, while reducing costs—for example, around storage—has become an attractive proposition for many. The proportion of those transitioning to a cloud environment is fairly consistent, two years ago (41%), compared to now (44%) and what is projected for two years' time (40%).

There are also security benefits of moving to the cloud, from access control to data visibility. It's worth noting, however, that although 65% of survey respondents had moved to the cloud to address cyber security threats, achieving security in the cloud is often not that simple. There have been numerous examples of default settings and misconfigured buckets causing security incidents. It is important to not rely on a cloud provider for security or assume the cloud environment is secure.

65%

of organizations moving to the cloud to address security threats

> **"Transitioning to a cloud environment does not come without complexity; many organizations require specialist skills to migrate to a cloud environment effectively and securely. Failing to do this can have quite the opposite effect, whereby gaps can be introduced due to a poor deployment. In an incident response scenario, a cloud environment can also become obfuscating as companies struggle to gain access to their cloud logs that could provide insight into how and what has been targeted in a cyber incident.**
>
> **To overcome this, organizations should look to experts to guide, test and assess their cloud environments for gaps in security controls. They should also have detailed incident response plans, which are regularly simulated, to build confidence that the cloud infrastructure enables response rather than hinders it."**

— **Sachin Kumar,**
Associate Managing Director

APAC Threat Landscape – By Market

Regional Threat Landscape

Across the board, countries and cities across APAC could be more resilient to cyberattacks if they had more robust incident response plans in place and had more readily available access to experts. This would help them address immediate cyber requirements, such as a breach incident, as well as consider cyber security for transitions over a longer-term basis, such as moving to a cloud-based infrastructure.

As we analyze each market, however, there are some similarities and differences that should be recognized.

- Australia was the least likely to have an incident response plan in place, and Hong Kong was the most likely.
- Malaysia and the Philippines suffered the most incidents, while Hong Kong suffered the least.
- Data loss was a concern across the board, but those in Indonesia were also more worried than others about the reputational damage of an incident. Singaporean businesses were primarily worried about business interruption.

