SOPHOS

The Future of Cybersecurity in Asia Pacific and Japan – Culture, Efficiency, Awareness

"A TRA Report sponsored by Sophos"

Introduction

The success of an organisation's cybersecurity investment lies in more than technology adoption. Organisations must also create a strong security culture, educate employees and establish a path-to-purchase that ensures robust security capabilities for today's rapidly evolving threat landscape.

This Tech Research Asia (TRA) report offers evidence-based guidance for decision makers across Asia Pacific and Japan (APJ) on how to boost their technology investments alongside their operational performance and internal cultures.

It is based on a comprehensive research program that included a quantitative survey of 900 cyber and information security decision makers in Australia, India, Japan, Malaysia, the Philippines and Singapore; interviews with industry experts; and five executive roundtables held in 2019 in Australia (2), India, Japan, and Malaysia.

The research reveals that organisations in APJ face a series of cybersecurity shortcomings in the areas of education, company culture, skills, budgeting and operational management. Overcoming these challenges won't be easy, but they are at the heart of problems with cybersecurity strategies and operational management today. There are opportunities to strengthen these areas in addition to the hardening of the technology platforms and tools used.

This report comprises four sections – the research results, individual country insights, a list of steps to consider, and the view of the report sponsor, Sophos.

The current security reality in APJ is this: Without improved efficiency and effectiveness of cybersecurity investments, organisations will continue to slip into a downward spiral of chasing quick-fixes for new threats. Companies will experience sub-optimal results for spending and struggle to be proactive, rather repeatedly having to react to incidents and breaches. In an era that is characterised by a rise in privacy legislation and governance, businesses will have to deal with the fallout of poor choices, which increasingly will extend beyond simplistic financial "per breach" cost calculations or brand impairment and into real life personal and societal damage.

What will your future look like?

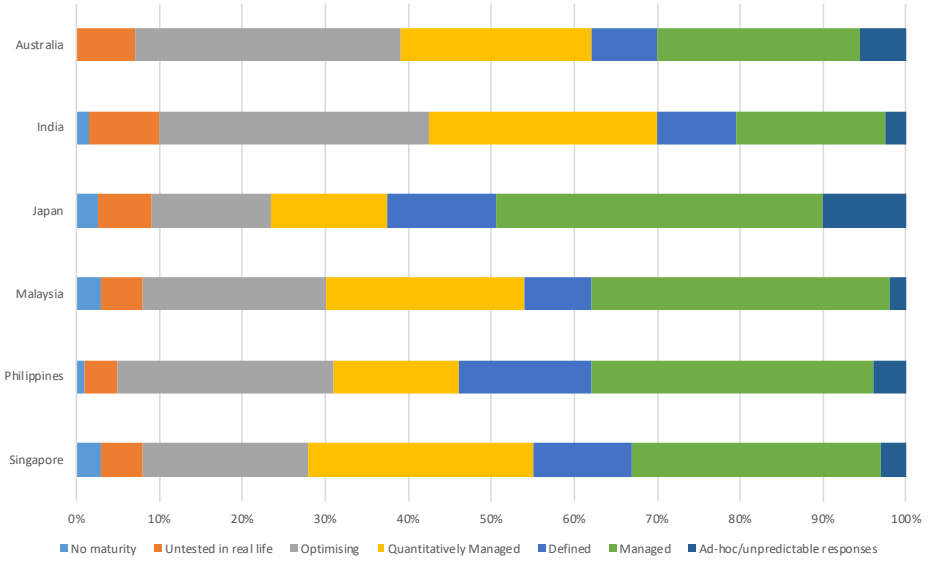
The Research Findings

The following research results are presented in three sub-sectors (The Security Setup, The Security Journey and The Future of Security), each with important data and findings highlighted.

The Security Setup: Maturity is not a strong point

The first segment of the research investigated the current state of affairs and approaches that exist in organisations across APJ. There are, of course, some differences between the countries canvassed and also within each market. However, it is evident that perceived security maturity remains low, with less than one third of respondents self-reporting that they are at the top "optimised" maturity level (where processes are monitored and are frequently improved and tailored to the unique needs of the organisation). The majority of organisations acknowledge that they have a low level of security maturity as evidenced in the following chart. (Refer to the appendix for a short description of the maturity rankings.)

