SOPHOS
Cybersecurity delivered.

The Future of Cybersecurity in Asia Pacific and Japan

3nd Edition, April 2022

A TRA report sponsored by Sophos

A Sophos Whitepaper. April 2022

Contents

Introduction

Welcome to the 3rd edition of the "The Future of Cybersecurity in Asia Pacific and Japan". First published in 2019, the reports examine cybersecurity issues confronting businesses throughout the region.

Not confined to attack vectors and vulnerabilities, our report series has always looked beyond cybersecurity technologies to broader issues such as maturity levels, budgets, awareness, education and training, and other practical factors shaping how companies manage their cybersecurity environment.

As with previous editions, this year's report provides a snapshot of business' views of three key issues:

- Cybersecurity strategy and execution
- Education and skills
- Defending against threats

This year we also expanded our focus to include issues relating to:

- Educating the board
- The cybersecurity skills shortage and those areas most in demand
- The most frequent attack vectors experienced by our research group
- The importance of threat hunting to companies' defence strategies

Drawn from a survey of 900 cyber and cybersecurity decision makers in Australia, India, Japan, Malaysia, the Philippines and Singapore, the research revealed a number of key findings:

Cyber Strategy and Execution

- **Spending is up, just**. On average, cybersecurity spending represents 11% of 2022 technology budgets, an increase from previous years.
- **Maturity ≠ capability**. Cybersecurity maturity levels continue to rise yet organisations continue to struggle with the same issues year on year. Either the self-assessed maturity levels are too optimistic or there are some serious systemic issues that are yet to be addressed.
- **Cybersecurity is not a part-time responsibility**. There is a clear trend of companies appointing dedicated security specialists rather than subsuming security responsibilities within the roles of current IT professionals.

Education and Skills

- **The cybersecurity skills shortage is here to stay**. 73% of companies expect to have difficulty recruiting cybersecurity employees in the coming two years.
- **Board level education is critical**. Only 40% of companies believe their board truly understands cybersecurity and the top frustration cybersecurity professionals experience is that the board and executive level assume that the company will never get attacked.
- **Vendors have a role to play in educating boards and executive teams**. 60% of respondents do not believe cybersecurity vendors fully provide them with the right information to help educate their boards and executive suites.

- **Outsourcing or keeping in-house?** The approach depends on the need. Strategy development, data management and compliance, and PII management remain mostly in-house. Operations such as threat hunting, remediation, incident response and penetration testing are typically outsourced or follow a blended mix of do-it-yourself and outsourced.

Defending against Threats:

- **Threat hunting is key to defence**. 90% of our respondents are using threat hunting as a means of protecting their organisation. 85% of current users rate it as 'important' or 'critical' to a successful cybersecurity capability.
- **Today's top attack vectors are** phishing, credentials, supply chain vulnerabilities, unpatched vulnerabilities, and malicious employees.
- **Tomorrow's top attack vector contents are similar to today, sort of**. Phishing, malware, poorly configured systems, corporate espionage and nation state attacks.

This report comprises three sections – the research findings, individual country insights containing key data points and considerations from the report sponsor, Sophos.

We sincerely hope the data and commentary provide you with insights as you consider your organisation's cybersecurity capabilities and environment.

The Research Findings

The research results are presented in three sub-sections, each with important data and findings highlighted:

1. Cybersecurity Maturity, Strategy and Execution
2. Education and Skills
3. Strengthening Defences

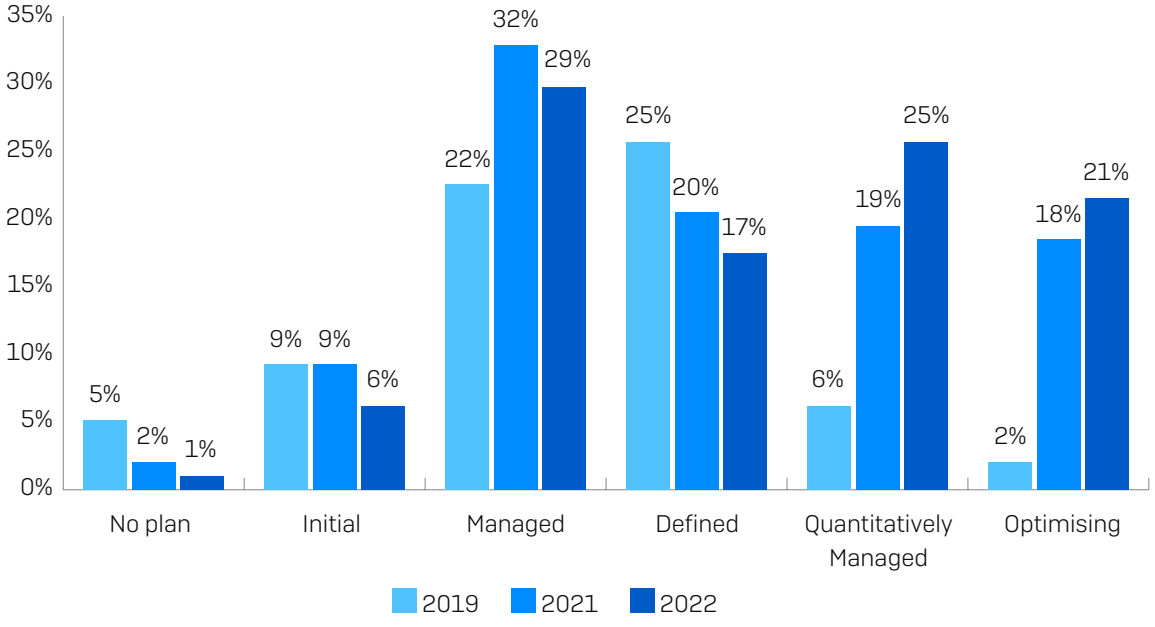
Cybersecurity Maturity, Strategy and Execution

Maturity

Since 2019, we have asked respondents to self-assess their cybersecurity maturity (the assessment criteria definitions can be found in the appendix) and they have reported continued improvements in their maturity levels, capabilities and understanding of the cybersecurity landscape.

Indeed, the 2022 data shows that 21% of companies surveyed believe themselves to be at the top level of maturity ('optimising'), a stark increase from the first edition of this report in 2019 when only 2% felt they were at that level.

Cybersecurity Maturity Level 2019-2022 (Self-Assessed)

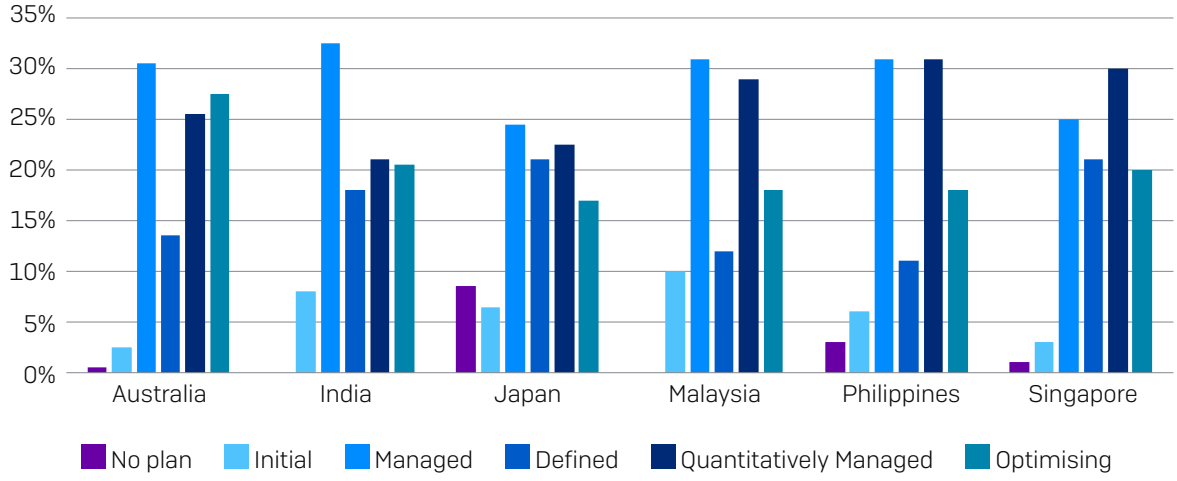


The chart clearly indicates a right shift over time towards higher levels of maturity, however it is interesting to take a closer look at individual countries, revealing that:

- Australia's profile shows the highest percentage of organisations considered mature (28%) yet also a relatively high level of those still developing capabilities (31% 'managed').
- India shows clear progression towards increased maturity with a similar profile to Australia of 'optimising' and 'managed', weighted more towards 'managed'.
- Japan's data reveals that 9% of companies have 'no plan' and a further 7% are in the 'initial' stage of developing capabilities.

- Similar to India, Malaysia shows 31% of companies are at the 'managed' level and has the highest percentage of all countries at the 'initial' stage, 10%.
- Philippines shows the highest level of organisations in the 'quantitatively managed' stage with 31%, suggesting that the companies in the country should continue their good progress towards 'optimising' in the coming year.
- Singapore arguably ranks second in maturity, just behind Australia with 50% of all respondents ranking themselves as either 'quantitatively managed' or 'optimising'.

Cybersecurity Maturity Level 2019-2022 (Self-Assessed) by Country, 2022



It is pleasing to see ongoing improvements in maturity levels. At the same time, we harbour a concern that companies are too optimistic with their self-assessment and offer two observations in support of this:

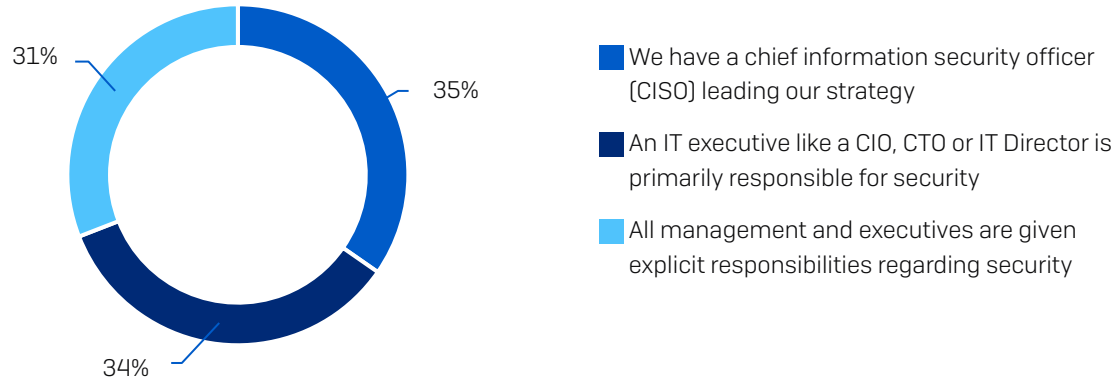
1. First, as we will see in the next section, with some respondents, there appears to be a reactionary tendency to change cybersecurity strategies after a breach or attack, creating an 'attack, change, attack, change …' cycle.
2. Second, despite ongoing improvements in maturity, of the common frustrations experienced by cybersecurity professionals, the data suggests that it is not technology solutions but rather misconceived assumptions and misunderstandings regarding the threat environment. I.e. issues related to education and awareness.