Figure 8: A Summary of APAC Statistics

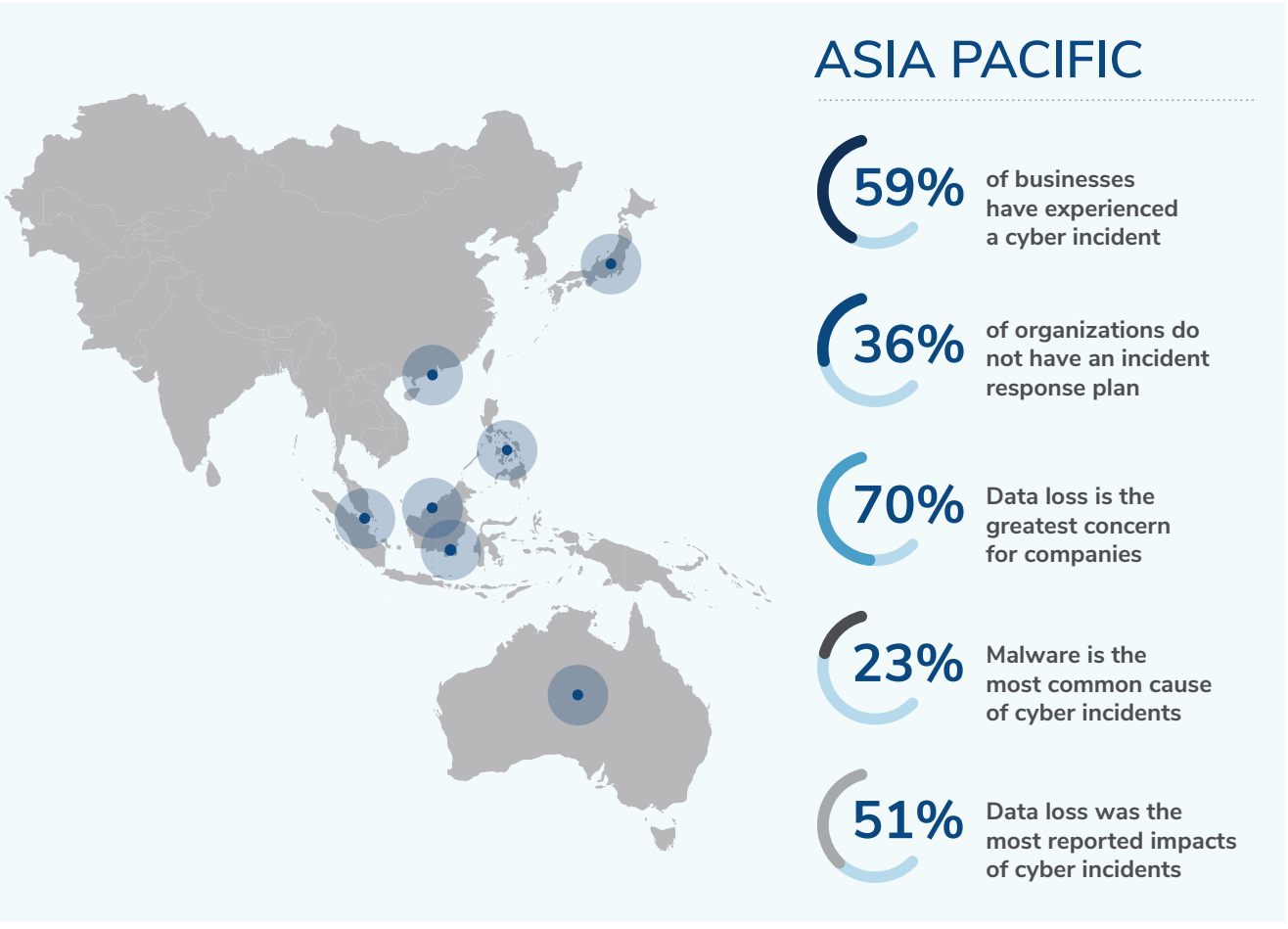


Figure 9: Causes of Cyber Incidents, By Market

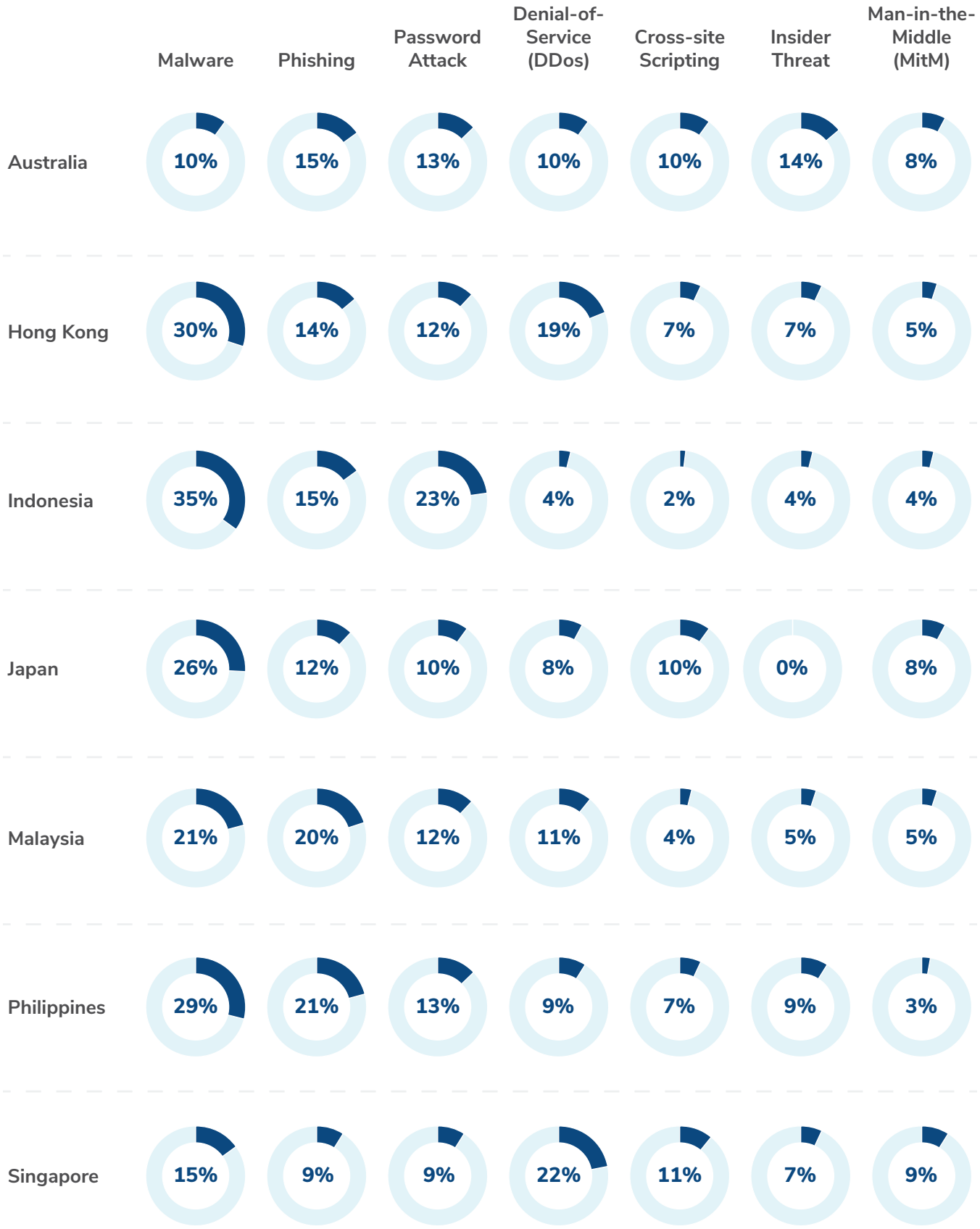
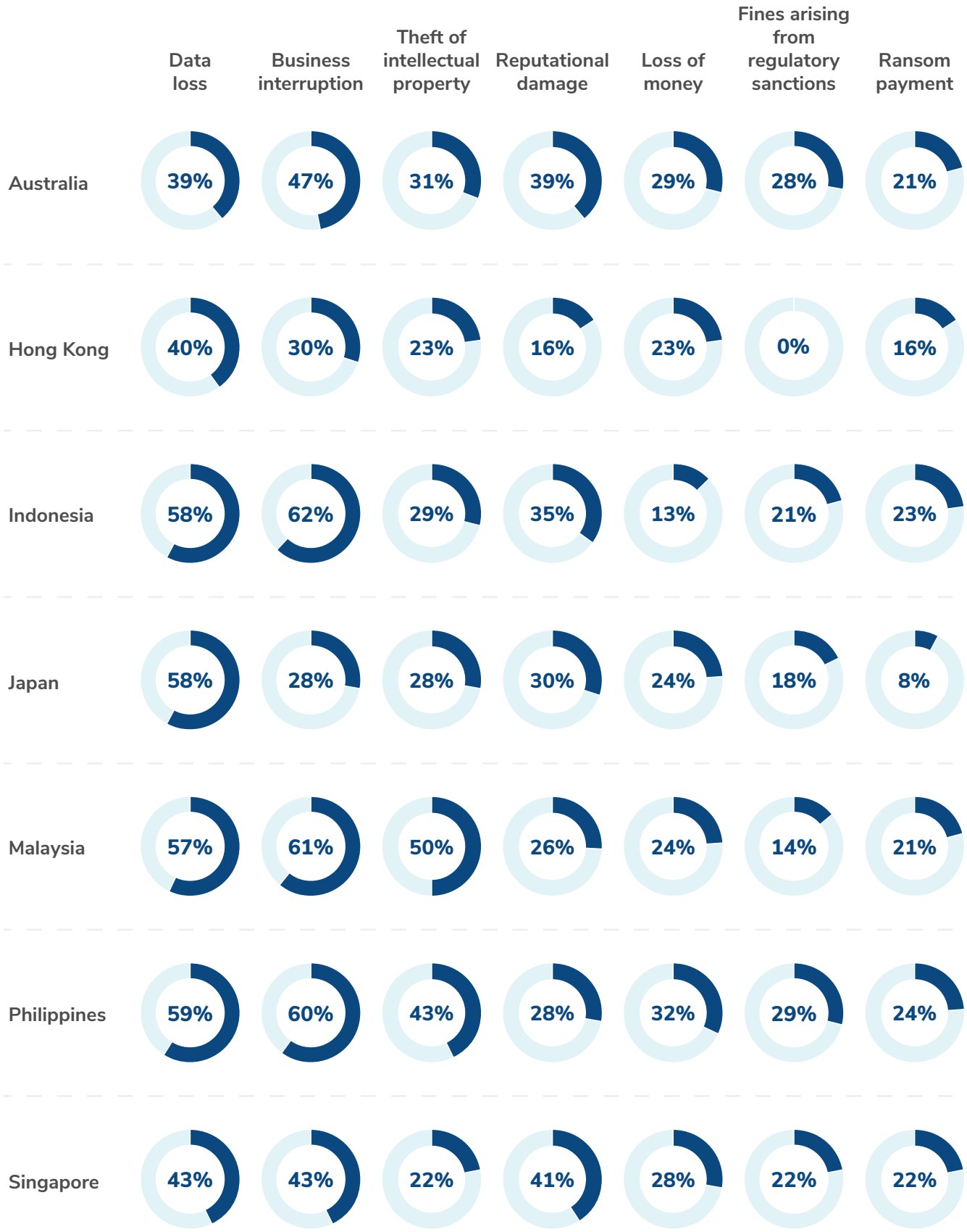


Figure 10: Impact of Cyber Incidents, By Market

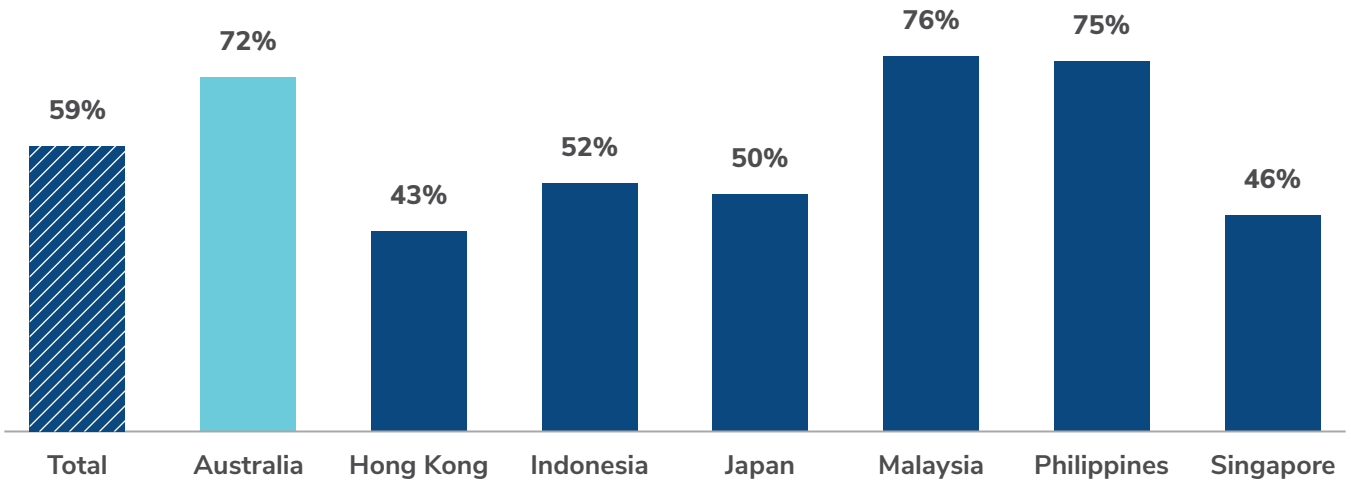


Australia

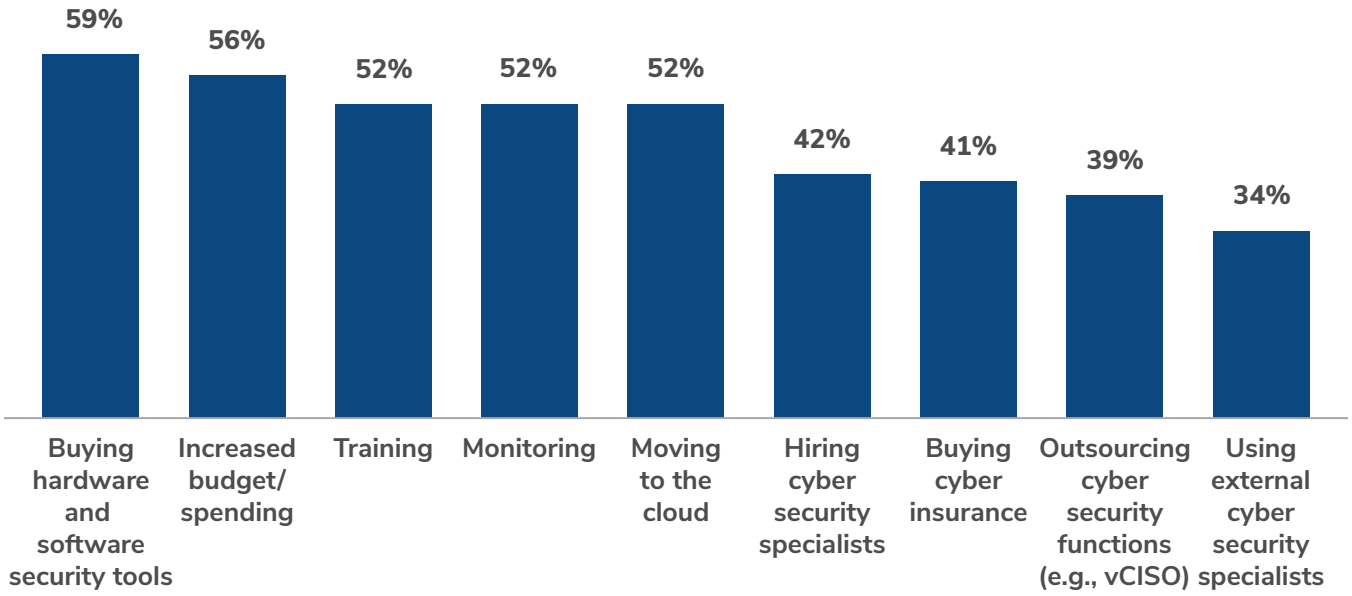
Across Australia, 72% of the businesses surveyed reported experiencing a cyber incident. This is much higher than the average in the APAC region (59%), and only surpassed by Malaysia and the Philippines.