Q. Please tell us which of the following terms best matches your level of maturity.

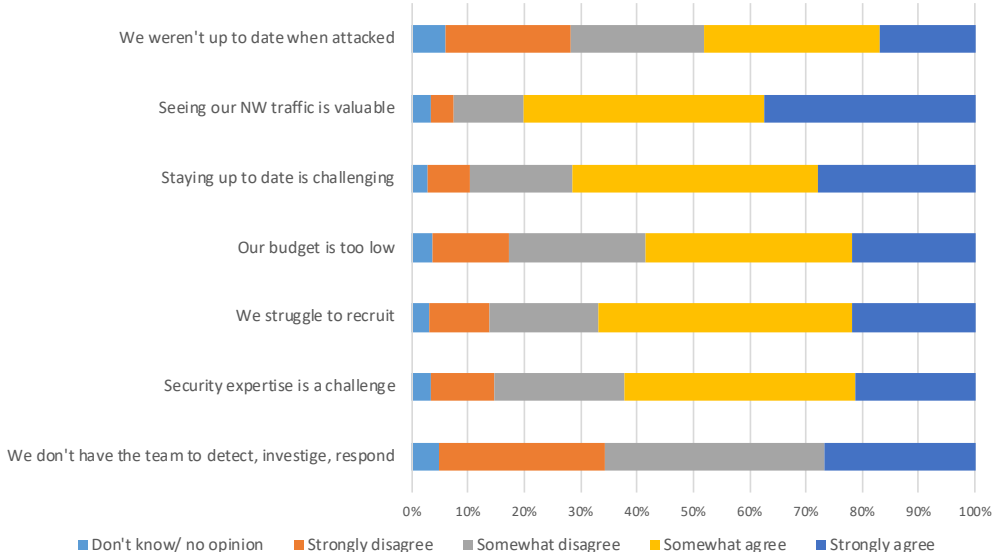


Of the countries surveyed, the research data suggests that India, Australia and Singapore have higher levels of security maturity (combined data points of 'quantitative' and 'optimising' scores) relative to Japan, Malaysia and the Philippines.

Interestingly, when asked if their organisation had a cybersecurity team in place that could properly detect, investigate and respond to threats, 59% of Indian companies and 47% of those in Australia stated 'no'. This is a clear case of perceptions being somewhat different to reality, with the contrast suggesting that maturity levels can be highly subjective unless properly quantified and regularly tested.

The data in the following chart reinforces this situation. It shows the level of agreement survey respondents have to a series of questions. Across many critical issues there is a strong level of agreement that more help is needed – for example budgets are too low, recruiting skills is difficult, and staying up to date is a challenge. All are factors that contribute to security maturity and indicate much more work is required to improve overall security posture.

Q. To what extent do you agree or disagree with these statements below?



Some of the other notable characteristics that are common across all markets are:

- Over 50% of budgets that relate to cybersecurity sit outside of IT. This suggests that communication skills and stakeholder management or negotiation are important to ensuring budget is spent appropriately. There was little significant variation in cybersecurity budgets in this regard with only companies in the Philippines and India having slightly above average allocation of cybersecurity budgets as an independent budget centre in its own right.
- The majority of organisations continue to keep most capabilities in-house and only in a few areas such as penetration testing and training does outsourcing become a more common approach.
- Organisational structures are varied with one third having a dedicated CISO, another third having cybersecurity led by an IT leader, and the remainder give responsibility to another executive. A similar split is evident in teams either being an independent and separate security team or constituting part of the IT department.

The 'dual-hat' organisational approach to leading cybersecurity, where a CIO or CTO also assumes CISO authority, emerged in the roundtable discussions as a pragmatic (with regard to limited resources and budgets) yet sup-optimal option for many organisations.

It was evident that communication, education, strategy determination and resourcing demand a dedicated cybersecurity lead that is not at risk of being subsumed into, and distracted by, the broader IT environment and issues. Indian organisations showed the greatest change in moving towards a CISO-led cybersecurity strategy in the coming 24 months, with Singapore showing the second highest CISO-led percentage.

It is further clear from the data that organisational structure and non-technical issues are felt across APJ and may be contributing to a low level of maturity. Notably, three in 10 organisations say they suffered a data breach in the past 12 months. In our view, this is low and it is more likely that around seven in 10 organisations have experienced breaches and all companies will have suffered cybersecurity incidents. One CIO at the Kuala Lumpur roundtable noted: "We get attacked every day and have suffered breaches – it is a fact of life in 2019". Similar comments were recorded at other roundtable events. The results and anecdotal evidence emphasise we are not succeeding based on current security approaches.

There was little variation in those disclosing a breach across individual countries. The percentages of those that have experienced breaches per country were as follows:

Japan	Australia	India	Malaysia	Singapore	Philippines
34.5%	34%	33.5%	32%	26%	24%

The Security Journey

The second sub-section is the security journey. And it is a journey that is changing. Consider the following research results, which characterise the new journey:

When changes are made and who is involved: 82% of organisations intend to make some changes in the next 12 months. The main triggers for this new activity – beyond the fact that more than 50% only made a change to their strategy over 12 months ago – is new technology and product development, compliance and regulation, and awareness of new attacks.

The top influences on investments are: #1 Dedicated Security Researchers. #2 Analysts and Consultants. #3 Penetration Testers. Other sources of influence are starting to make an impact and change the way leaders make decisions, namely design thinking workshops, government manuals on cybersecurity, and artificial intelligence- (AI) and machine learning- (ML) led advisory systems.

Notably, as 50% of security budgets sit outside of the IT budget, a broad list of executives are involved in influencing security investment decisions – it's not just the CISO or CIO.

Key issues being considered: One of the biggest issues, if not the biggest, is not technical in nature – it is human. More than 70% say education of employees and leadership is the biggest challenge and 60% struggle to provide this. Two thirds of organisations also struggle to recruit and find it difficult to stay up to date with the pace of developments, research and news.

On the tech-side of key issues, there is a strong desire for better network visibility and control – 80% value this capability. AI is welcomed with an additional 12% of organisations intending to adopt the technology within 24 months. More than four in 10 organisations see IT and OT convergence as an area that could help their security posture.

What is IT and OT convergence?

OT is short for operational technology. This is technology that is used to run and maintain the operational side of a business. OT systems are most common in manufacturing and industrial environments and typically are used to monitor, process and adjust devices, for example supervisory control and data acquisition (SCADA) systems in energy companies or sensors embedded into a manufacturing plant to monitor machine wear. Typically, OT has not been networked and historically it has had little integration with IT systems.