We're certainly not suggesting cybersecurity strategy and education are 'do once and forget' approaches, yet we are concerned that organisations are doing themselves a disservice by assigning artificially high levels of maturity and creating a false level of optimism around their capabilities.

Strategy and Execution

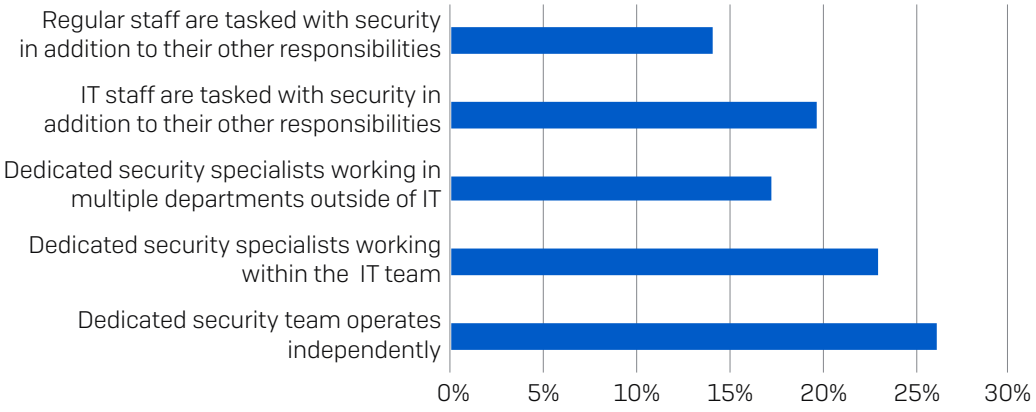
Chief Information Security Officers (CISOs) lead strategy in 35% of organisations with another 34% of respondents stating that IT executives (CIO, CTO) are responsible. 31% of companies follow a blended model with responsibilities spread across others in the executive and management group. This has remained relatively stable since our first report in 2019.

Who Leads Cybersecurity Strategy?



Our data also reflects appointing dedicated operational cybersecurity staff is preferred to tasking 'regular' IT staff or other non-security employees with security in addition to their other responsibilities.

How does your organisation approach cybersecurity operations?



Looking at how companies assign responsibilities between inhouse, outsourced or a combination of the two varies considerably depending on the tasks required. What can be said is that no requirement shows a majority choice of 'in-house' and in many cases a 'better together' ethos combining outsourced and in-house is evidenced.

Broadly speaking, strategy development, education and data management, and compliance are marginally preferred in-house. Compared to 2021 when we stated – *"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."* – this in-house preference has decreased in 2022.

Areas relating to defending and recovering from attacks (e.g. penetration testing, incident response, threat hunting, remediation, etc) show preference for either a directly outsourced or blended approach.

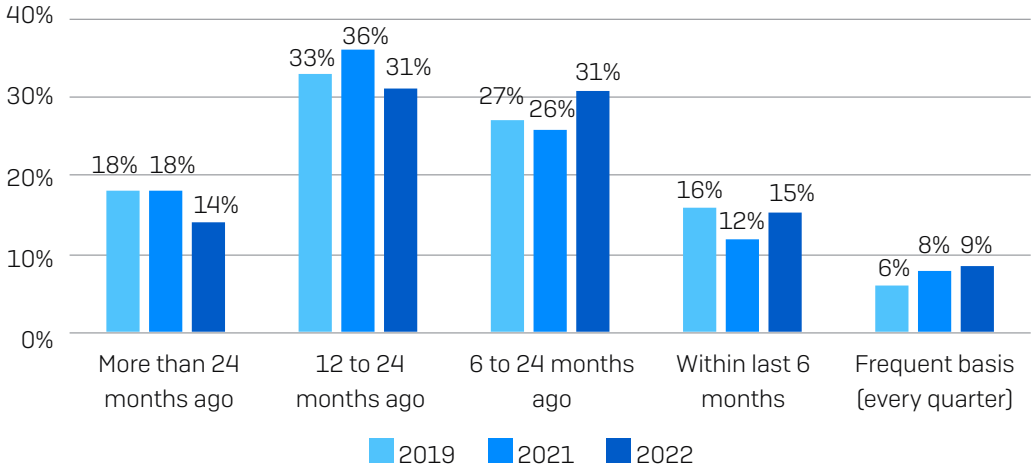
Changes in Strategy

Our last finding within this section considers the reasons for, and frequency of, changes in cyber-security strategy. Respondents were asked when they last made a significant change in their approach and why.

In contrast to data from 2019 and 2021, 2022 data highlighted that organisations are making more changes in a shorter time:

- 31% made changes in the last 7-12 months
- 15% within the last 3-6 months
- 9% make frequent changes every quarter

When was the last time you made a significant change in your information or cybersecurity approach? 2019-2022



The primary factor causing organisations to change their cybersecurity strategy is experiencing an attack or breach in their own environment or in another organisation.

We also saw this when we asked organisations when they will next review and potentially change their strategy. 16% said they will make quarterly changes and another 33% said they will make a change in the coming 4-6 months. Why? Again, due to attacks experienced.

This factor has held the top spot so far in every edition of the research whilst other considerations including changing overall technology strategy, adoption of a new technology solution, budget issues, digital transformation programs, the impact of regulator changes, etc have all fluctuated in their importance.

We cannot help but consider if companies are stuck in a cybersecurity spiral: the more attacks, the more potentially reactionary changes come into play creating a cycle of new threat, new change, new tool, new threat … and repeat.

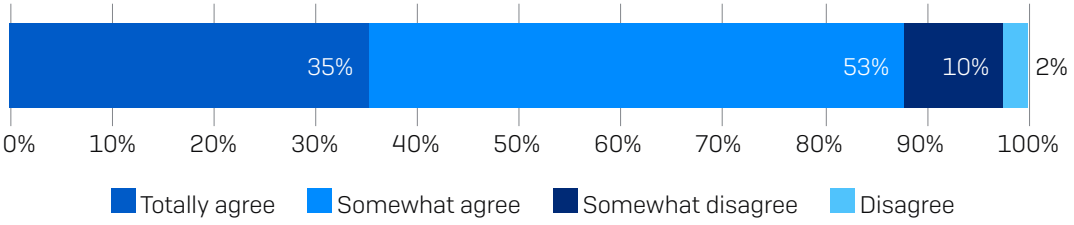
In some instances, a lack of understanding of cyber realities by non-cybersecurity professionals and executives exacerbates the problems of the security spiral and it is the issue of education and skillsets, which we will now look at.

Education and Skills

As a preface to this section, we asked our research participants to rate their level of agreement with the following statement, *"The biggest challenge to our security in the next 24 months will be the awareness and education of our employees and leadership"*.

- 35% of companies 'totally agreed'
- 53% of companies 'somewhat agreed'
- 12% of companies 'disagreed'

Please rate your agreement with the following statement: The biggest challenge to our security in the next 24 months will be the awareness and education of our employees and leadership



No wonder then that we see this issue arise in many of the common frustrations cybersecurity professionals experience in their roles.

Common Strategy and Operational Frustrations

In previous reports, we have asked cybersecurity professionals what frustrates them most about their company and its experience with security.

This year our top 5 saw significant upward movement in 4 of the 5 factors and we broadly consider the majority are related to frustrations around awareness, perception, messaging and education.

1. **Wishful thinking or blissful ignorance**. 'Executives assume we'll never get attacked'. Regardless of wishful or blissful, the top frustration is a view through rose-tinted glasses that 'it will never happen to us'. Until it happens … usually triggering a change in strategy and subsequent disruption.
2. **Lack of skilled security specialists**. 'We can't employ enough skilled security specialists.' Specialists can be expensive and keeping the ones you have from being poached, even more so. Yet companies don't put enough investment and time into training and educating general employees to support security capabilities (see #6 in the table).
3. **We're all doomed and going to die (i)**. 'There's too much "fear and doubt" messaging making it hard to talk about cybersecurity.' The much-abused fear, uncertainty and doubt (FUD) messaging has regained its prominence after last year. It's hard to educate when the audience has their heads out the window looking for a non-existent meteor.
4. **We're all doomed and going to die (ii)**. 'Executives assume our company will get attacked but there's nothing we can do to stop it.' 'Ah yes, there's the meteor. We knew it was going to happen. Why didn't you stop it? While you're at it, clean up the mess immediately.'
5. **It's all moving too fast**. 'We can't keep up with the pace of security threats.' It's impossible to keep across everything that could happen so we'll do the best we can and revert to #1 on the list.

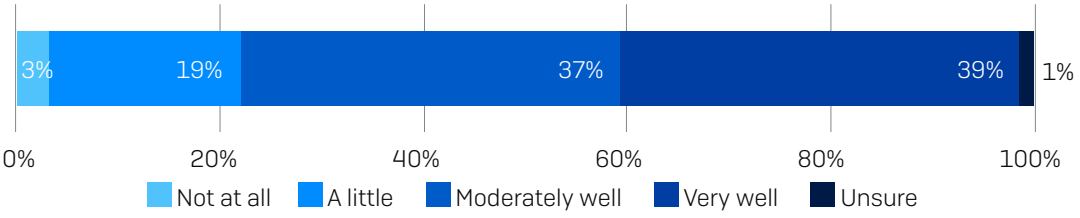
Top Issues Causing Frustration	2019	2021	2022
1. Our executives assume our company will never get attacked	7	7	1
2. We can't employ enough skilled security specialists	5	3	2
3. There's too much 'fear and doubt' messaging that makes it hard to talk accurately about cybersecurity	4	11	3
4. Our executives assume our company will get attacked but there's nothing we can do to stop it	10	8	4
5. We can't keep up with the pace of security threats	8	9	5
6. We don't put enough investment and time into training our general staff	6	6	6
7. There is not enough budget for cybersecurity	2	2	7
8. The executive team pay lip-service to cybersecurity but don't truly believe in it	9	5	8
9. There is too much noise regarding security	11	10	9
10. Our executives assume cybersecurity is easy and me/my cybersecurity peers over exaggerate threats and issues	3	1	10
11. Cybersecurity is frequently relegated in priority	1	4	11

With the exception of lacking skilled security specialists (ranked #2 in the previous table), we'd suggest the other top 5 factors are addressable through concerted education and awareness programs, starting at the board and executive level and flowing through to the rest of the organisation.