Data loss is the greatest concern for Australian businesses (61%), despite it not causing the most impact. Business interruption was reported as having the greatest impact (47%), ahead of data loss and reputational damage at 39%.

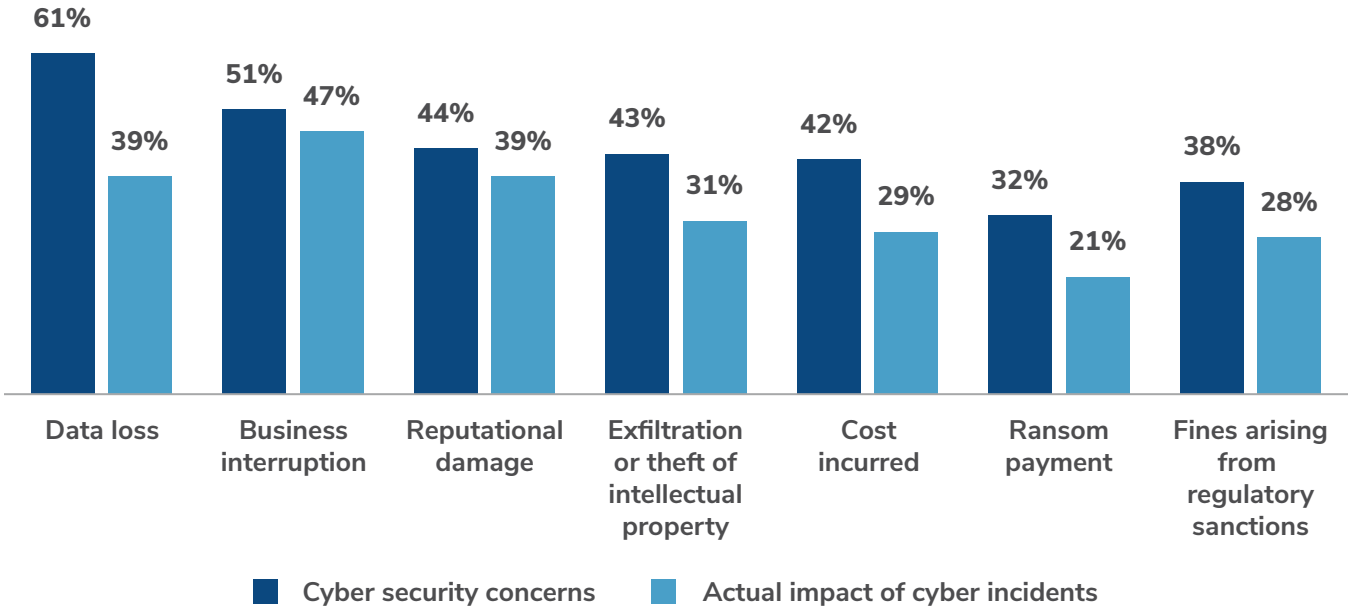
Proportion of Businesses that Have Experienced a Cyber Incident, by Market



Measures Implemented to Address Cyber Security Threats



Cyber Security Concerns and Impact of Actual Incidents

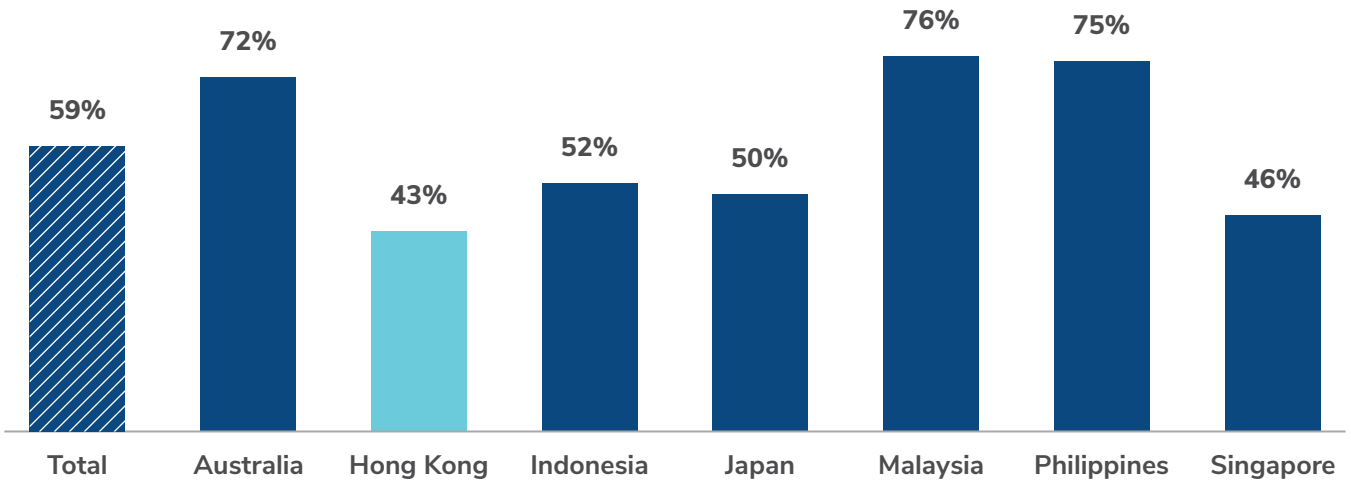


Hong Kong

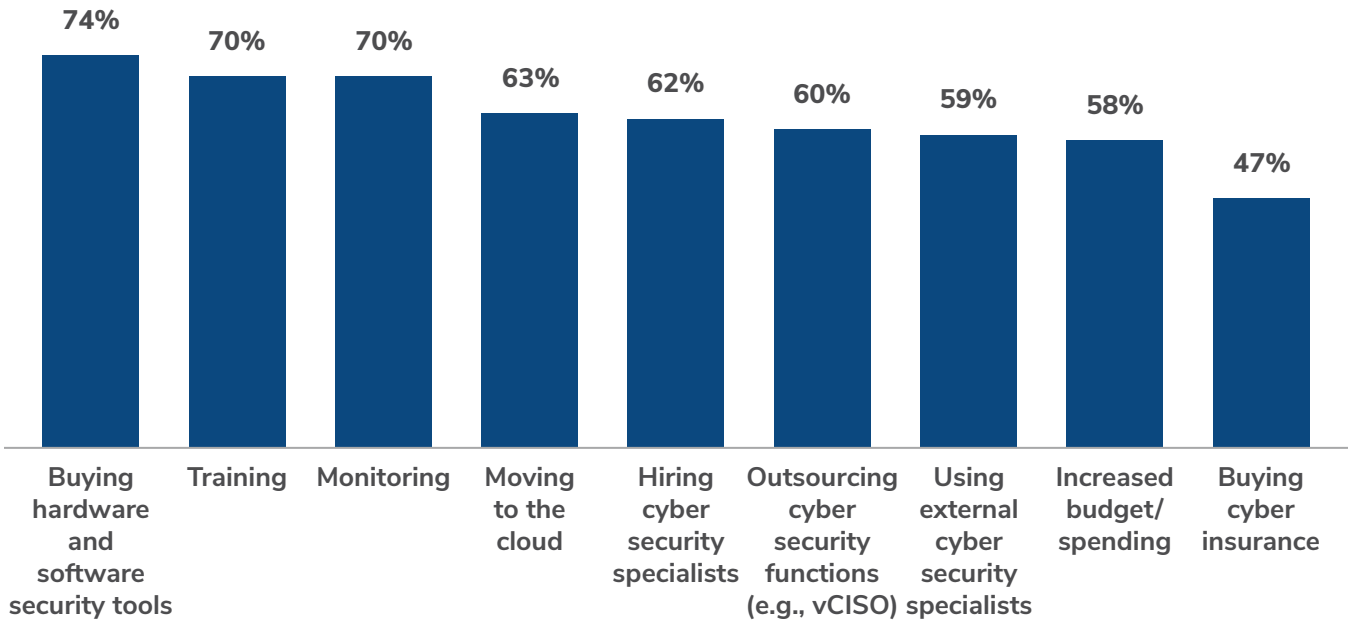
Hong Kong businesses reported experiencing the lowest number of cyber incidents in APAC, with 43% of organizations having been affected, compared to the average of 59%.

Organizations are most concerned about data loss (68%), which is well-founded, with 40% of the most recent cyberattacks reportedly causing data loss. Organizations were also concerned about business interruption (54%) and reputational damage (57%). It's also important to note that while 28% of organizations were concerned with regulatory fines or sanctions, zero respondents reported having suffered regulatory fines following a cyber incident. This is likely to change as Hong Kong's Privacy Commissioner for Personal Data (PCPD) steps up their enforcement of data protection laws.