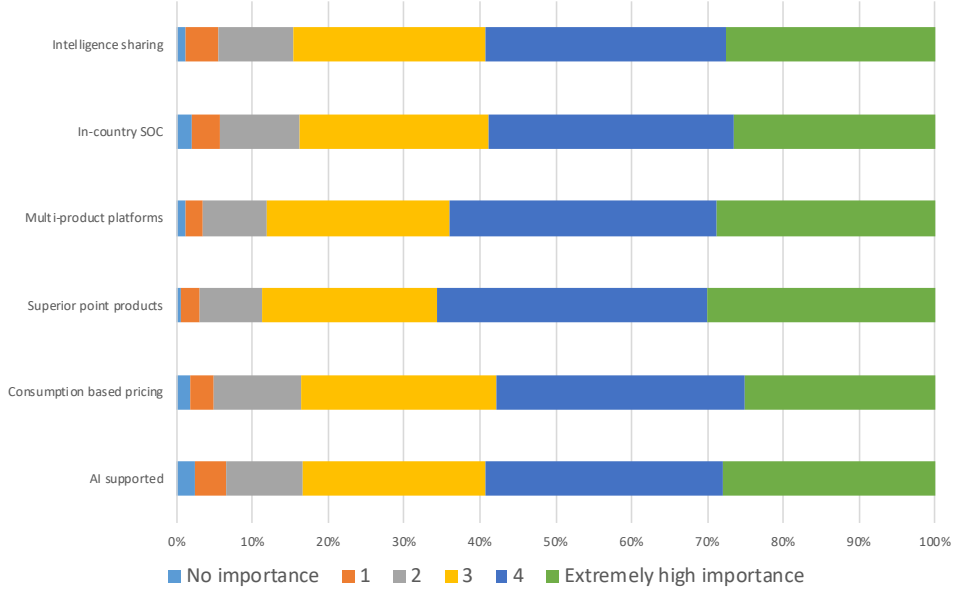
As IT systems increasingly integrate with OT systems, greater co-operation and co-ordination is required between previously separate OT and IT groups within the business. This in turn both exacerbates the security complexities faced by organisations and encourages greater focus and clarity on holistic cybersecurity strategy, capabilities and posture.

Importantly, there is a belief that the future is stark when it comes to the cybersecurity threat landscape. The research results tell us that all current threats remain serious in the next 24 months. Phishing and AI-led attacks (such as the use of machine learning tools that scan systems for weaknesses or create images to breach identity safeguards that use biometrics such as facial recognition) are of most growing concern.

The purchasing phase: When it comes to investment, APJ organisations like both point solutions and integrated platforms. At roundtable events, several participants noted they want best-of-breed solutions that can help with specific industry-based challenges or needs, while others appreciated the efficiency of an integrated platform.

68% of organisations are happy with their current suppliers and likely to repurchase. However, one in two will increase the number of third-party providers they use. This latter data point is partly because security and business needs are increasingly specialised based on industry (developing new products and services or addressing compliance). It is also because many organisations are looking for new tools and partners each time they encounter a new attack or threat.

The study examined what factors were important to organisations when considering information and cybersecurity solutions. The following chart shows the top factors:



For many businesses there is an expectation that their cybersecurity vendors and partners should both thrive on their own and play well with others. Also important is information sharing to bolster capabilities.

At a country level, AI is of very high importance to Indian organisations and of least importance to those in the Philippines. The availability of technically superior point product solutions is of highest importance in Indian, Australian and Malaysian organisations, and less so for those in Singapore. The same observation can be made for the availability of consumption-based pricing. At the same time, multi-product integrated platforms are identified as key considerations for India, Australia and the Philippines, suggesting a relatively more diverse market in these countries.

The research also explored issues that companies cited as causing frustration for their cybersecurity strategies and activities and where cybersecurity vendors need to help. The top five issues were:

1. **Relegation in priority of cybersecurity:** The inconsistent focus given to security by the board/executive management committee that fluctuates depending on how intensively/frequently the organisation is under attack/experiencing incidents. The higher the level, the higher the priority for cybersecurity. As the level subsides, so too does the priority.
2. **Lack of budget:** An issue impacting in multiples ways, ranging from the expense involved in hiring skilled employees, the availability of cybersecurity budgets, and the relative effectiveness of the budget spend on technology solutions.
3. **Lack of understanding of the complexity of issues.** The misguided view that 'security is easy. It's just about buying new <insert appropriate technology solution here>'. The data and executive roundtables jointly confirmed there is a lack of appreciation about the complexity of issues faced – at a board and executive level through to general employees. Education was seen as a key area of focus for many organisations to help address this.
4. **The 'we're all doomed' fear, uncertainty and doubt (FUD) messaging.** The data highlighted that the FUD approach of certain vendors in the industry has started to lose its effectiveness. Instead, businesses are keen to understand how vendors and their partners can help address key areas and point to the light at the end of the tunnel not being an oncoming train.
5. **Lack of resources.** As with many technology deployments, resourcing is an issue for all organisations. Budgets, staff, and even skilled vendors and partners can be lacking in certain industries or technology sections (for example the distinct lack of cloud cybersecurity experts in the early days of cloud infrastructure migration and more recently around AI and ML deployments).