There's just one issue with that approach: our data suggests cybersecurity professionals perceive low levels of security understanding amongst their company's board.

Approximately only 4 in 10 cybersecurity professionals believe their company board truly understands cybersecurity. This issue is compounded by our research data that shows 22% of respondent companies had boards that require monthly or quarterly updates on cybersecurity (and this number is expected to increase to 26% of boards in 2024).

In your opinion does your company board truly understand cybersecurity?

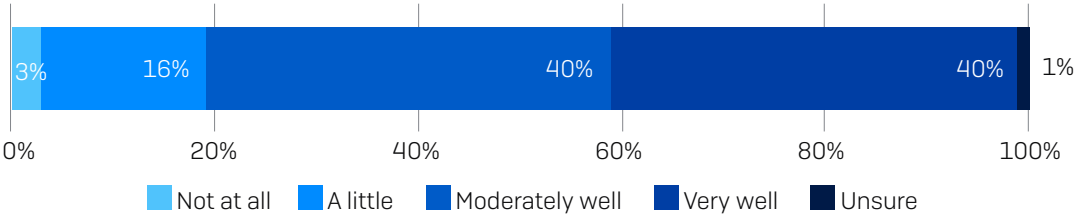


It is unclear as to what percentage of those boards really understand the issues contrasted with those that are following a compliance, 'check-box' tick philosophy without truly comprehending the issues.

Regardless, there is definitely an educational need to address here. In many instances, companies look to vendors or a mix of internal resources and vendors to help educate, especially in areas such as strategy, awareness and training.

Our data suggests that whilst vendor intentions are honourable, the outcomes are not quite as hoped for: only 40% of companies feel their cybersecurity vendors provide the right information to help educate the board about cybersecurity.

Do you feel your cybersecurity vendors provide you with the right information to help educate your board about cybersecurity?



Of course, it's not just as simple as pointing the finger at vendors and decrying 'Aha, it's your fault!' There is a larger issue at play here where both business and technology executives have traditionally struggled to clearly communicate with each other pretty much since the first IT person plugged in an electrical cord and someone in the business said, 'Oh, what does that do?'

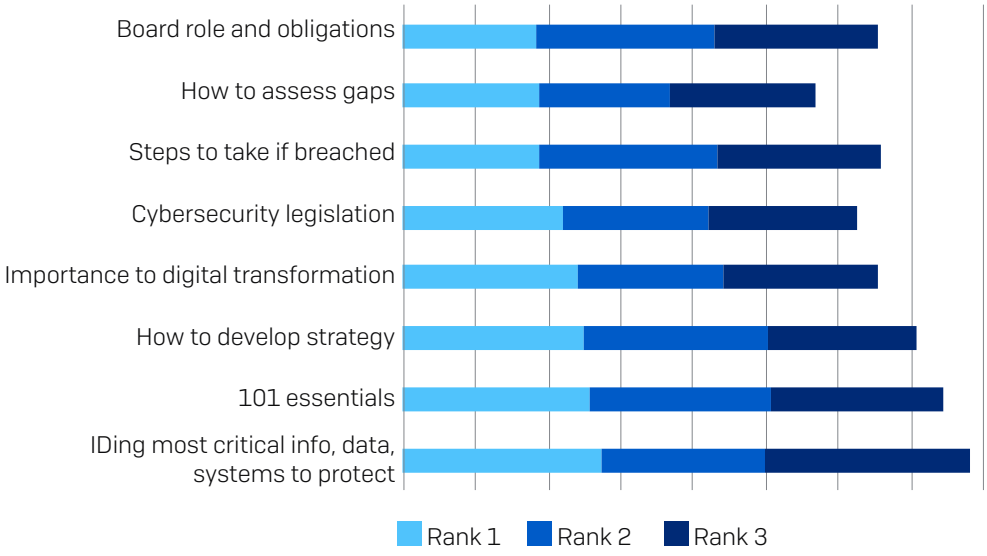
So, what are the key areas that require an educational focus?

The (very short) cybersecurity education issues to help educate list

This is a cascading approach that builds layer upon layer and provides a starting point for organisations considering their first steps.

1. **The crown jewels gambit**. The first priority revolves around helping boards understand that it's impossible to protect everything and it's more effective to focus on identifying the most critical information, data and systems to protect.
2. **We know what we want to protect, where do we start?** Cybersecurity 101 courses educate on basic principles, the genuine likelihood of attack, attack vectors, threat actors and other terminology that is second language to cybersecurity principals and sometimes mystifying to those who aren't.
3. **Strategy and implications on our digital transformation program**. With the basics clearly defined, developing the strategy and integrating with the inevitable digital transformation program is a critical consideration.
4. **The practicalities**. Once steps 1-3 are clearly articulated the focus becomes more operational in nature – what legislation is applicable, what to do if breached, ransom payment policy, gap assessments and future roles and obligations, etc.
5. **Compliance**. Underpinning many of the issues is the need to clearly understand compliance, the regulatory environment under which the business operates, what's legally required when breached and what are the appropriate controls around data security and management.

What information would you like to educate your company board?



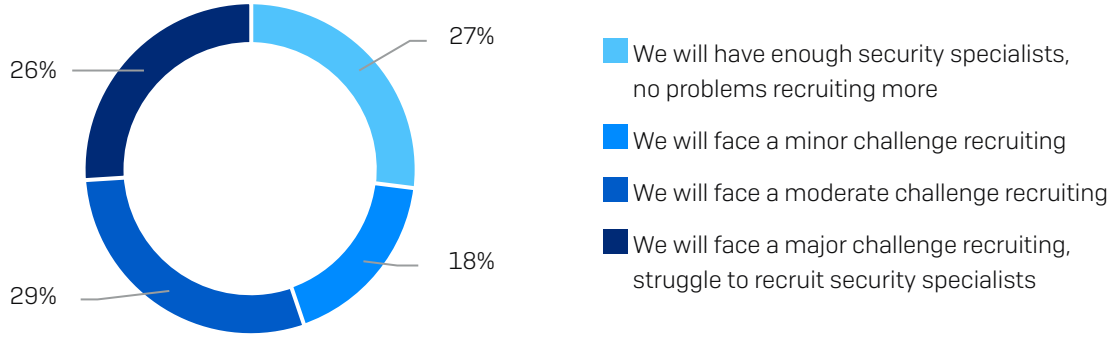
With the board education issue addressed, let's look at the one remaining issue in our top 5 frustrations, skills shortages.

Cybersecurity Skills

A new coverage area for this report, our data indicates a clear problem for our survey cohort with ongoing skills shortages. Given the impact of this issue, we will be incorporating analysis into future editions of the report.

On average, 73% of firms expect to have problems with recruiting cybersecurity employees over the coming 24 months (26% face a major challenge, 29% face a moderate challenge and 18% face a minor challenge).

What is your view on the availability of skills security employess for your organisation in the next 24 months?



Skills and Capabilities in Demand

Of course, the issue does vary considerably by country with Japan (35% of companies), Philippines (31% of companies) and India (29% of companies) expecting to experience major challenges recruiting in the coming 24 months.

Interestingly, another 38% of organisations in the Philippines expect no problems over the same period. Australia (31% of companies) and Malaysia (30% of companies) round out the top 3 countries expecting no issues with recruiting.

With recruiting being problematic, companies have clearly identified several areas where they would like to increase skills and capabilities for their internal security specialists:

1. Cloud security policies and architecture
2. 'Train the trainer' employee and executive cybersecurity training skills
3. Software vulnerability testing
4. Staying up to date with the latest threats
5. Policy compliance and reporting
6. Offensive security capabilities including threat hunting
7. Automation of incident handling
8. Forensic analysis
9. Edge computing security

The following table provides some greater insight into the top 3 skills priorities identified in each country:

	Priority 1	Priority 2	Priority 3
Australia	Knowledge of cloud security policies/architecture	Staying up to date with the latest threats	Employee and executive training
India	Knowledge of cloud security policies/architecture	Software vulnerability testing	Employee and executive training
Japan	Employee and executive training	Software vulnerability testing	Staying up to date with the latest threats
Malaysia	Staying up to date with the latest threats	Policy compliance and reporting	Employee and executive training
Philippines	Knowledge of cloud security policies/architecture	Software vulnerability testing	Staying up to date with the latest threats
Singapore	Knowledge of cloud security policies/architecture	Software vulnerability testing	Staying up to date with the latest threats

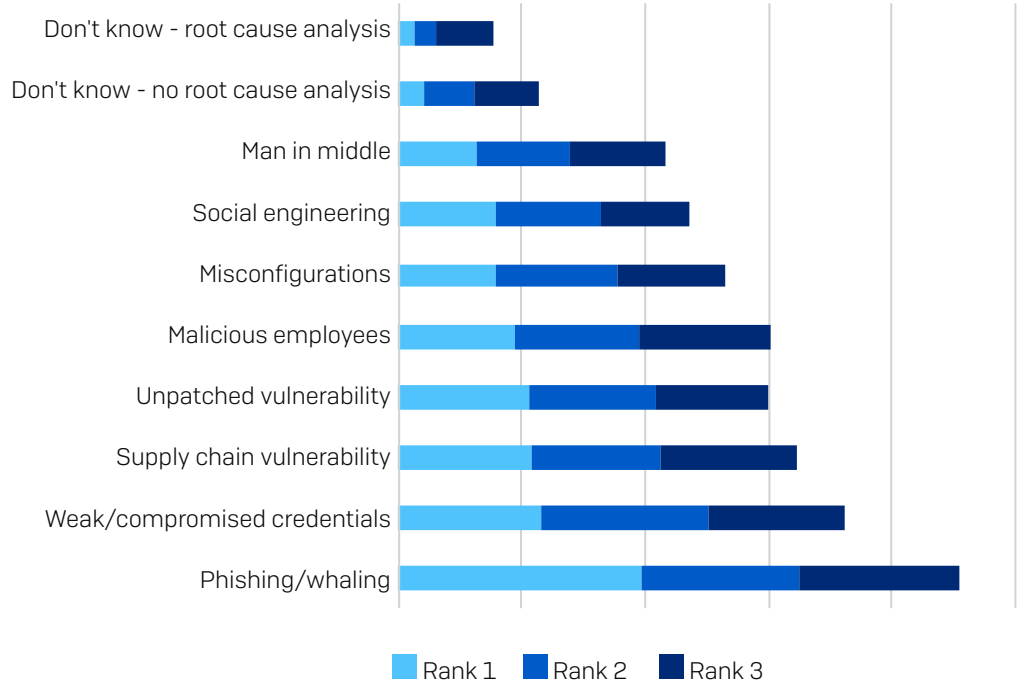
Strengthening Defences

Common Attack Vectors

Another new question for 2022, we asked organisations what were the most common security attack vectors their company experienced and, in a related theme, which threats they perceived as the most important now and in 24 months' time.