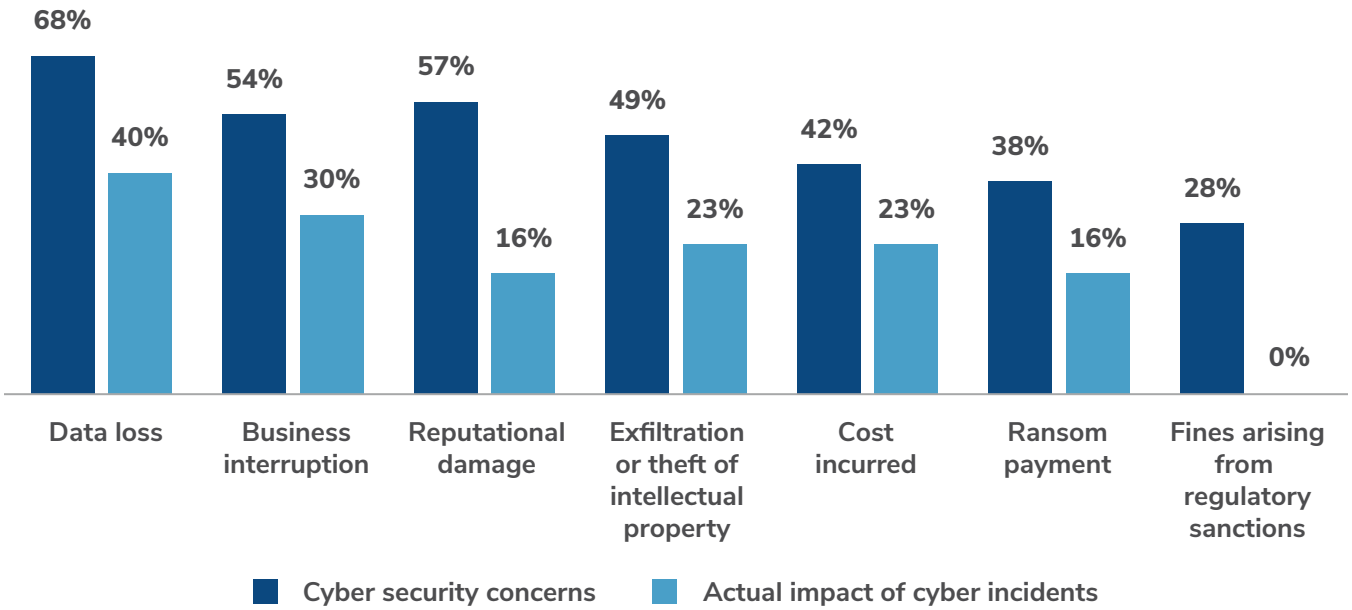
Proportion of Businesses that Have Experienced a Cyber Incident, by Market



Measures Implemented to Address Cyber Security Threats



Cyber Security Concerns and Impact of Actual Incidents



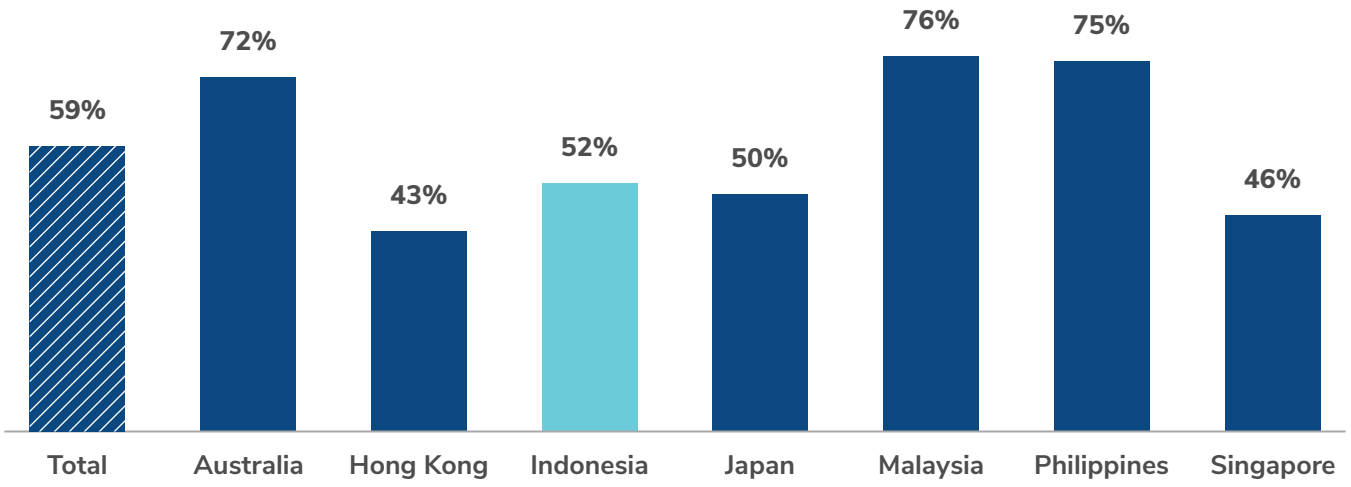
Indonesia

Just over half of Indonesian businesses reported experiencing a cyber incident (52%), which is under the APAC average of 59%.

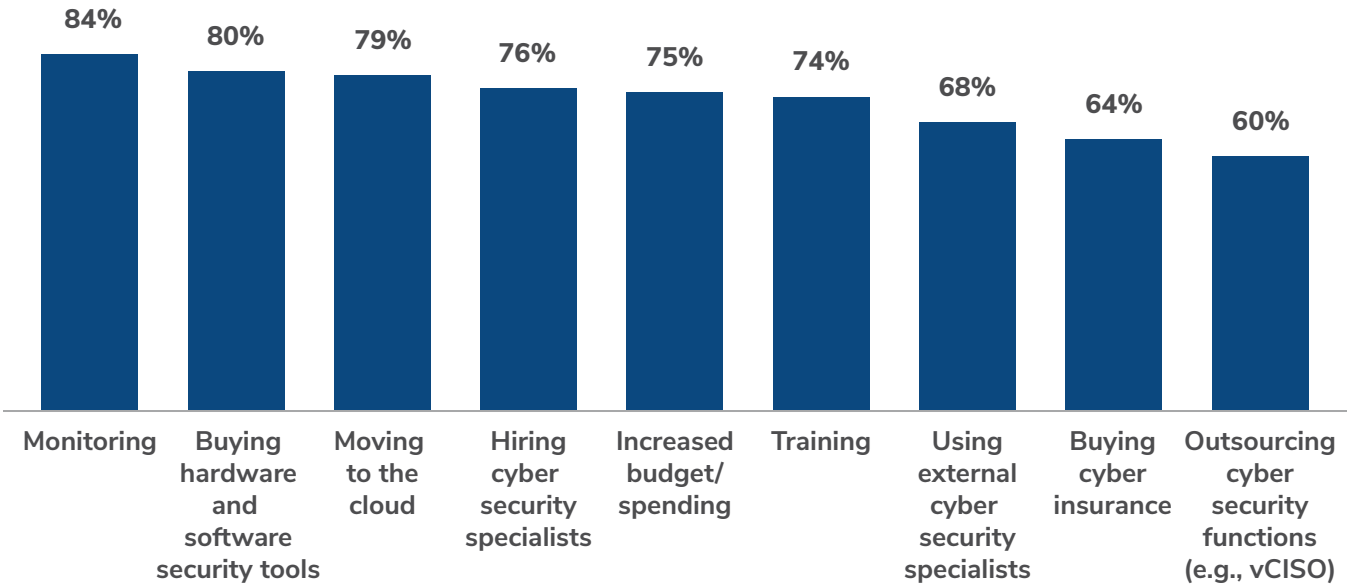
As represented across the APAC region, data loss in Indonesia is the primary concern (82%). This is followed by 70% of Indonesian organizations being concerned about reputational damage, the highest across APAC.

Although data loss is the greatest concern, the most significant reported impact was business interruption, cited by 62% of respondents. Indonesian businesses were the least likely to cite financial costs as an impact of cyberattacks (13%).

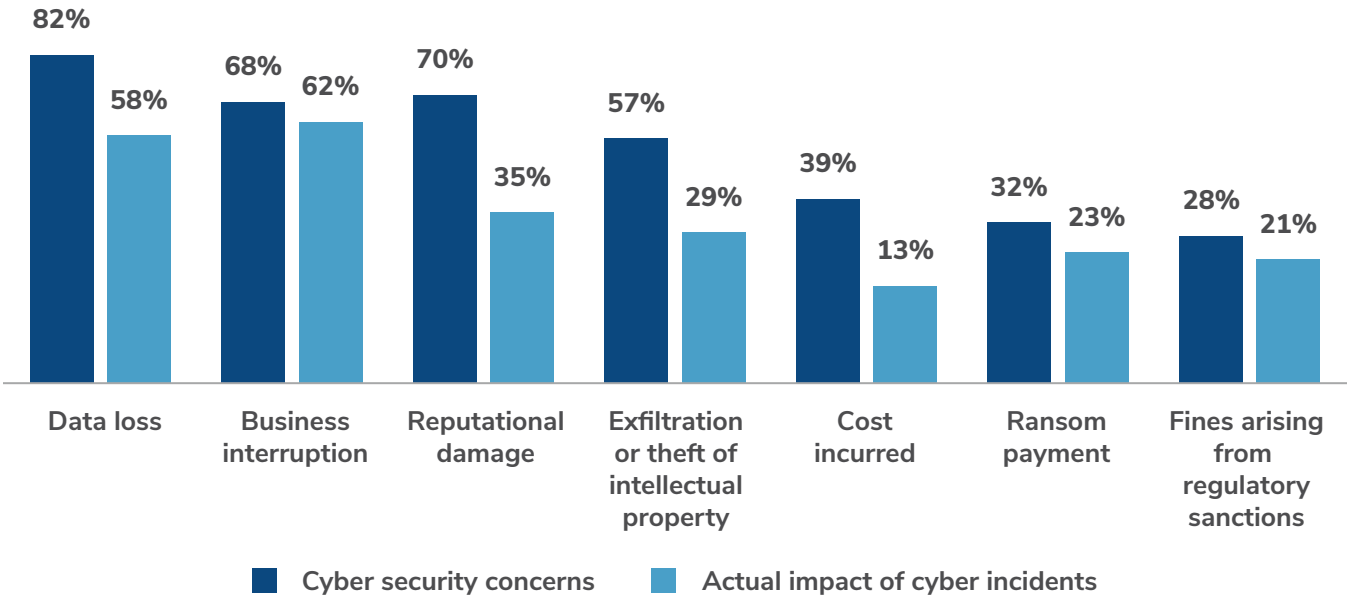
Proportion of Businesses that Have Experienced a Cyber Incident, by Market