Delving more deeply into specific country markets, the data revealed some nuances among the top frustrations as noted in the following table:

Country	Top 1	Top 2	Top 3
Australia	Security is 'easy'	Prioritisation	Budgets
India	Prioritisation	"We'll never get hacked"	Security is 'easy'
Japan	Budgets	Skills shortage	Training and education
Malaysia	"We'll never get hacked"	"We'll will get hacked and there's nothing that can be done"	Security is 'easy'
Philippines	'Noise' makes it difficult to understand	Prioritisation	Budgets
Singapore	Prioritisation	Budgets	Skills shortage

Organisations' needs are clear, and vendors and partners need to ensure that their engagements are built as much around the business issues as the technical prowess of the solutions offered.

The Future of Security

When it comes to the future of security, the research indicated there is a considerable cybersecurity skills shortage in all markets.

More than this, educating leaders and employees is for the majority the biggest challenge faced. Sixty per cent of respondents say they struggle to provide this education – a notable result considering some estimates suggest more than 50% of incidents are caused by internal employees or partners. It was also interesting to note the research data suggests education is a never-ending requirement, especially as businesses find it challenging to ensure internal resources are up to date on the constantly evolving threat landscape.

When it comes to technology, the survey respondents indicated that the technologies that will most impact their organisation's security in the next 24 months were artificial intelligence and machine learning, digital transformation programs, IT and OT convergence and the shift to cloud computing.

While there is a lot of hype and confusion around AI and ML in the market, the research results indicate there is considerable interest and appetite in how these technologies can help in the future.

TRA data shows that on average 33% of organisations are considering the use of AI and ML in their cybersecurity operations and this will increase by another 12.4% in the coming 24 months. There is a clear shift towards adopting AI and ML for security approaches, particularly for pro-active defence and fraud mitigation, and scanning systems. In the coming 24 months, AI and ML deployments will predominantly be in the areas of pro-active defence, fraud mitigation and scanning systems as the following chart illustrates:

Of the countries, the most aggressive adopters are India and Singapore, although all show potential for uptake.

Concluding comments

To conclude, it is important to note that there are many technical issues related to cybersecurity today. There are multiple vulnerabilities and risks that relate to technology alone. However, this research also highlights that there are considerable improvements to be made in non-technical areas in addition to technology investments.

Combining a robust platform approach to cybersecurity that is hardened by skilled experts and partners with an improved operational and cultural emphasis will help our chances of success in future.

Cybersecurity in Australia

- 34% of Australian organisations said they had been breached in the last 12 months – the second highest of all the surveyed countries, second only to Japan (34.5%)
- 37% of Australian firms state their approach is either untested, ad-hoc or managed and 55% believe they have a relatively high maturity, either quantitatively managed or optimised, putting them second to India 60%)
- Just under half (47%) of Australian respondents feel their organisation does not have a cybersecurity team in place that could properly detect, investigate and respond to threats
- Skills, education and resources
  - 65% struggle to recruit skilled cybersecurity professionals
  - 59% state that there is insufficient budget for cybersecurity
  - 68% observe that staying up to date with cybersecurity technology is challenging
- The most serious attack vectors in Australia (receiving a seriousness rating of 9 or 10 out of 10) are malware, phishing and ransomware
- The top three frustrations experienced as relates to information or cybersecurity are:
  - Our executives assume cybersecurity is easy and me/my cybersecurity peers over exaggerate threats and issue
  - Cybersecurity is frequently relegated in priority
  - There is not enough budget for cybersecurity
- The top technologies or issues Australian security decision makers think will impact their organisation's security in the next 24 months are digital transformation programs, agile development, and AI and machine learning

"Repeat offenders are a nuisance. We spend a lot of time educating our people but there's still a core group that are significant contributors (to breaches). Finally, we got sick of it and now we have a company-wide demerits policy. It's a bit like a driver's licence. Make too many mistakes and you're out. We have board and exec buy in for that without too much issue. Obviously, we don't make it as draconian as it sounds but it has provided a strong motivator."

"1 in 3 breaches? I wish. I bet that's only the ones they know about. It's higher than that."

"Data breach (Notifiable Data Breach legislation) really made us rethink. Our board suddenly became even more focused on security as a result."

"Gamification worked for us (education of employees). We try to keep it relatively positive and highlight wins and successes not big mistakes."

Cybersecurity in India

- 33.5% of Indian organisations said they had been breached in the last 12 months – the third highest of all the surveyed countries
- 30.5% of Indian firms state their approach is either untested, ad-hoc or managed and 60% believe they have a relatively high maturity, either quantitatively managed or optimised
- Two thirds (59%) of Indian respondents feel their organisation does not have a cybersecurity team in place that could properly detect, investigate and respond to threats
- Skills, education and resources
  - 69% struggle to recruit skilled cybersecurity professionals
  - 65% state that there is insufficient budget for cybersecurity
  - 66% observe that staying up to date with cybersecurity technology is challenging
- The most serious attack vectors in India (receiving a seriousness rating of 9 or 10 out of 10) are malware, phishing and backdoor vulnerabilities (i.e. when a backdoor is created in a system and is then used by unauthorised third parties)
- The top three frustrations experienced as relates to information or cybersecurity are:
  - Cybersecurity is frequently relegated in priority
  - Our executives assume our company will never get attacked
  - There's too much fear and doubt messaging that makes it hard to talk accurately about cybersecurity
- The top technologies or issues Indian security decision makers think will impact their organisation's security in the next 24 months are AI and machine learning, IT and OT convergence, and digital transformation programs

"We (India) do have cybersecurity legislation in place and we're supposed to notify the government of any breaches. Realistically hardly any of us do. It's not really worth the attention and the inconvenience."