The first two vectors are addressable in part through ongoing education and awareness campaigns: phishing and whaling (where threat actors target the C-suite and board) and weak or compromised employee credentials.

What are the most common security attack vectors your company experiences?



From a country perspective, there was little variation in attack vectors, with companies from all 6 countries identifying phishing/whaling as the most prevalent activity.

	Vector 1	Vector 2	Vector 3
Australia	Phishing/whaling	Weak/compromised credentials	Supply chain vulnerability
India	Phishing/whaling	Weak/compromised credentials	Social engineering
Japan	Phishing/whaling	Unpatched vulnerability	Supply chain vulnerability
Malaysia	Phishing/whaling	Malicious employees	Supply chain vulnerability
Philippines	Phishing/whaling	Weak/compromised credentials	Malicious employees
Singapore	Phishing/whaling	Misconfigurations	Man in middle

Threat Landscape Rankings

As in previous years, we asked our respondents to rate which threats they perceived as the most serious to their organisation.

Consistent with our findings on attack vectors, phishing topped the list, followed by malware. Both threats have been ranked as either a top 1 or 2 issue in previous research and we were not surprised to see them again for 2022.

It was more noteworthy to consider the rise of 'poor systems' to third place, up from 13th in 2021. Its prominence raises an interesting question over the effectiveness of the 'security by design' approach adopted by many APJ organisations (casting another slight shadow over the actual cybersecurity maturity assessment levels raised earlier in this report).

Other noticeable ranking changes in 2022 include:

1. Malicious employees rising from 11th in 2021 to 7th in 2022
2. Social engineering falling from 4th (2021) to 9th in 2022
3. Distributed denial of service (DDOS) attacks dropping from 5th (2021) to 12th (2022)
4. Zero-day vulnerabilities falling from 8th (2021) to 13th (2022)

Threat Rankings	2019	2021	2022
Phishing and whaling	1	2	1
Malware	2	1	2
Poor systems	13	13	3
Corporate espionage	6	6	4
Nation state attacks	5	3	5
Encryption backdoors	4	7	6
Malicious employees	7	11	7
AI/ML attacks	10	12	8
Social engineering	3	4	9
3rd party errors	8	10	10
Employee errors	9	9	11
Distributed denial of service (DDOS)	12	5	12
Zero-day vulnerabilities	11	8	13

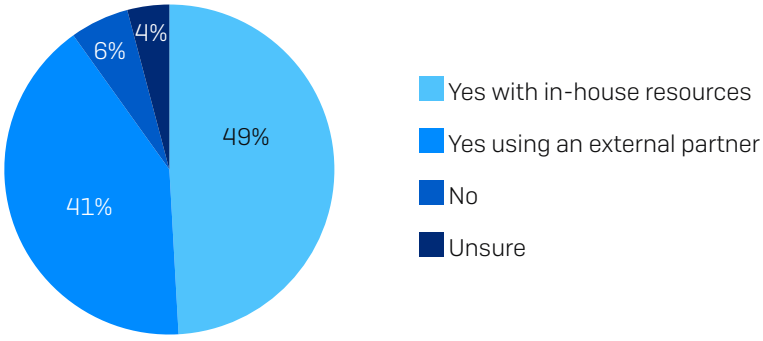
Threat Hunting Adoption and Importance

Alongside maintaining up-to-date security tools, active threat hunting emerged in this year's research as a key consideration for strengthening cybersecurity defences.

On average, across our survey cohort, 90% of organisations stated they undertook threat hunting to bolster their cybersecurity capabilities.

The story is one of overarching positivity for threat hunting across the region. 85% of all threat hunting users stated the approach is critical (21%) or important (64%) to their company's overall cybersecurity capability.

Does your organisation undertake threat-hunting activities to bolster its cybersecurity defence?



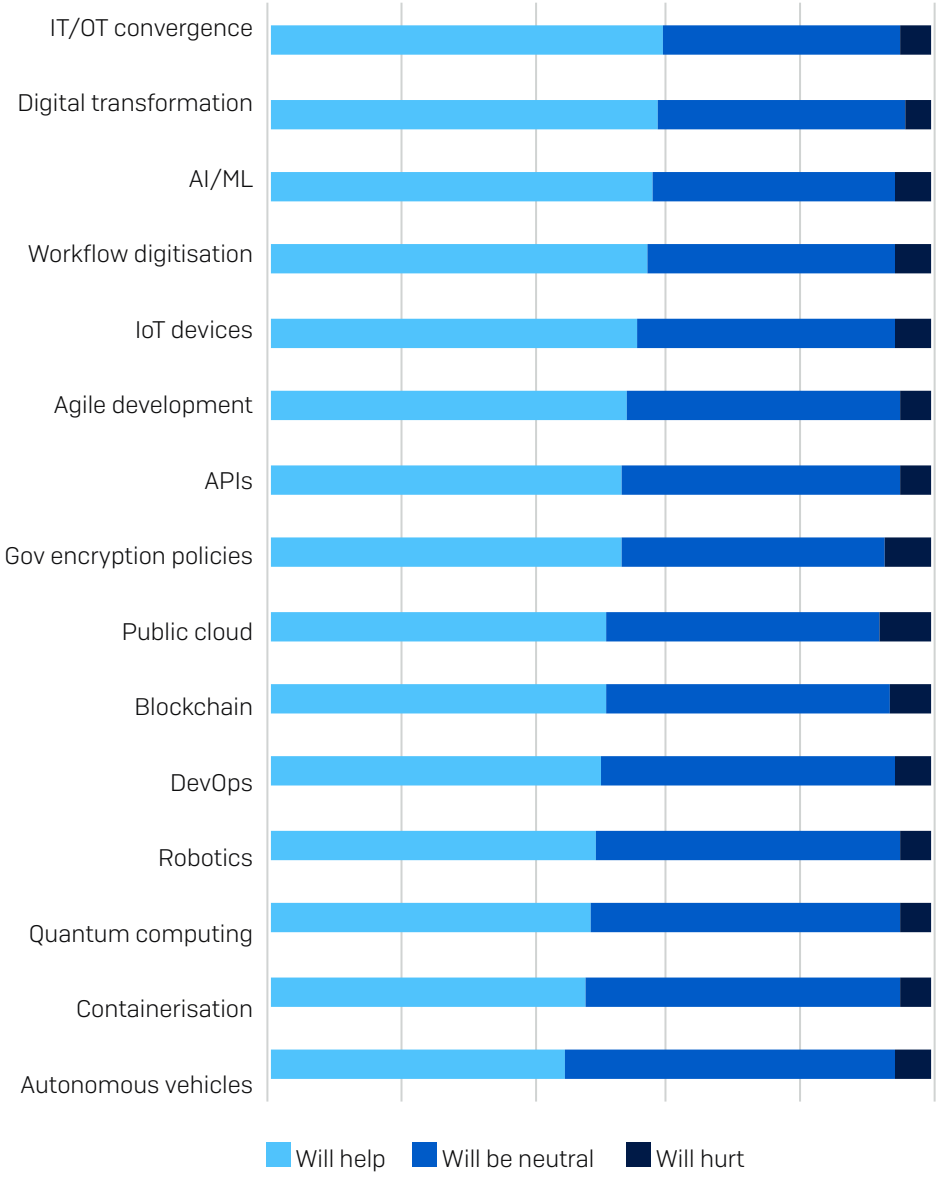
We would caution slightly against the ebullience in the data. Whilst not quantitatively tested, we made an observation that some users may consider log analysis, incident response, digital forensics, pen-testing and vulnerability assessments as valid examples of threat hunting consequently potentially inflating the adoption numbers.

Technologies and Issues Impacting the Cybersecurity Defence Landscape

Every year we ask our respondents which technologies or issues they think will impact their organisation's cybersecurity in the coming 24 months.

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 are IT and OT convergence, digital transformation, artificial intelligence and machine learning, workflow digitisation, and IoT devices.

Which of the following technologies or issues do you think will impact your organisation's security in the next 24 months?

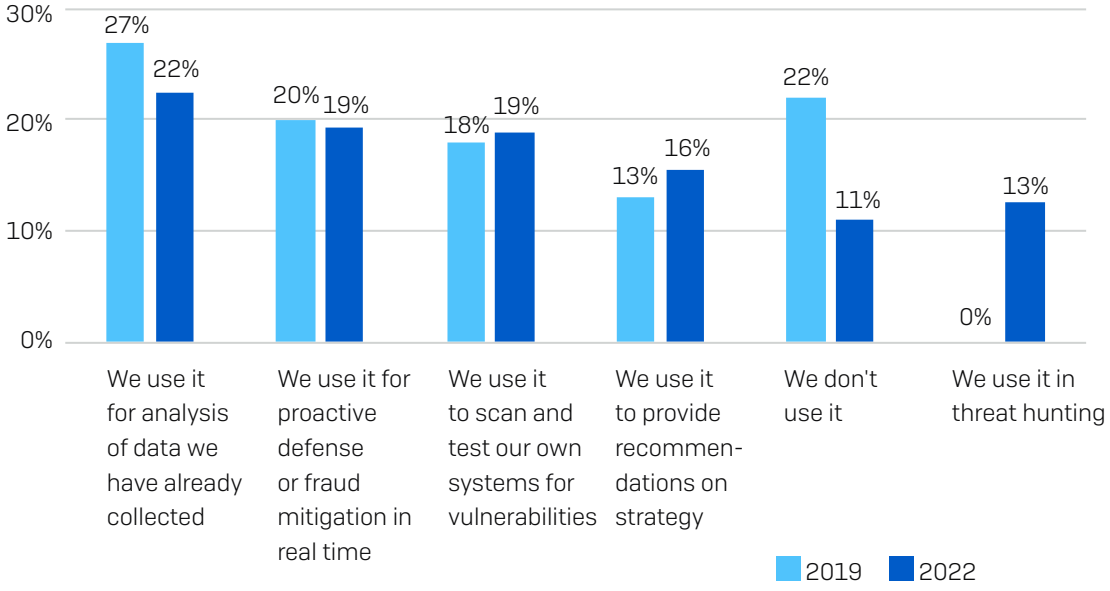


We were a little surprised to see containerisation (a way of encapsulating software code so it can run uniformly on any infrastructure) rank very low as an issue. Many organisations suffer from container sprawl in their cloud infrastructure and require a solution (such as Kubernetes) to effectively manage their environment. This, in turn, potentially increases the surface attack area as additional components are added. We expect to see containerisation rise in ranking as more large enterprises and government organisations continue their adoption.