Measures Implemented to Address Cyber Security Threats



Cyber Security Concerns and Impact of Actual Incidents

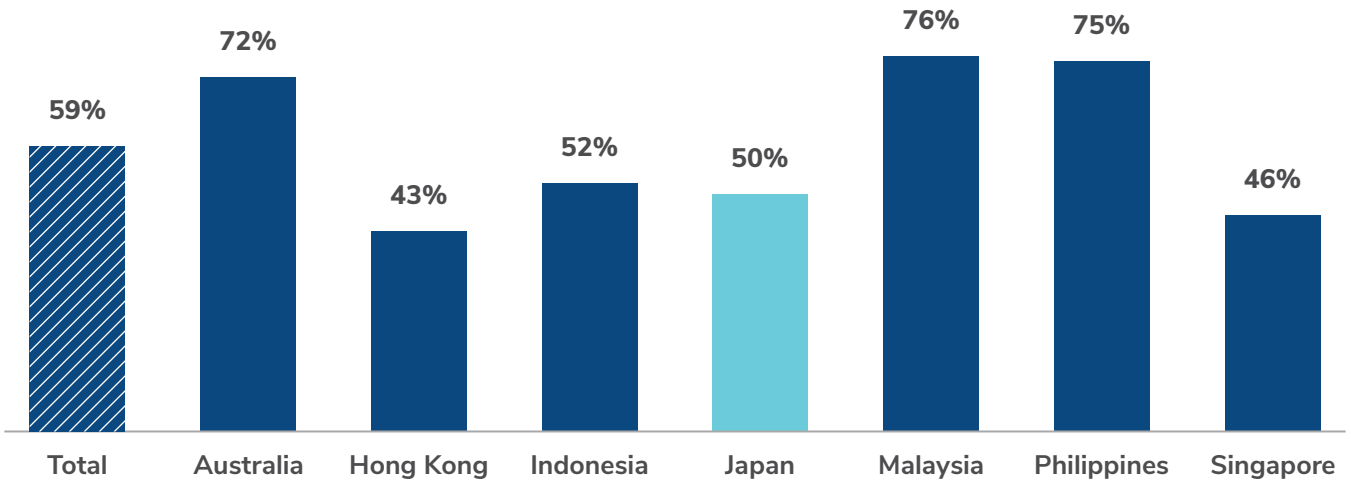


Japan

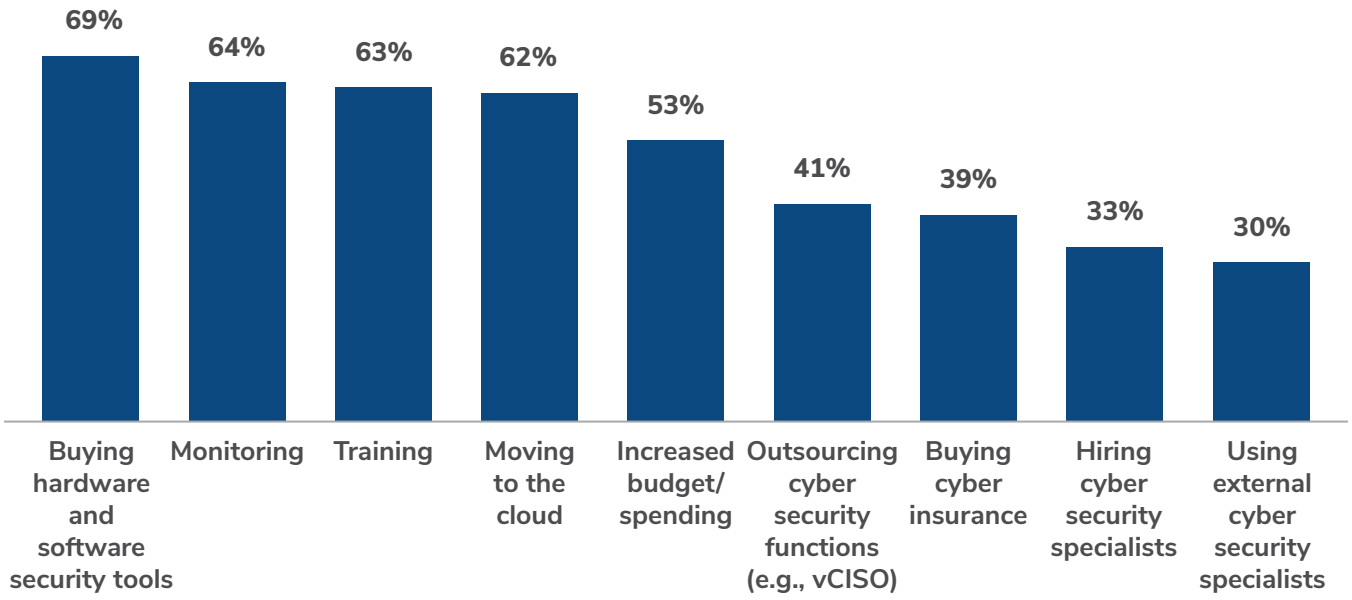
Half of Japan's businesses reported being impacted by a cyber incident (50%), which is under the Asia Pacific average of 59%. Like the rest of the region, data loss is their primary concern, reported by 71% of respondents.

The biggest impact of cyberattacks in Japan was data loss, at 58%. Of all the markets analyzed in APAC, Japan was the least likely to report ransom payments as an impact of cyberattacks (8%), despite 36% of respondents being concerned about it.

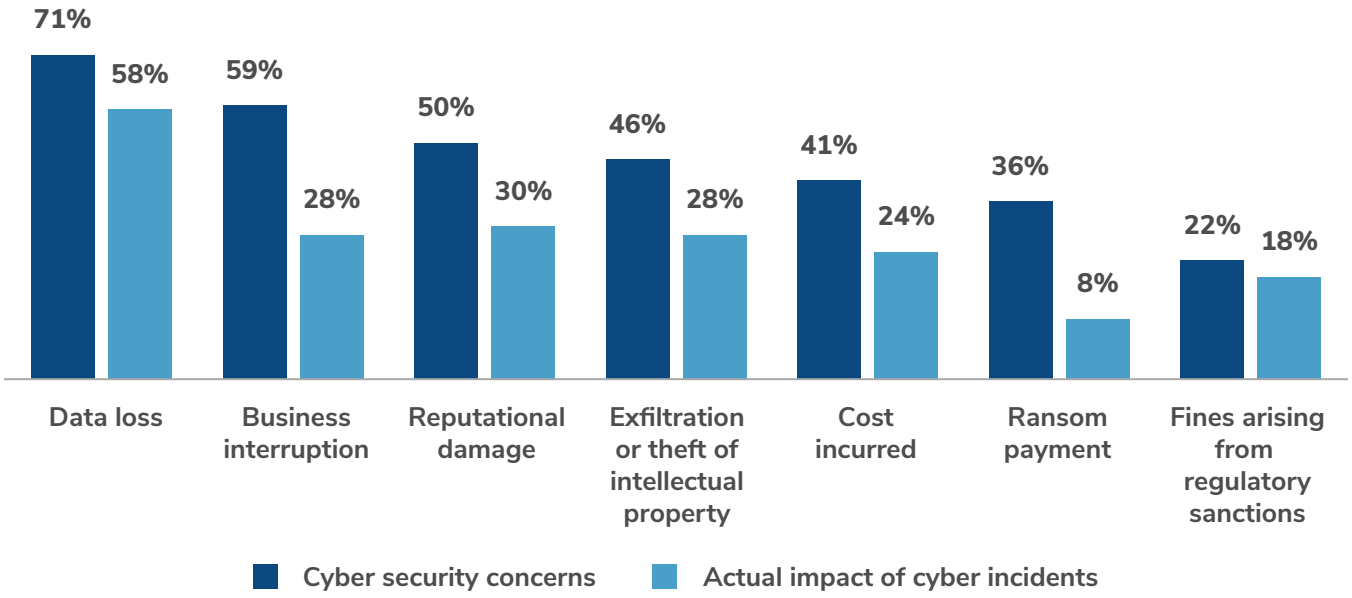
Proportion of Businesses that Have Experienced a Cyber Incident, by Market