"There's so much activity (attacks) that we just had to get better at security or forget about it. There's almost no middle ground."

"The interest in cloud has forced us to reassess our overall security strategy. Rather than a more hardware driven approach we're looking much more towards partnerships with managed security providers to ensure that we don't get caught out."

"Education is a problem for us. I firmly belief that until CIOs or employees start losing their jobs, it is exceedingly difficult to make our employees cognisant of security risks and, most critically, keep the awareness at the front of their minds."

Cybersecurity in Japan

- 35% of Japanese respondents said they had been breached in the past 12 months – the highest percentage of all countries
- 38% of Japanese firms have no cybersecurity maturity or their approach is untested or ad hoc
- Two thirds (51%) of Japanese respondents feel their organisation does not have a cybersecurity team in place that could properly detect, investigate and respond to threats
- Skills, education and resources
  - 72% struggle to recruit skilled cybersecurity professionals
  - 61% state that there is insufficient budget for cybersecurity
  - 75% observe that staying up to date with cybersecurity technology is challenging
- The most serious attack vectors in Japan (receiving a seriousness rating of 9 or 10 out of 10) are employee error, employee malicious acts, and poor systems design
- The top 3 frustrations experienced as relates to information or cybersecurity are:
  - There is not enough budget for cybersecurity
  - We struggle to employ skilled security specialists
  - We don't put enough time and investment into training our general staff
- The top technologies or issues Japanese security decision makers think will impact their organisation's security in the next 24 months are AI and machine learning, public cloud computing, and IoT devices

"I have consulted on several AI projects and proof of concepts. There is certainly a gap between the hype and reality. Many organisations simply haven't achieved the outcomes they expected. That said, we do see opportunity for AI in security."

"We expect a rise in the number of attacks that target our systems in order to get to our customers as we get closer to Tokyo 2020 Olympics. Supply chain attacks are a serious issue and will only get worse."

"A lot of our customers are hardening their security stances as they move to cloud. And they should – it is a different way of operating."

Cybersecurity in Malaysia

- 32% of Malaysian organisations say they have been breached in the past 12 months
- 3% of Malaysian firms have no cybersecurity maturity, 5% say their approach is untested and 2% say their approach is ad hoc
- Two thirds (51%) of Malaysian respondents feel their organisation does not have a cybersecurity team in place that could properly detect, investigate and respond to threats
- Skills, education and resources
  - 72% struggle to recruit skilled cybersecurity professionals
  - 60% state that there is insufficient budget for cybersecurity
  - 83% observe that staying up to date with cybersecurity technology is challenging
- The most serious attack vectors in Malaysia (receiving a seriousness rating of 9 or 10 out of 10) are phishing, malware, and ransomware
- The top 3 frustrations experienced as relates to information or cybersecurity are:
  - Executives assume our company will never get attacked
  - Executives assume our company will get attacked but there's nothing we can do to stop it
  - Executives assume cybersecurity is easy and cybersecurity professionals over exaggerate threats and issues
- The top technologies or issues Malaysian security decision makers think will impact their organisation's security in the next 24 months are digitisation of processes and workflows, IT/OT convergence, and public cloud computing

"We are setting up smart factories with lots of IoT sensors and automation. We know this is going to create more vectors for attack and data that we need to protect. Yet there is an ongoing challenge in getting the time and resources to secure things as we implement them."

"We of course do what we can to protect our systems and data to the best of our ability. But the reality is we know we are going to be attacked and it is really only a matter of time until we suffer a breach. What I would like is the capability to immediately know how and to what point in time we recover our systems to. That is the hard part – responding to incidents effectively."

Cybersecurity in Philippines

- 24% of Philippines organisations say they have been breached in the past 12 months
- 1% of Philippines firms have no cybersecurity maturity, 5% say their approach is untested and 4% say their approach is ad hoc
- Two thirds (44%) of respondents from Philippines feel their organisation does not have a cybersecurity team in place that could properly detect, investigate and respond to threats
- Skills, education and resources
  - 62% struggle to recruit skilled cybersecurity professionals
  - 60% state that there is insufficient budget for cybersecurity
  - 79% observe that staying up to date with cybersecurity technology is challenging
- The most serious attack vectors in Philippines (receiving a seriousness rating of 9 or 10 out of 10) are phishing, malware, and ransomware
- The top 3 frustrations experienced as relates to information or cybersecurity are:
  - There is too much noise regarding security
  - Cybersecurity is frequently relegated in priority
  - There is not enough investment and time into training general staff
- The top technologies or issues Philippines security decision makers think will impact their organisation's security in the next 24 months are AI and ML, IT/OT convergence, and digital transformation programs