In our 2021 report, we noted that, *"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."* Our latest data indicates fluctuation in the use of AI for data analysis and fraud mitigation and we expect this to continue year on year as the technology evolves and familiarity improves.

There is a clear trend towards increased adoption of AI and ML for other use cases and we expect it to be built into all security platforms more deeply going forward. Of note too is the overall decrease in the number of companies that stated they did not use AI and ML in 2019 (22%) and those that don't use it today (12%).

What is the role of AI and machine learning in your organisation's approach to security today?



In closing

The issue isn't technology. It's education.

Increasing spend on cybersecurity (be this on staff, managed security providers or technology) is sub-optimal unless organisations understand from the top down the true nature and critical threat that cybersecurity attacks constitute to an entities' existence, operational capabilities, and customers.

A true and frank assessment of actual cybersecurity maturity may give some organisations a pause for thought and possible rethinking of their true capabilities. Likewise, sustained and concerted board and executive level education campaigns are important to both improve management comprehension of cybersecurity issues and remove one of the major frustrations experienced by cybersecurity professionals.

In last year's conclusion we stated, ***"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 the future."*** That statement remains valid today.

The following sections of the report provide relevant data points for each of the 6 countries included in our research:

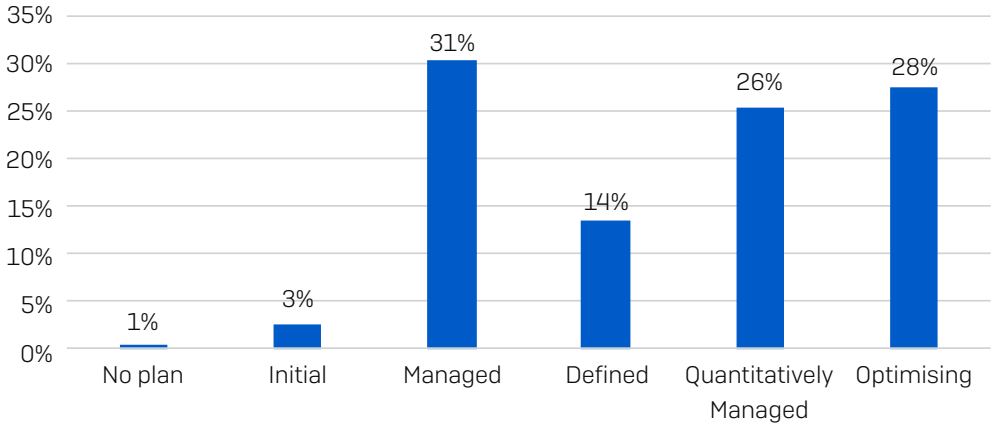
1. Australia
2. India
3. Japan
4. Malaysia
5. Philippines
6. Singapore

Cybersecurity in Australia

Spend on cybersecurity as percentage of total technology budget: 11.8%

Cybersecurity Maturity Profile

Cybersecurity Maturity Rating – Australia



Who leads cybersecurity strategy?

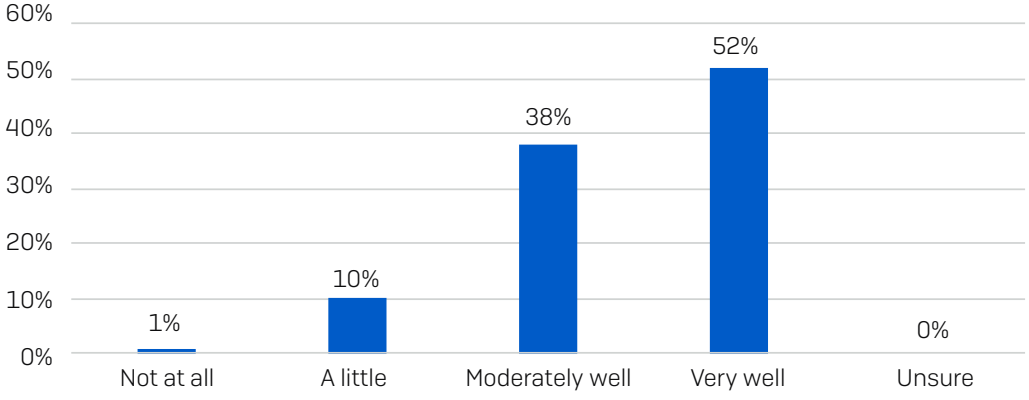
CISO: 38%, CIO/CTO: 32%, Shared Group Responsibility/Other: 29%

Top frustrations of cybersecurity professionals:

1. Cybersecurity is frequently relegated in priority
2. There is not enough budget for security
3. Our executives assume cybersecurity is easy and me/my cybersecurity peers over exaggerate threats and issues

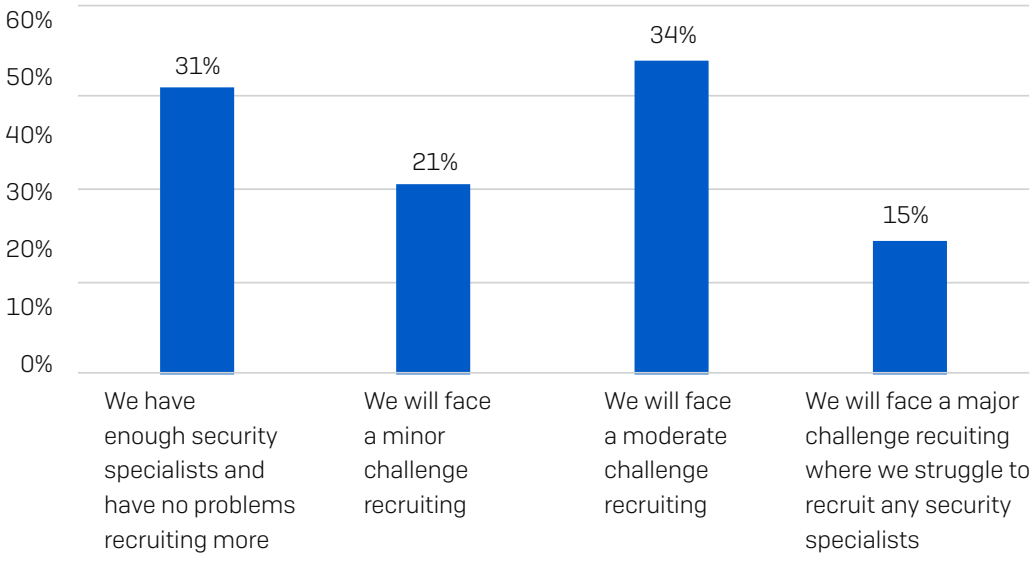
Board Level Understanding of Cybersecurity

Perceived Board Level Understanding of Security – Australia
How well do you think your company board understands cybersecurity issues?



Cybersecurity Professional Recruitment Difficulty Level

What is your view on the availability of skilled security employees for your organisation in the next 24 months? Australia



Top skills in demand:

1. Knowledge of cloud security policies/architecture
2. Staying up to date with the latest threats
3. Employee and executive training

Top attack vectors:

1. Phishing and whaling
2. Weak or compromised credentials
3. Supply chain vulnerabilities

Top rated threats in 2022:

1. Poorly designed systems
2. Malware
3. Phishing and whaling
4. Nation state attacks
5. Corporate espionage

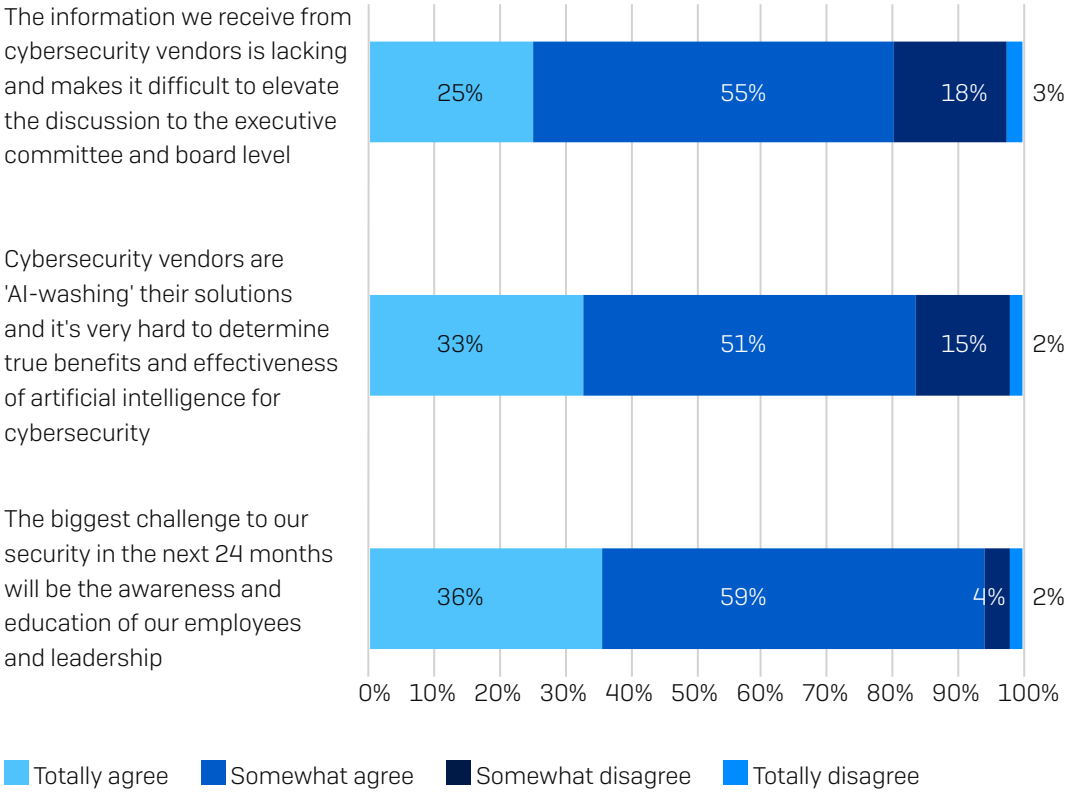
Rated threats 2021-2022

2021	2022
Malware	Poorly designed systems
Phishing and whaling	Malware
Ransomware	Phishing and whaling
Nation state	Nation state
Backdoors	Corporate espionage
DDoS	Encryption backdoors
Corporate espionage	Ransomware
Employee error	DDoS
Poorly designed systems	Social engineering
AI/ML attacks	Employee error
Partner/3rd party error	Malicious employees
Malicious employee	AI/ML attacks
Zero-day vulnerabilities	Zero-day vulnerabilities
Social engineering	3rd party error