Measures Implemented to Address Cyber Security Threats



Cyber Security Concerns and Impact of Actual Incidents

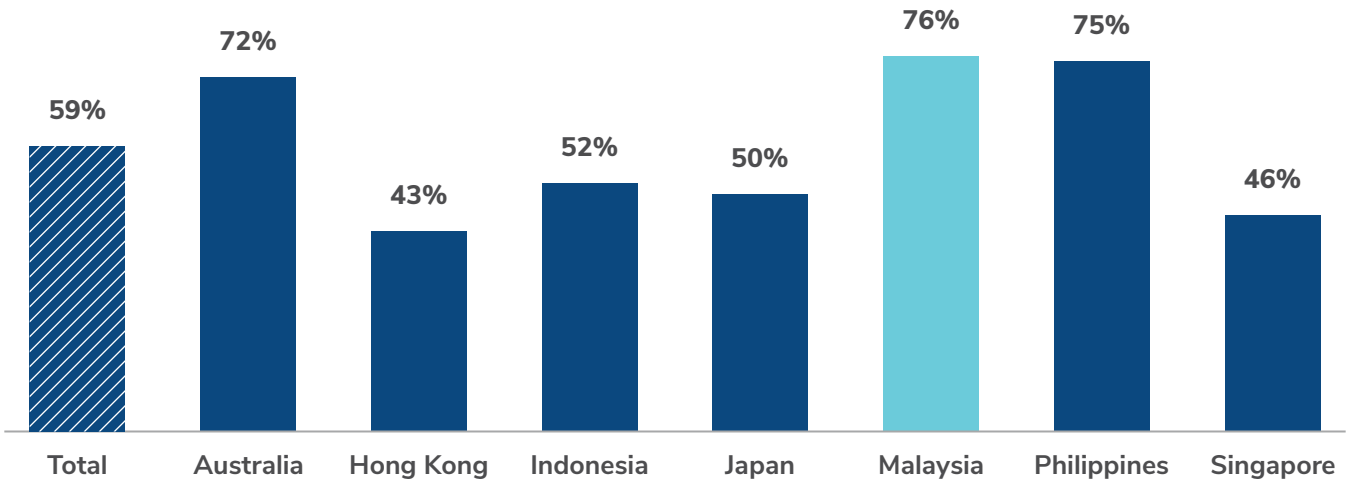


Malaysia

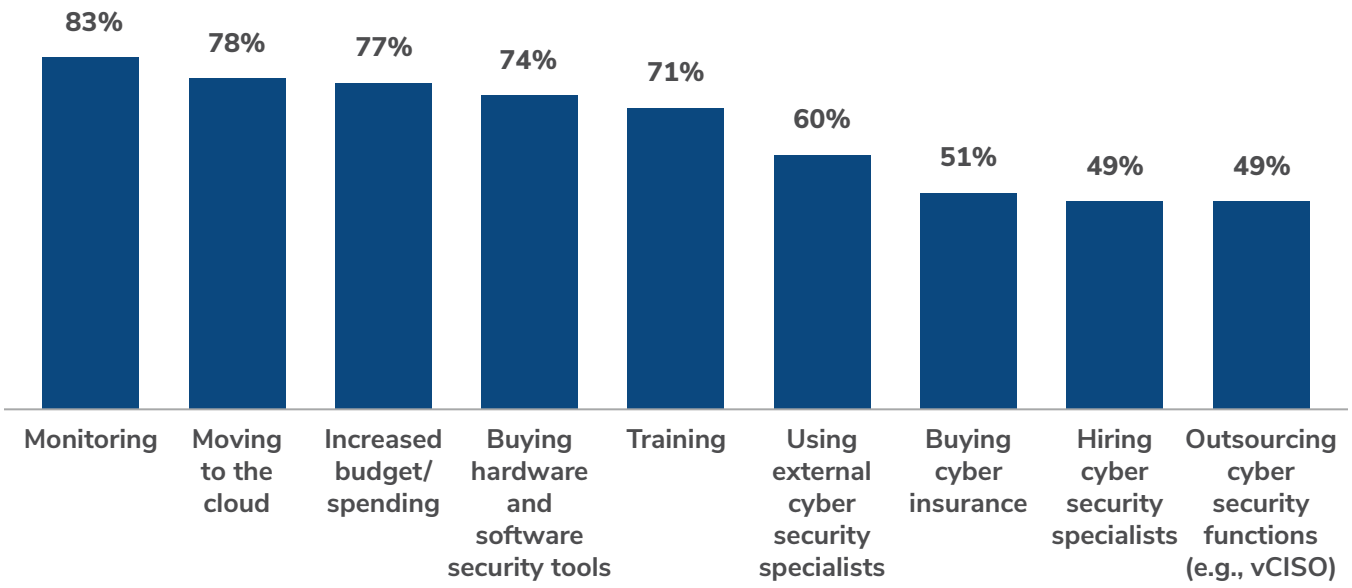
Malaysia has experienced more cyberattacks than any other country in the APAC. Seventy-six percent of the 100 organizations surveyed reported a cyberattack, this is almost twice the number reported by Hong Kong, which reported the lowest at 43%.

The country's concern around data loss caused by a cyber incident was also joint highest with Indonesia (82%). Malaysian businesses' concern for data loss is substantiated by the reported impacts, with 57% of incidents resulting in data loss.

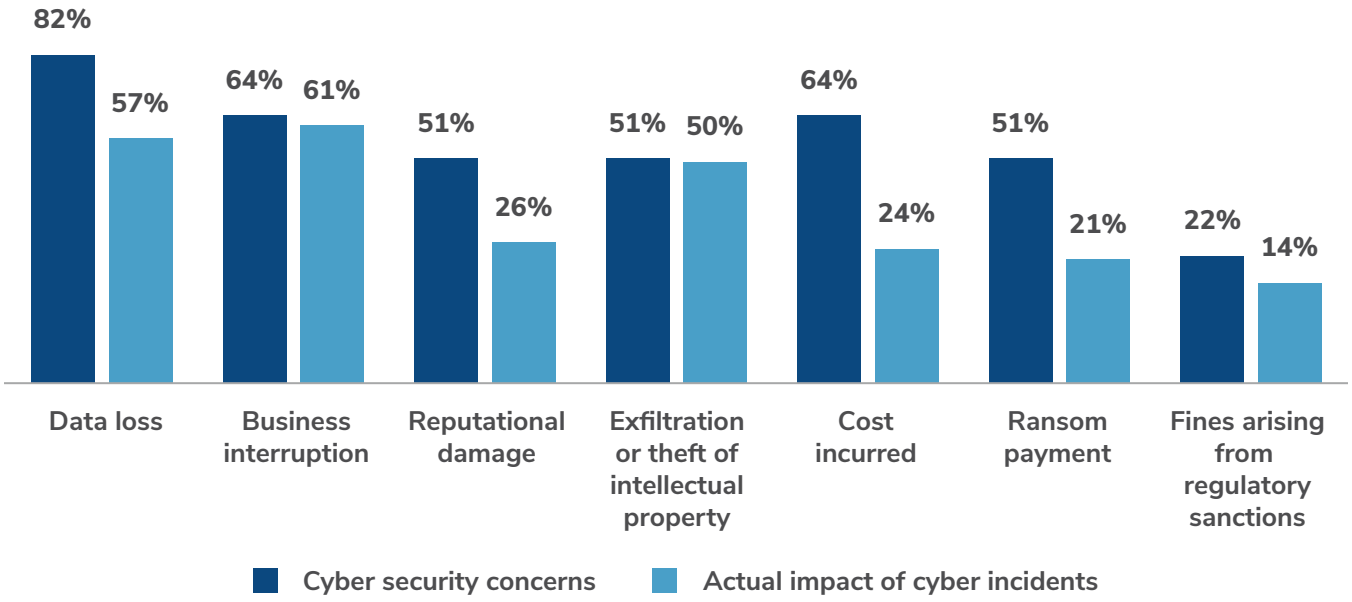
Proportion of Businesses that Have Experienced a Cyber Incident, by Market



Measures Implemented to Address Cyber Security Threats



Cyber Security Concerns and Impact of Actual Incidents



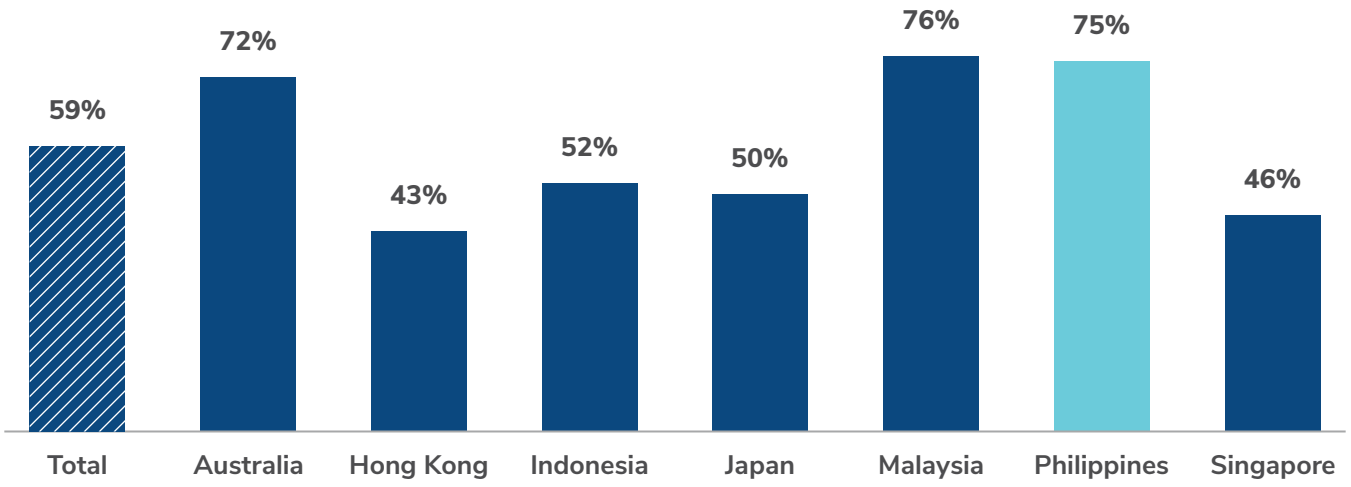
Philippines

Seventy-five percent of organizations in the Philippines have experienced a cyber incident, which is much higher than the APAC average of 59%.