Cybersecurity in Singapore

- 26% of Singapore organisations say they have been breached in the past 12 months
- 3% of Singapore firms have no cybersecurity maturity, 5% say their approach is untested and 3% say their approach is ad hoc
- Two thirds (46%) of Singaporean respondents feel their organisation does not have a cybersecurity team in place that could properly detect, investigate and respond to threats
- Skills, education and resources
  - 57% struggle to recruit skilled cybersecurity professionals
  - 45% state that there is insufficient budget for cybersecurity
  - 65% observe that staying up to date with cybersecurity technology is challenging
- The most serious attack vectors in Singapore (receiving a seriousness rating of 9 or 10 out of 10) are ransomware (32%), malicious employees (31%), and AI/ML attacks (31%)
- 76% of Singapore firms say educating employees and leaders is their biggest challenge. 64% struggle to provide the education and awareness required.
- The top 3 frustrations they experience as relates to information or cybersecurity are:
  - Cybersecurity is frequently relegated in priority
  - There is not enough budget for cybersecurity
  - Lack of skilled security specialists
- The top technologies or issues Singapore security decision makers think will impact their organisation's security in the next 24 months are digital transformation programs, digitisation of processes and workflows, and following DevOps methodologies

Steps to Consider

TRA offers the following steps as a starting point for improving cyber and information security effectiveness beyond existing technical-based maturity frameworks. They are not intended to be exhaustively comprehensive or to act as a silver bullet. Every organisation is different and these steps should not replace proper due diligence. However, we trust they stimulate new thinking for informing your future approach. They are presented in no particular order.

- Get a holistic health check and review KPIs to make sure they include non-technical metrics. It is important to go beyond your common penetration testing experiences that commonly focus on technical capabilities or vulnerabilities. You may benefit from getting an external party's perspective and advice.
- Review partners and supply chain risks. It is increasingly evident that the partners you work with are a potential attack target. What mechanisms do you have in place to ensure partners are meeting your security expectations and requirements?
- Ensure all new product and services development is done with security by design. Ensure your security experts are part of all new development projects at the first stage and security is considered a competitive advantage (not a hindrance).
- Be transparent and bring security discussions out of the shadows. The history of recent data breaches and security incidents suggests transparency and honest, regular communication while fixing or remediating issues can help turn negative situations into positive outcomes.
- Consider regular hackathons or design thinking workshops for security-related issues. Set education and skills as key objectives and goals for these activities. Also ensure you have non-IT or non-security stakeholders involved from the lowest to the highest levels of the organisation.
- Encourage and enable employees to undertake security-related training and courses. There are many excellent online courses and resources available. Providing incentives for employees to do this may help and will ensure that traditional training mechanisms and communication is enhanced. Positive gamification can also help boost awareness.
- Cultivate and embrace a new security culture to make it part of your DNA and value proposition. This will require a long-term commitment from executives down to all levels of employees. It will require compelling communication programs and a "walk the talk" mentality.
- Use a discovery team to get ahead of emerging technology in cybersecurity, especially the use of artificial intelligence and machine learning. Establish or enable a multi-stakeholder team to discover, discuss, plan and report on opportunities and risks you face. This team should be fluid and involve individuals from various parts of the organisation and change frequently. Use them as ambassadors for an improved security culture.

- Benchmark against industry peers and share best practices. Consider whether you can formalise an exchange of information and insights between similar organisations as your own to uncover different ways of improving in non-technical areas.
- Get ahead of privacy and compliance and ensure all of your people are familiar their obligations. Privacy legislation, especially PII (personally identifiable information, i.e. customer/consumer/constituent data) is changing globally. Ensure all areas of your business are aware of how privacy requirements may impact their roles.
- Automate as much as possible – but do so with your people, not to them. The hoary adage of working smarter, not harder applies just as much to cyber and information security as anywhere else. However, keep in mind that before automating areas like manual processes, notifications, and data analysis, you should optimise the process involved in collaboration with the people it affects.
- Brace for continued regulatory changes and pressures. Certain countries such as Australia, New Zealand and Singapore are mooting additional, stronger changes to data privacy laws for consumers/citizens. Even in Asian countries not typically associated with robust data privacy and breach laws, there is growing momentum to strengthen compliance and legal requirements.
- What happens when you do suffer a data breach? Ensure you have pre- and post-breach plans that address key issues such as reporting lines, who has authority to speak publicly if required, who leads the incident response team and what is your internal communication plan? The external plan? What are your service provider agreements?

A view from Sophos

The following is the opinion of the report sponsor, Sophos, and not TRA

Security is hard. We all know it. What does it really mean to "be secure"? Ultimately, security is about managing risk. To do that effectively, you must be able to identify key areas where your actions will have an outsized impact on protecting your organisation, your employees and the data your company has been entrusted with.

This process starts with being able to measure what is happening on your network, servers and databases, wherever they might be. Then, you analyse that data to begin to look for anomalies or unexpected behaviours. This requires knowledge of your business, but more importantly, a comprehensive understanding of attack techniques and playbooks: which things are important and which things are simply bumps in the road.

According to the survey, more than 60 per cent of respondents said they struggle with security education, recruiting skilled staff, and staying up to date with the evolving threat landscape. This is not a good foundation for effective risk management. It also contradicts respondents' perceptions of the maturity of their security programs.

All of this has resulted in a lack of visibility into security risk and an overestimation of respondents' ability to defend their organisations. On average, less than one third of respondents believed their organisations had been the victim of a breach in the last year, whereas anecdotal evidence suggests this number should be close to 100 percent.

The role of the IT channel

Sizeable gaps exist in finding security expertise and in staying up to date with technology, and this represents a huge opportunity for the channel. Right now, organisations in APJ most commonly engage vendors for point solutions in traditional outsourcing/licensing contracts. However, in the next 24 months, organisations predict they will engage vendors and service providers on multi-year contracts for holistic solutions and licensing contracts – suggesting that the channel has a growing role to play in these businesses' security journeys.