Adoption of threat hunting

66% of companies do in-house, 31% use an external partner, 3% no/unsure

Please rate your agreement with the following statements – Australia

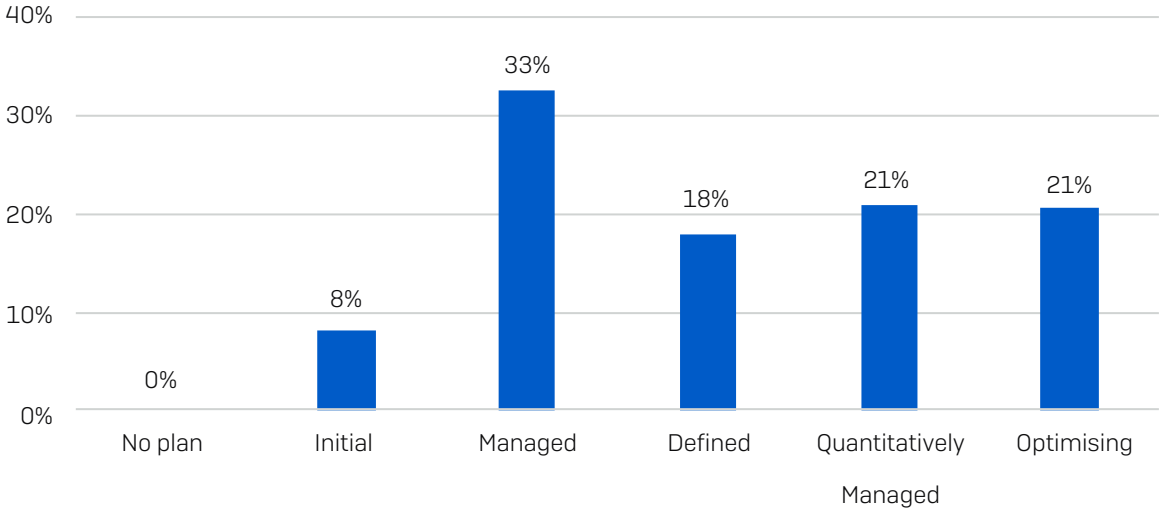


Cybersecurity in India

Spend on cybersecurity as percentage of total technology budget: 10.7%

Cybersecurity Maturity Profile

Cybersecurity Maturity Rating – India



Who leads cybersecurity strategy?

CISO: 34%, CIO/CTO: 34%, Shared Group Responsibility/Other: 32%

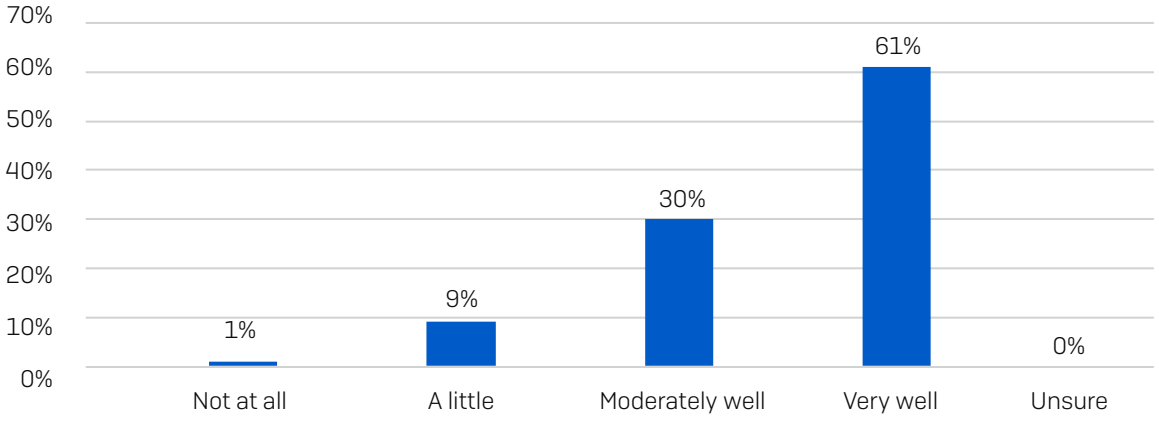
Top frustrations of cybersecurity professionals:

1. Our executives assume cybersecurity is easy and me/my cybersecurity peers over exaggerate threats and issues
2. There's too much 'fear and doubt' messaging that makes it hard to talk accurately about cybersecurity
3. Cybersecurity is frequently relegated in priority

Board Level Understanding of Cybersecurity

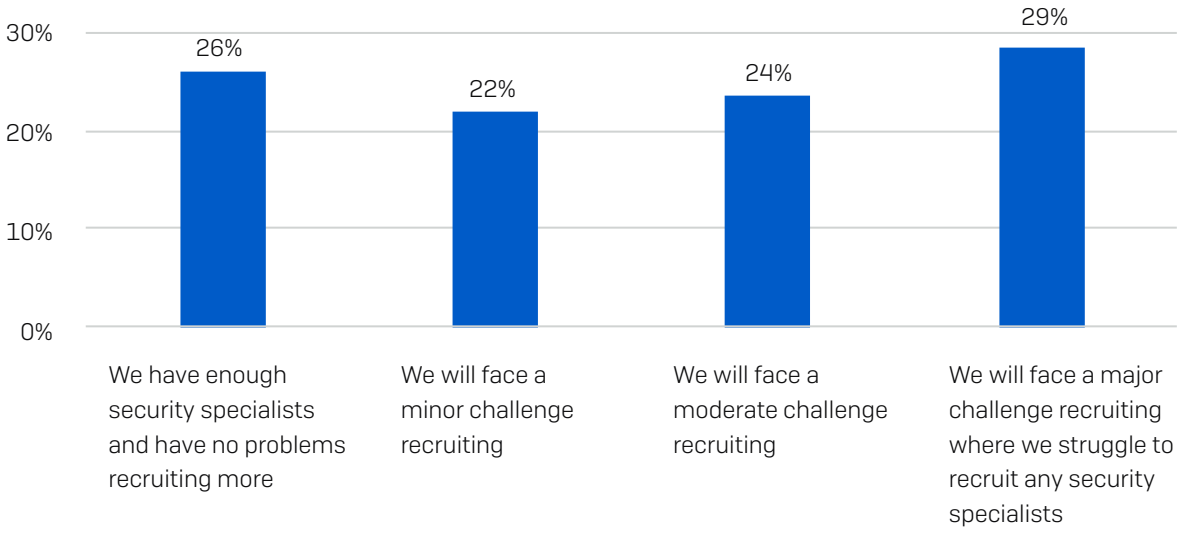
Perceived Board Level Understanding of Security – India

How well do you think your company board understands cybersecurity issues?



Cybersecurity Professional Recruitment Difficulty Level

What is your view on the availability of skilled security employees for your organisation in the next 24 months? India



Top skills in demand:

1. Knowledge of cloud security policies/architecture
2. Software vulnerability testing
3. Employee and executive training

Top attack vectors:

1. Phishing and whaling
2. Weak or compromised credentials
3. Social engineering

Top rated threats in 2022:

1. Malware
2. Malicious employees
3. Third party error
4. Poorly designed systems
5. Phishing and whaling

Rated threats 2021-2022

2021	2022
Malware	Malware
Phishing and whaling	Malicious employees
Backdoors	3rd party error
AI/ML attacks	Poorly designed systems
Ransomware	Phishing and whaling
Nation state	Encryption backdoors
Poorly designed systems	Social engineering
Malicious employee	Corporate espionage
Zero-day vulnerabilities	AI/ML attacks
Social engineering	Zero-day vulnerabilities
Corporate espionage	Employee error
Employee error	Nation state
Partner/3rd party error	DDoS
DDoS	Ransomware

Adoption of threat hunting:

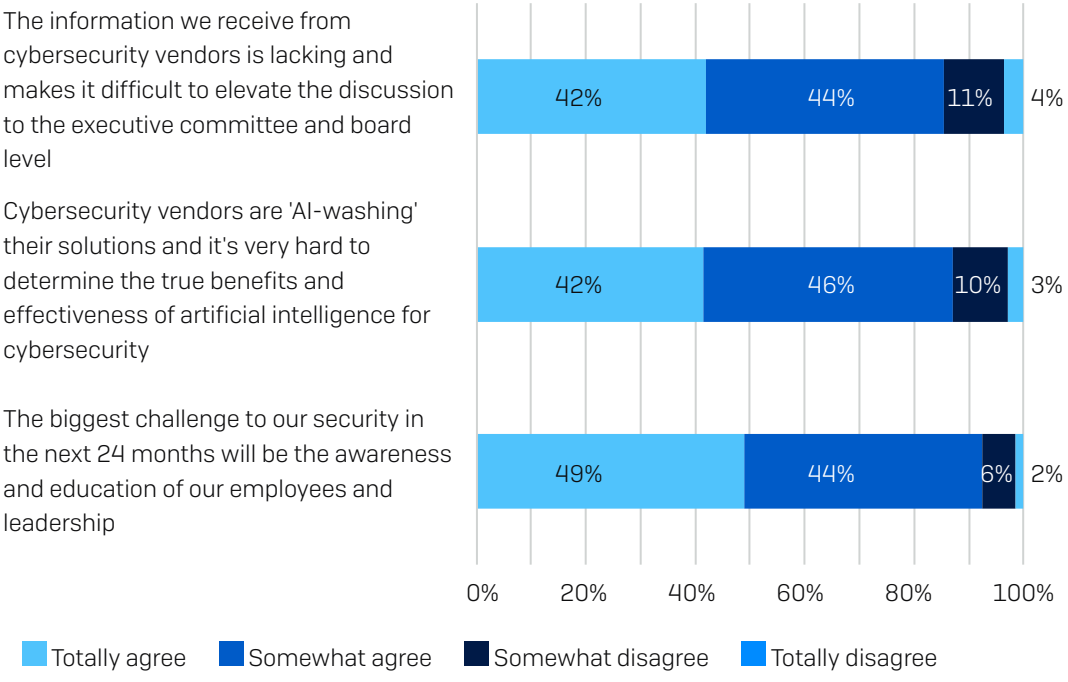
54% of companies do in-house, 41% use an external partner, 6% no/unsure

Please rate your agreement with the following statements – India

The information we receive from cybersecurity vendors is lacking and makes it difficult to elevate the discussion to the executive committee and board level

Cybersecurity vendors are 'AI-washing' their solutions and it's very hard to determine the true benefits and effectiveness of artificial intelligence for cybersecurity

The biggest challenge to our security in the next 24 months will be the awareness and education of our employees and leadership

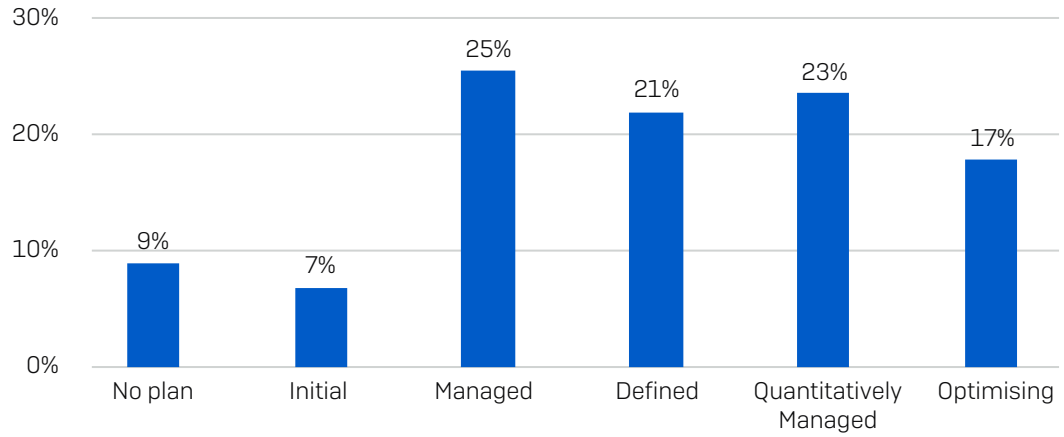


Cybersecurity in Japan

Spend on cybersecurity as percentage of total technology budget: 12.3%

Cybersecurity Maturity Profile

Cybersecurity Maturity Rating – Japan



Who leads cybersecurity strategy?