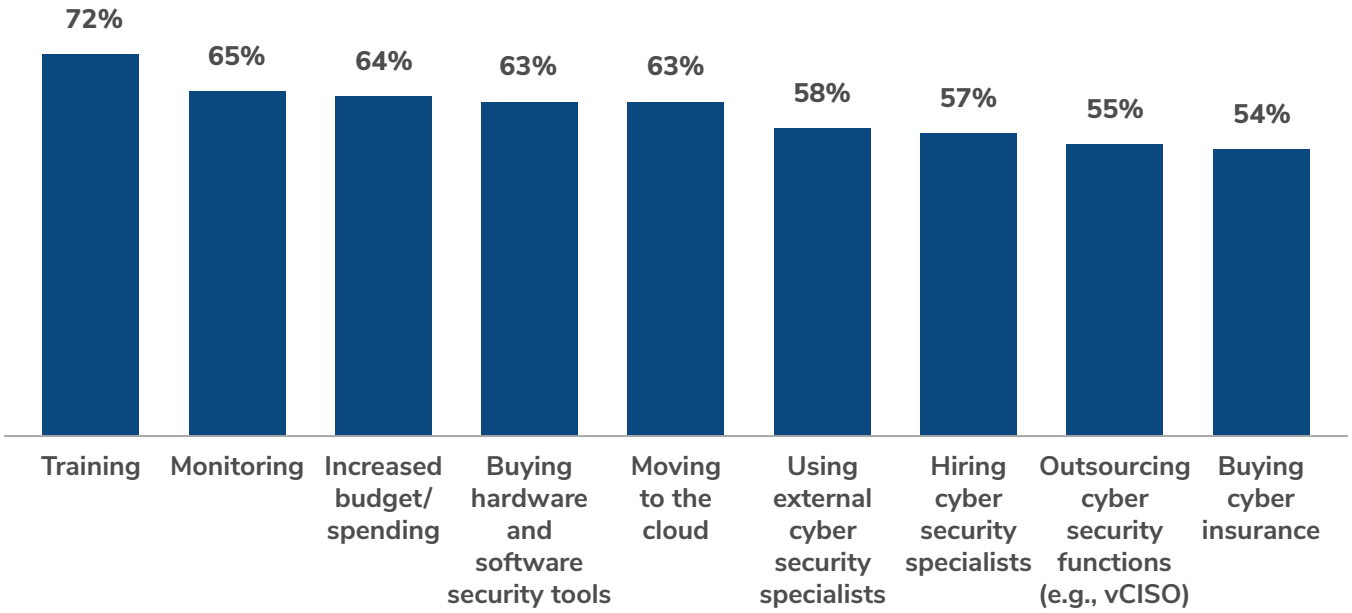
The greatest concern among organizations in the Philippines is data loss (70%). Compared to other countries across APAC, however, respondents were also much more concerned about intellectual property (60%).

While 60% of respondents cited business interruption as the most significant consequence of a cyberattack in the Philippines, 29% also cited regulatory fines, higher than in any other APAC country.

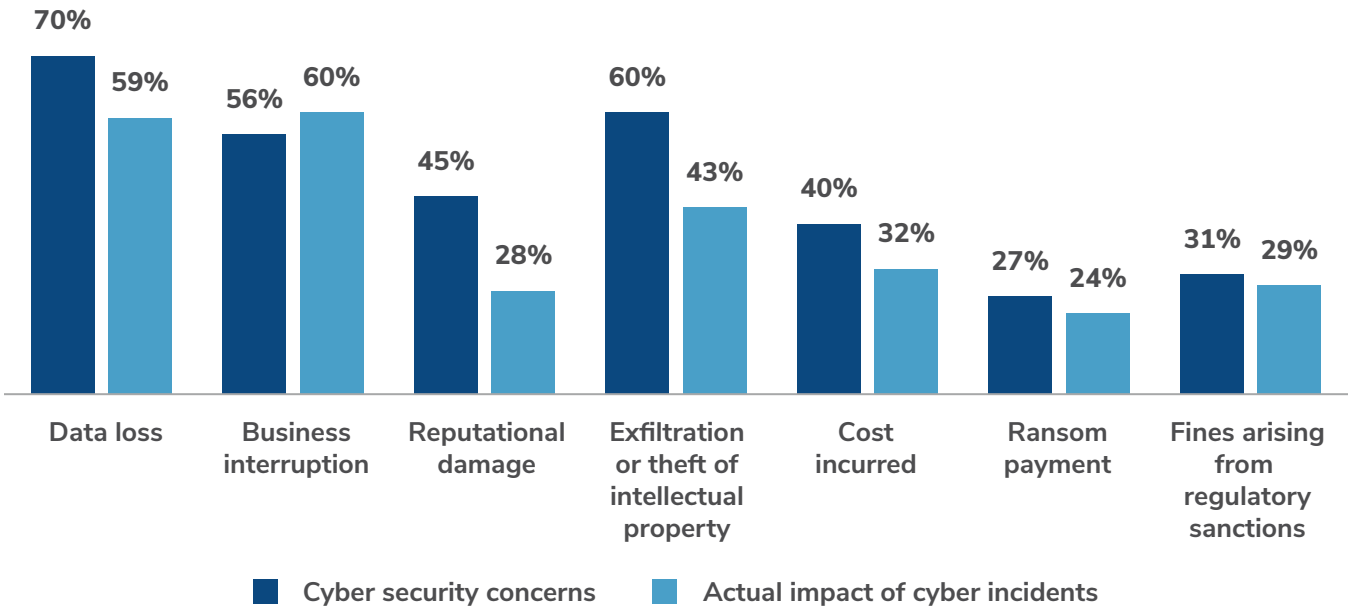
Proportion of Businesses that Have Experienced a Cyber Incident, by Market