However, there is a growing requirement by organisations for the channel to do more. Respondents want partners to demonstrate that they understand their business and are looking for partners to provide comprehensive end-to-end support. To stay relevant, channel partners must pass on the expertise they learn from their trusted security vendor advisors to their customers and help educate them about best practices and innovative technologies that will keep their organisations secure.

The rapid pace at which cybercriminals are advancing cyberattacks leaves no room for error. The channel must take on the role of educator to help drive proactive approaches to cybersecurity

You can't find what you are not looking for, and if those responsible are understaffed and lack knowledge of the current threat landscape, all they can do is put out obvious fires and hope for the best. This has led to incredibly high rates of burnout among security professionals and the misconception in management that everything is being handled, so business continues as usual.

The report reflects the challenge security professionals have when talking to business leaders with two in three respondents struggling to convince the business that security must be a priority. Across the region there is a perception at the C-level that security isn't that hard, and you can just buy another magic box and make the threat go away.

Proactive security is essential and one of the key indicators of a mature security program. Unfortunately, many respondents indicated security was only a priority to management and the board during active incidents. This leads to a reactive security posture that waits until it is too late to invest in critical security controls and training. Unlike physical possessions, there is no ability to recover stolen data once it's gone. Increasingly strong penalties from regulatory authorities should be a strong incentive to change this behaviour.

Underequipped, underfunded and undereducated security teams are unlikely to be able to detect breaches in their most critical early stages. Today's security teams need to understand that they cannot solely rely on prevention for all threats and that detection and response are key. This requires having the tools to effectively find suspicious activity and access to a network of security knowledge to interpret that information and lead them to appropriate corrective action.

Today's attacks are a different breed, and as usual cybercriminals are looking for the weakest link to prey upon. What's different this time is that the attacks are being executed, in part, directly by human hands. No algorithm or machine will stop a human with the time and incentive to breach your security.

Sophos refers to these attacks as automated, active attacks. The digital thieves have created automated systems to allow their crimes to scale by finding organisations that have left the door ajar with regards to their security. After they identify the weakest in the herd, a human takes over to exploit the victim by hand to impose the greatest possible amount of pain to profit from their desperation. If you thought defending against bots, worms and Trojans was tough, you don't want to see the pain a determined malicious person can inflict.

Appendix

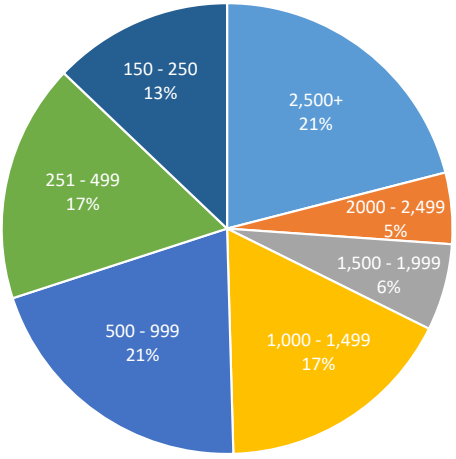
Definitions for the Cybersecurity Maturity Model:

- No plan: As it reads – there is no cybersecurity capability in place
- Ad-hoc: Reactive to specific projects and initiatives but no overall strategy to govern activities
- Untested in real life: Theoretical plan that has yet to be implemented within the organisation, group or division
- Managed: Basic level strategy in place that ensures projects and activities are undertaken in a planned manner with basic performance, measurement and controls in place to track progress
- Defined: Capability is proactive rather than reactive and organisation-wide with appropriate guidance for projects and activities in a co-ordinated program
- Quantitative: Capabilities, performance and assessment are metrics-based with quantified objectives that are aligned to company cybersecurity strategy and goals
- Optimised: Focus on continuous improvement cycles with a proven ability to adapt to change