CISO: 32%, CIO/CTO: 33%, Shared Group Responsibility/Other: 35%

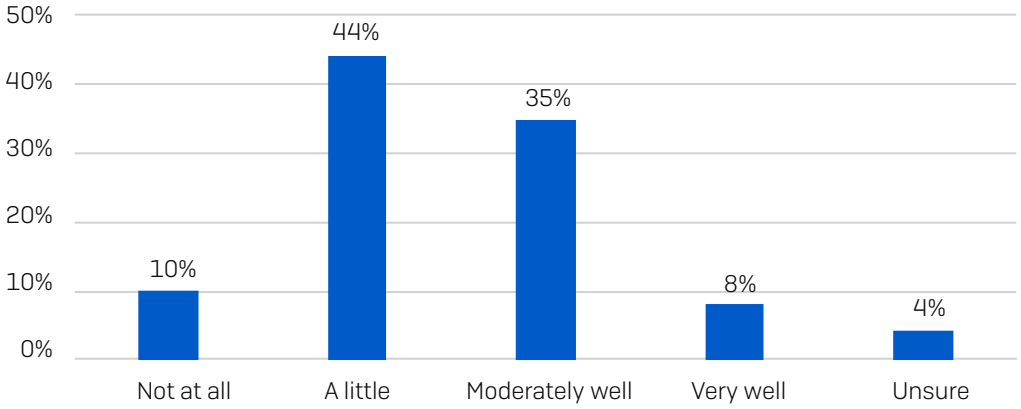
Top frustrations of cybersecurity professionals:

1. We can't employ enough skilled security specialists
2. We can't keep up with the pace of security threats
3. There's too much 'fear and doubt' messaging that makes it hard to talk accurately about cybersecurity

Board Level Understanding of Cybersecurity

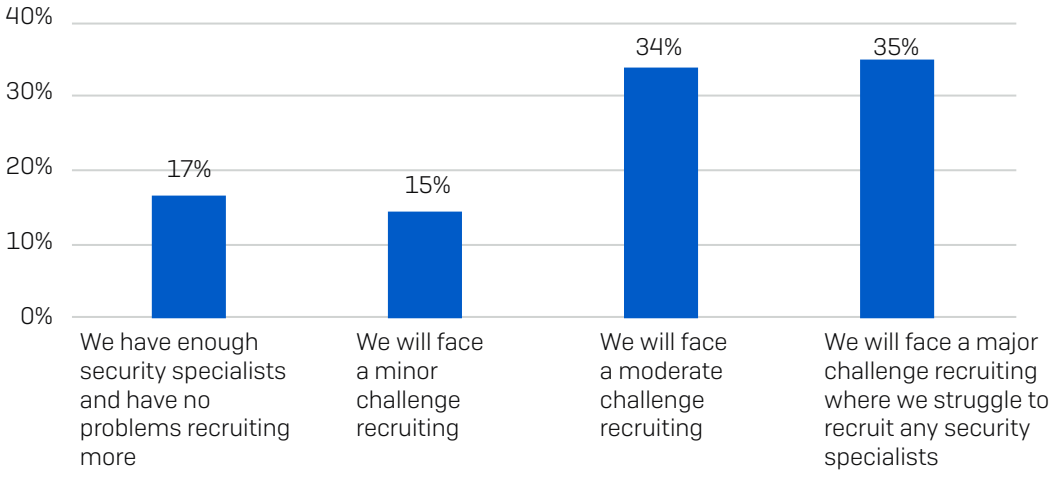
Perceived Board Level Understanding of Security – Japan

How well do you think your company board understands cybersecurity issues?



Cybersecurity Professional Recruitment Difficulty Level

What is your view on the availability of skilled security employees for your organisation in the next 24 months? Japan



Top skills in demand:

1. Employee and executive training
2. Software vulnerability testing
3. Staying up to date with the latest threats

Top attack vectors:

1. Phishing and whaling
2. Unpatched vulnerabilities
3. Supply chain vulnerabilities

Top rated threats in 2022:

1. Phishing and whaling
2. Malicious employees
3. Employee error
4. Ransomware
5. Corporate espionage

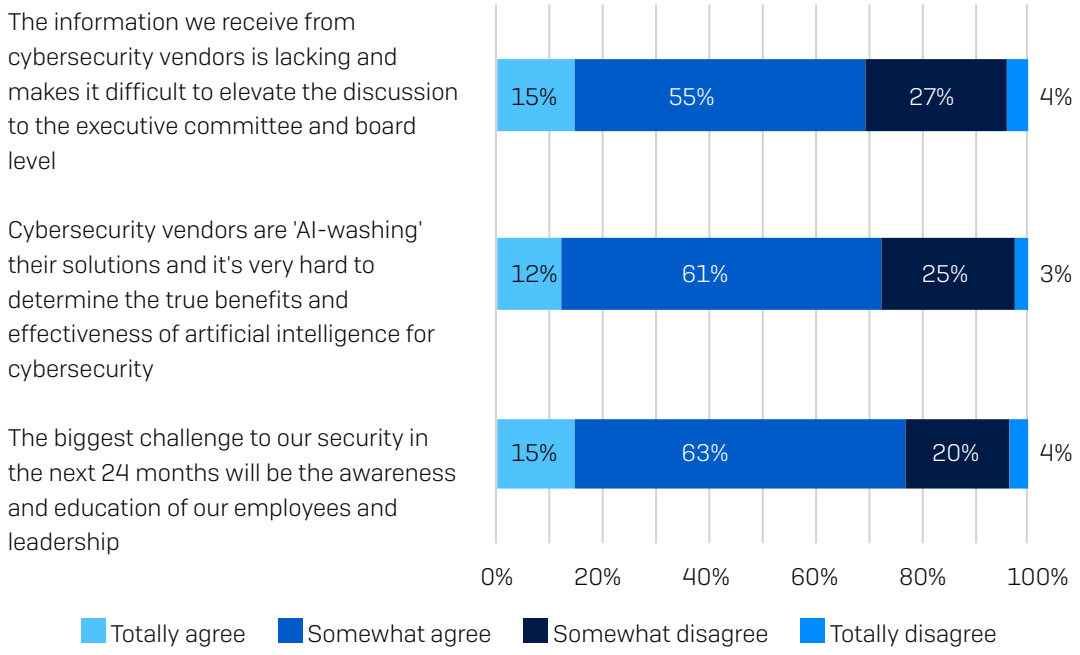
Rated threats 2021-2022

2021	2022
Employee error	Phishing and whaling
Malicious employee	Malicious employees
Poorly designed systems	Employee error
Ransomware	Ransomware
Malware	Corporate espionage
Phishing and whaling	Malware
DDoS	Poorly designed systems
Backdoors	AI/ML attacks
Partner/3rd party error	Zero-day vulnerabilities
Nation state	Nation state
Corporate espionage	3rd party error
Zero-day vulnerabilities	Encryption backdoors
AI/ML attacks	DDoS
Social engineering	Social engineering

Adoption of threat hunting:

27% of companies do in-house, 52% use an external partner, 23% no/unsure

Please rate your agreement with the following statements – Japan

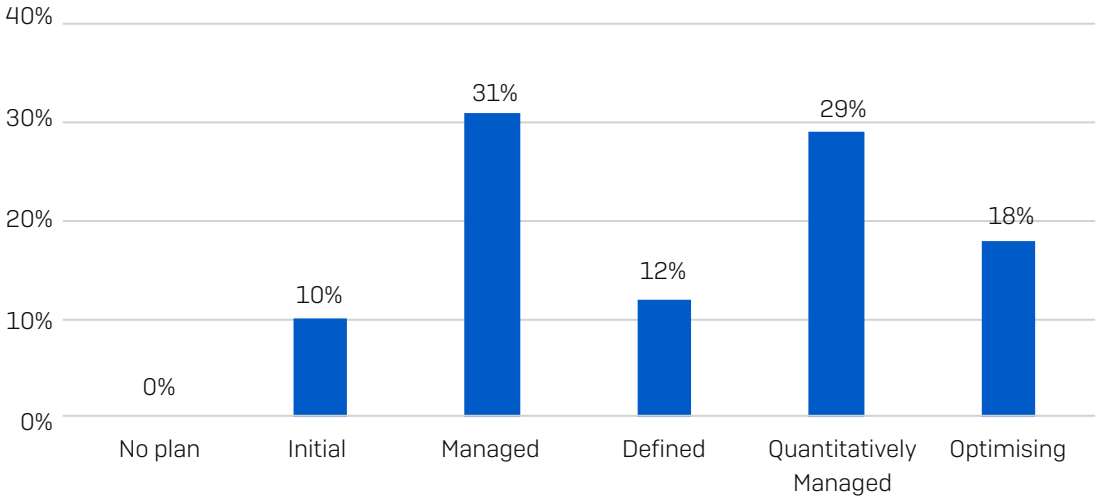


Cybersecurity in Malaysia

Spend on cybersecurity as percentage of total technology budget: 8.6%

Cybersecurity Maturity Profile

Cybersecurity Maturity Rating – Malaysia



Who leads cybersecurity strategy?