Measures Implemented to Address Cyber Security Threats



Cyber Security Concerns and Impact of Actual Incidents

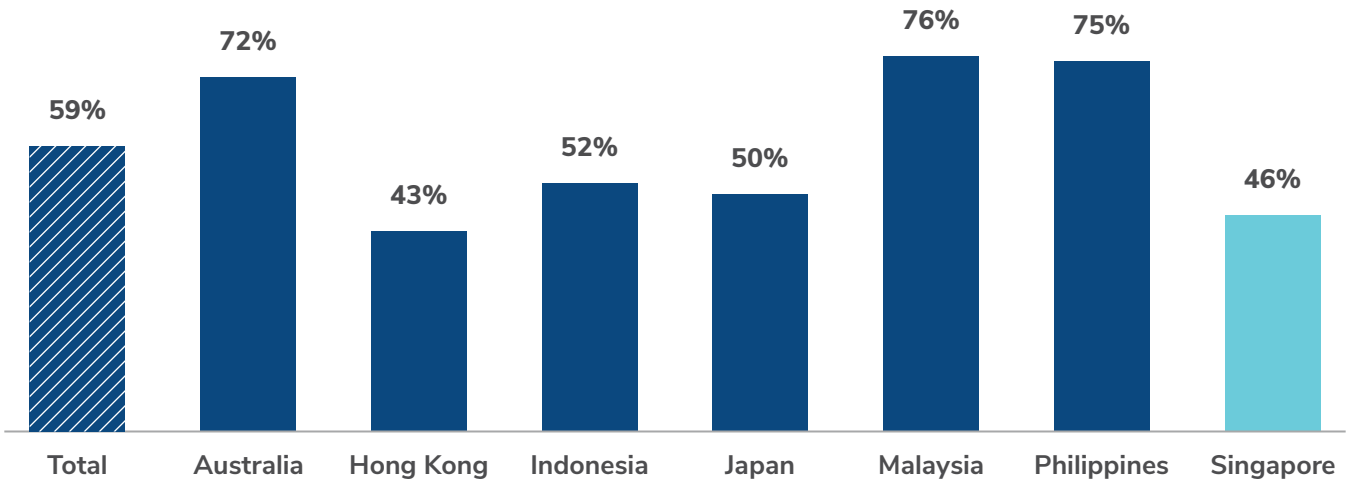


Singapore

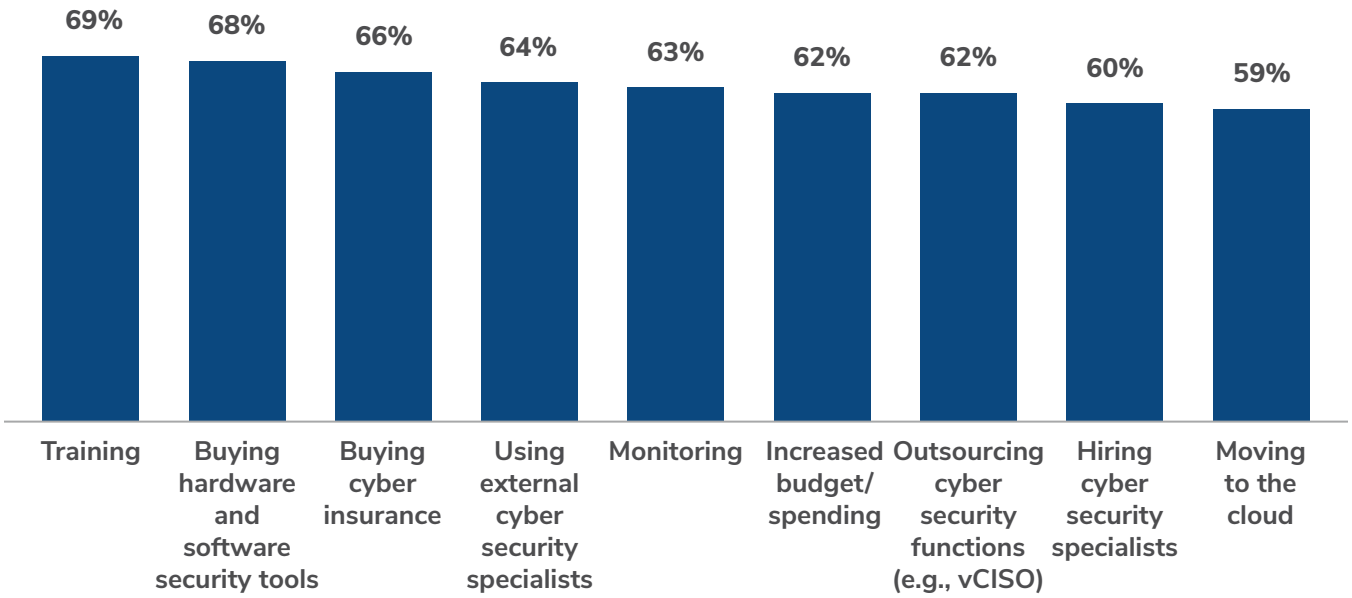
Almost half of Singapore businesses have experienced cyber incidents (46%), which is lower than the overall APAC average of 59%.

The Singapore market is most concerned about data loss (55%) and business interruption (52%), which was representative of the greatest concerns across the whole APAC region. Data loss and business interruption were also the most reported impact of cyberattacks by 43% of those surveyed.

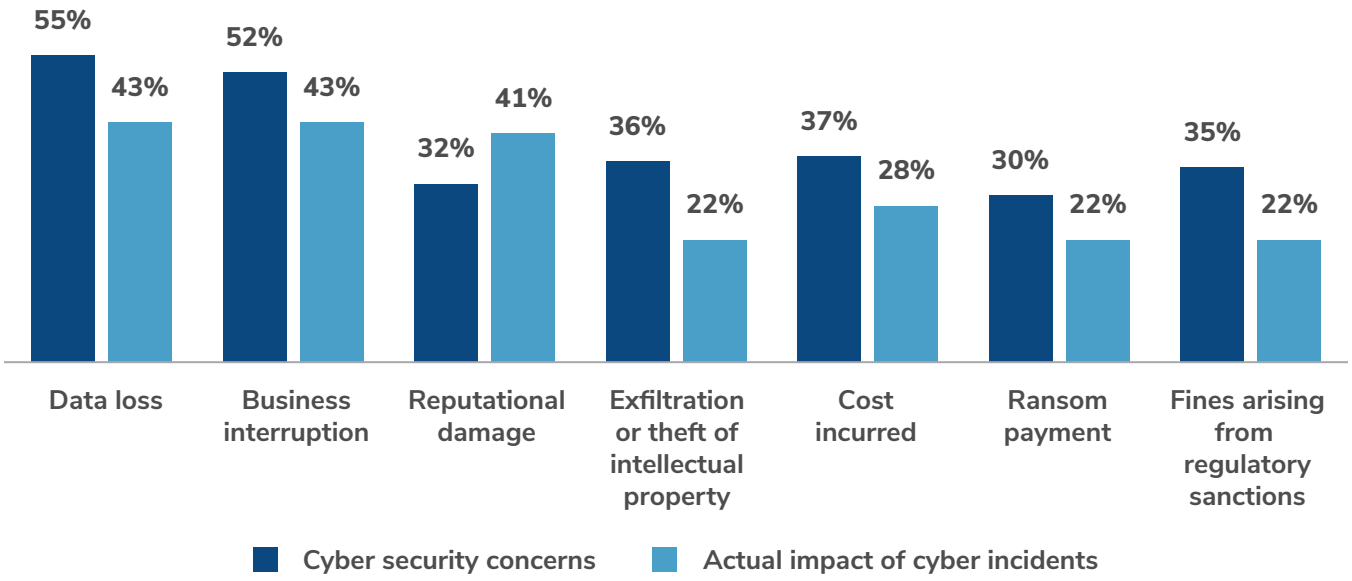
Proportion of Businesses that Have Experienced a Cyber Incident, by Market



Measures Implemented to Address Cyber Security Threats



Cyber Security Concerns and Impact of Actual Incidents



Best Practice Recommendations

Adopting a more proactive approach to cyber security can seem daunting at the outset. However, following a pragmatic and structured roadmap with clearly defined steps can not only enhance security but also deliver peace of mind. Taking a longer-term perspective also reduces the financial and reputational risks of responding to cyberattacks without effective prior planning.

Key recommendations for enhancing cyber resilience can be found in Kroll's 10 Essential Cyber Security Controls. In particular, they include:

Leverage Managed Detection and Response

Organizations can significantly strengthen their cyber security posture by deploying managed detection and response (MDR) service, which combines technology and specialist expertise to monitor for and respond to threats on a 7x24x365 basis. MDR gives organizations the capacity to detect and contain them before they have a greater impact.

Implement Incident Response Planning

A critical aspect of boosting cyber resilience is to establish a clear, measurable incident response playbook that sets out clear and specific steps to follow in the event of an attack. Incident response planning provides businesses with a roadmap for effective and timely action, as well as reducing the risks created by damaging delays or missteps in the response process.

Undertake Tabletop Exercises

As part of incident response planning, organizations benefit from gaining a detailed understanding of their security vulnerabilities and potential adversaries. This can be achieved through incident response tabletop exercise scenarios which have been customized to test the organization's response plan and its stakeholders and help improve and evolve a security program. Tabletop exercises provide valuable insights into a company's level of preparedness, the steps it will need to take in the event of a real-world attack and any remediation of the plan stemming from the tabletop exercise.

Commission Assessments and Penetration Testing

Regular penetration testing and assessments allow businesses to identify and address undiscovered or under-prioritized vulnerabilities in their security and mitigate them before they can be maliciously exploited. Companies should carefully consider which type of testing or assessments will be most appropriate for their requirements and ensure that the proposed process will conclude with strategic recommendations and remediation advice.

Embed Key Controls

Organizations should aim to move beyond security silos to embed cyber security centrally within their business practices and processes. This is achievable when undertaken in small incremental steps via a number of key controls. From enabling multifactor authentication (MFA) to managing the risks of virtual private networks (VPNs), companies can benefit significantly by employing the gamut of measures to strengthen their security and reduce the likelihood of cyberattacks.

Appoint a vCISO

For organizations that do not have the resources for senior security personnel, appointing a vCISO is a commercially sound option to provide the security team some guidance and for the company to gain access to experiences that might prove a challenge to source, not least during an incident. vCISOs can help a company create/accelerate data security initiatives, inform management and validate existing programs for the board with unique perspectives on regulatory, technology and operational cyber impacts.

Please refer to the About Us section below if you would like to discuss this whitepaper, best practices or how we might support you.

Conclusion

Global business continues to feel the impact of an onslaught of cyberattacks, and APAC is no exception, with 59% of organizations reporting an attack and 32% reporting multiple attacks. There is a further risk that this number will increase as the regulatory landscape continues to evolve and more incidents are reported.

Incident response plans, policies and recovery plans are invaluable when it comes to surviving a cyberattack, as is having access to experienced personnel. Currently, only two-thirds (64%) of organizations surveyed have plans in place, and a fraction less than that have access to cyber security specialists (62%), leaving around a third of businesses without sufficient plans or expertise to navigate an attack.

Businesses have unsurprisingly focused on continuity and operational stability during the pandemic, but Kroll now urges businesses in these regions to consider scaling up response plans and investment in cyber expertise. It will enable them to remain resilient and recover quickly if an attack does occur, paying dividends in the long run.

Explore Kroll's cyber security solutions at kroll.com/cyber

Get in touch with a cyber expert 24x7 using our global hotlines at kroll.com/hotlines

Methodology

This report is based on 700 online interviews conducted in March and April 2022 with decision-makers in the IT, risk, security and legal professions. The sample was evenly split across key APAC markets: Hong Kong, Singapore, Malaysia, Philippines, Australia, Indonesia and Japan. Respondents were from companies with a turnover of greater than $10 million and quotas were set to ensure no more than 25% came from any sector within each market.

Research was conducted between March 2022 and April 2022.

KROLL

About Us

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities.

From incident response to risk assessments, and complex forensics to breach notification and litigation support, Kroll's cyber experts can help in every step of the way toward cyber resilience. With over 600 experts, our global team handles 3,200+ incidents every year, including some of the most complex and highest profile matters in the world.

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.