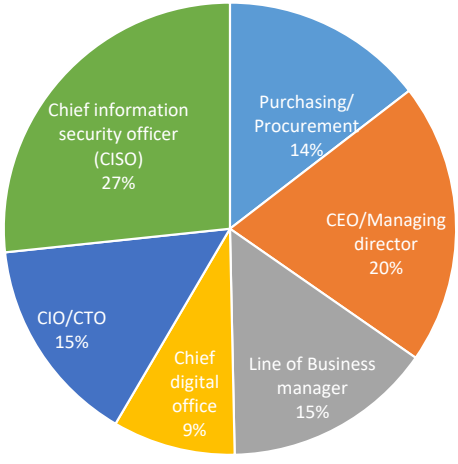
Demographics & Methodology

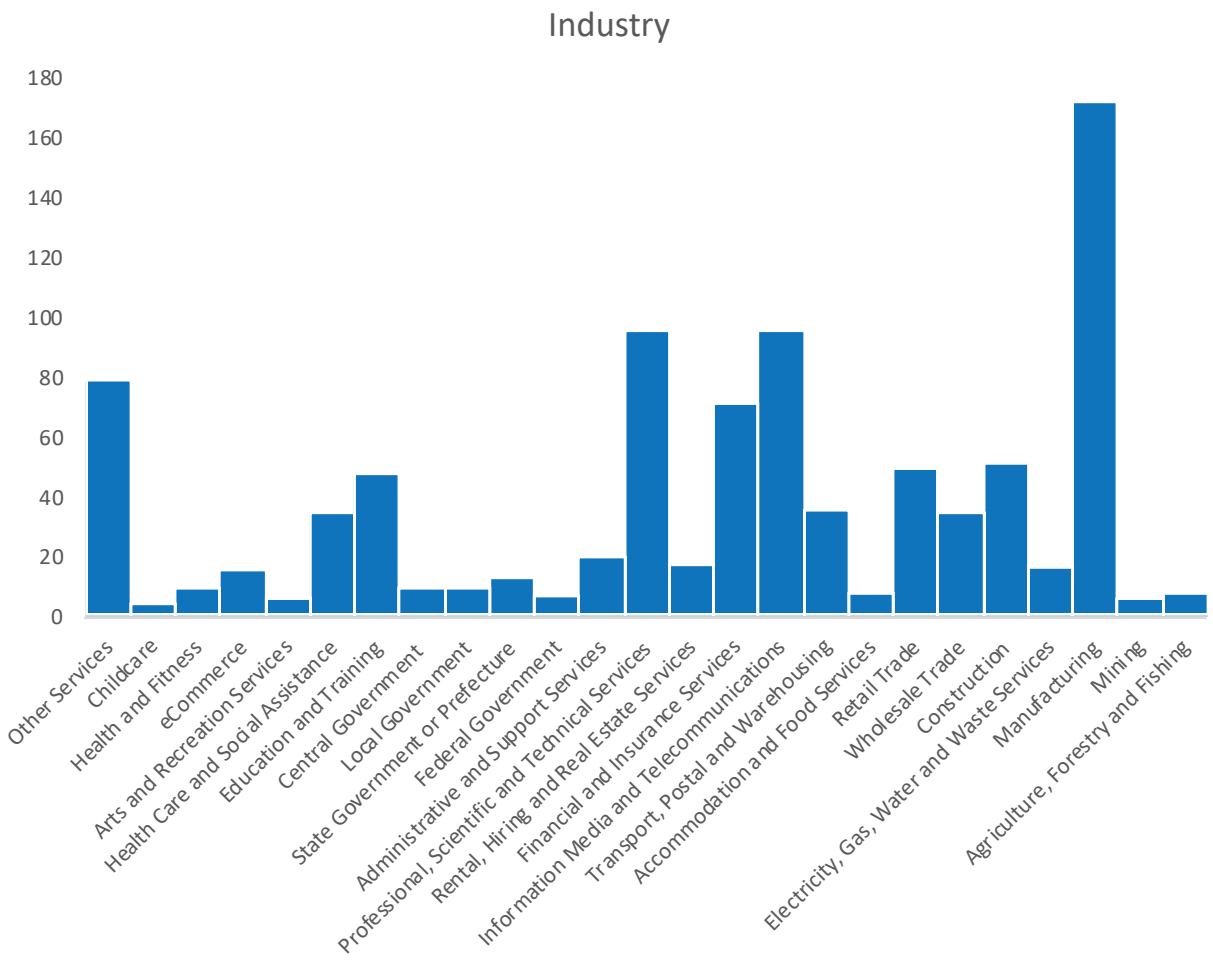
In February 2019 Sophos commissioned Tech Research Asia (TRA) to undertake research into the Asia Pacific and Japan cybersecurity landscape. This included a major quantitative component with a total of 900 responses captured – 100 each in Malaysia, Philippines and Singapore, and 200 each in Australia, India and Japan. The demographics of these respondents are included below in chart form. In addition, TRA facilitated four executive roundtable events in Malaysia, India, Japan and Australia where qualitative insights were gathered. For any further questions on the methodology used in this research please contact TRA.

Number of Employees



Role





About Sophos

As a worldwide leader in next-generation cybersecurity, Sophos protects nearly 400,000 organisations of all sizes in more than 150 countries from today's most advanced cyberthreats. Powered by SophosLabs – a global threat intelligence and data science team – Sophos' cloud-native and AI-enhanced solutions secure endpoints (laptops, servers and mobile devices) and networks against evolving cybercriminal tactics and techniques, including automated and active-adversary breaches, ransomware, malware, exploits, data exfiltration, phishing, and more. The award-winning Sophos Central cloud-based platform integrates Sophos' entire portfolio of best-of-breed products, from the Intercept X endpoint solution to the XG Firewall, into a single system called Synchronized Security. Sophos products are exclusively available through a global channel of more than 47,000 partners and Managed Service Providers (MSPs). Sophos also makes its innovative commercial technologies available to consumers via Sophos Home. The company is headquartered in Oxford, U.K., and is publicly traded on the London Stock Exchange under the symbol "SOPH." More information is available at www.sophos.com.

About Tech Research Asia

TRA is a fast-growing IT analyst, research, and consulting firm with an experienced and diverse team in Sydney | Melbourne | Singapore | Kuala Lumpur | Hong Kong | Tokyo. We advise executive technology buyers and suppliers across Asia Pacific. We are rigorous, fact-based, open, and transparent. And we offer research, consulting, engagement and advisory services. We also conduct our own independent research on the issues, trends, and strategies that are important to executives and other leaders that want to leverage the power of modern technology. TRA also publishes the open and online journal, TQ.

www.techresearch.asia

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

18-08-08 WP-NA [MP]

SOPHOS