CISO: 35%, CIO/CTO: 38%, Shared Group Responsibility/Other: 27%

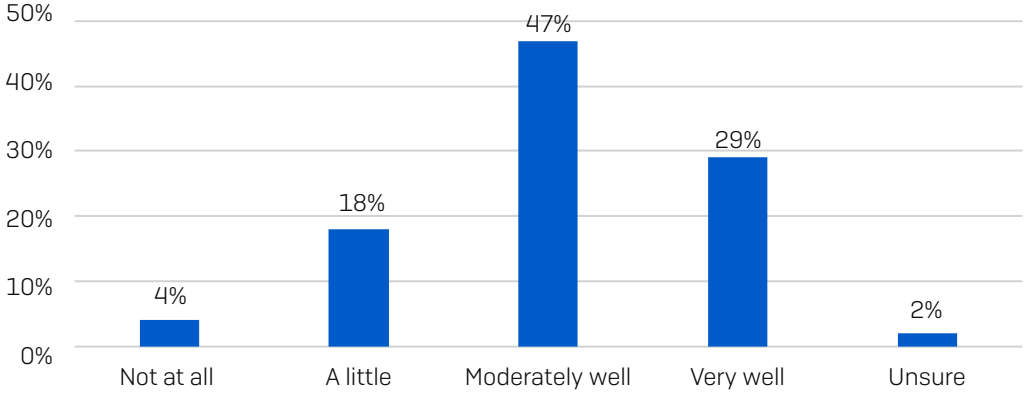
Top frustrations of cybersecurity professionals:

1. We can't keep up with the pace of security threats
2. We can't employ enough skilled security specialists
3. We don't put enough investment and time into training our general staff

Board Level Understanding of Cybersecurity

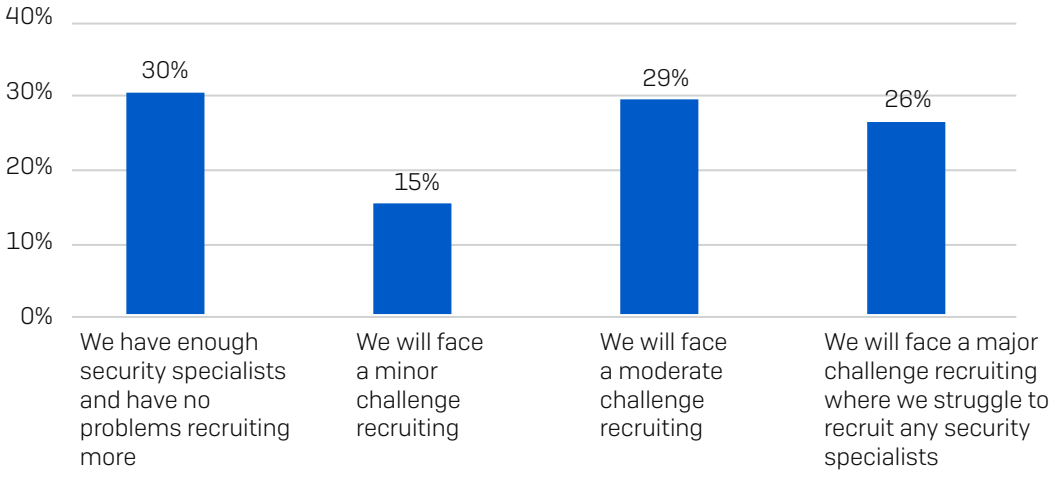
Perceived Board Level Understanding of Security – Malaysia

"How well do you think your company board understands cybersecurity issues?"



Cybersecurity Professional Recruitment Difficulty Level

What is your view on the availability of skilled security employees for your organisation in the next 24 months? Malaysia



Top skills in demand:

1. Staying up to date with the latest threats
2. Policy compliance and reporting
3. Employee and executive training

Top attack vectors

1. Phishing and whaling
2. Malicious employees
3. Supply chain vulnerabilities

Top rated threats in 2022:

1. Malware
2. Malicious employees
3. Employee error
4. Ransomware
5. Corporate espionage

Rated threats 2021-2022

2021	2022
Phishing and whaling	Malware
Ransomware	Malicious employees
Malware	Employee error
Malicious employee	Ransomware
AI/ML attacks	Corporate espionage
Social engineering	Encryption backdoors
DDoS	Phishing and whaling
Backdoors	AI/ML attacks
Poorly designed systems	Zero-day vulnerabilities
Zero-day vulnerabilities	Poorly designed systems
Corporate espionage	3rd party error
Employee error	Nation state
Partner/3rd party error	DDoS
Nation state	Social engineering

Adoption of threat hunting:

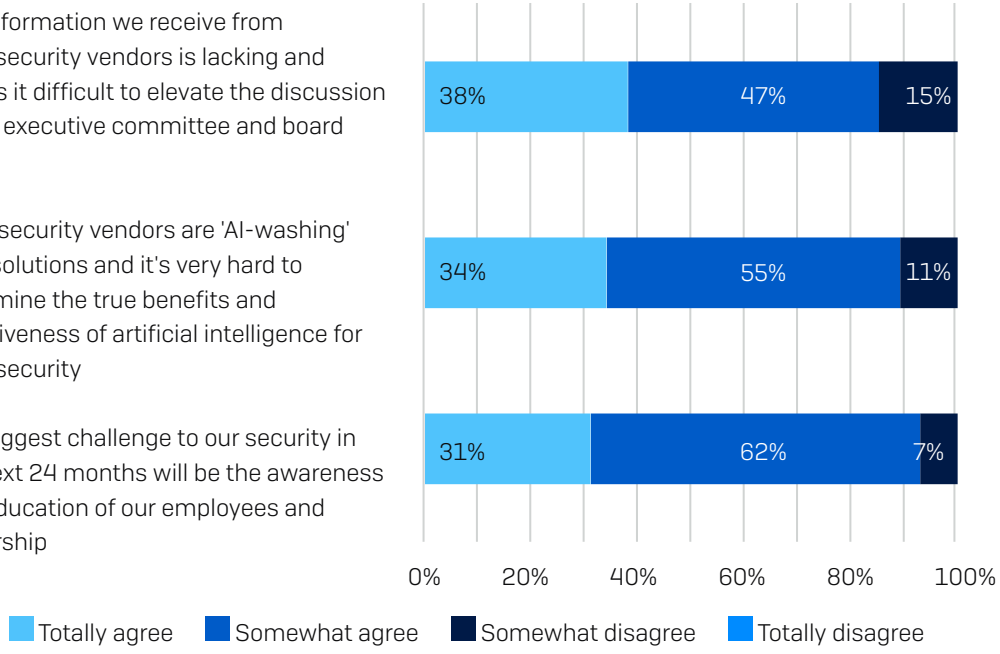
20% of companies do in-house, 60% use an external partner, 20% no/unsure

Please rate your agreement with the following statements – Malaysia

The information we receive from cybersecurity vendors is lacking and makes it difficult to elevate the discussion to the executive committee and board level

Cybersecurity vendors are 'AI-washing' their solutions and it's very hard to determine the true benefits and effectiveness of artificial intelligence for cybersecurity

The biggest challenge to our security in the next 24 months will be the awareness and education of our employees and leadership

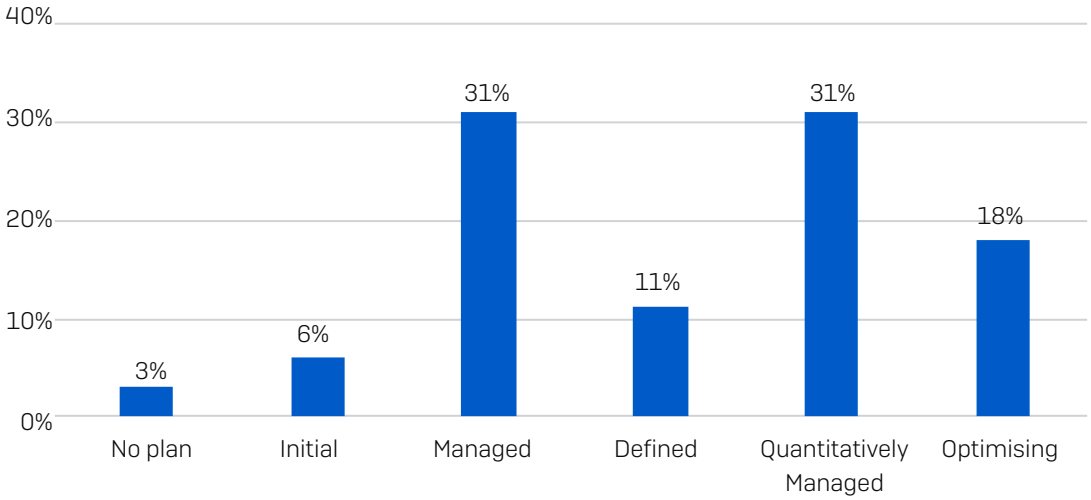


Cybersecurity in the Philippines

Spend on cybersecurity as percentage of total technology budget: 13.3%

Cybersecurity Maturity Profile

Cybersecurity Maturity Rating – Philippines



Who leads cybersecurity strategy?

CISO: 33%, CIO/CTO: 36%, Shared Group Responsibility/Other: 31%

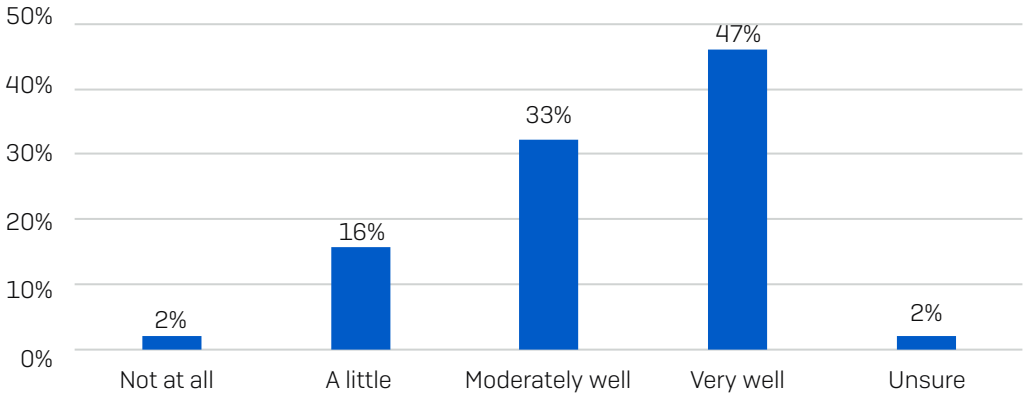
Top frustrations of cybersecurity professionals:

1. Cybersecurity is frequently relegated in priority
2. Our executives assume cybersecurity is easy and me/my cybersecurity peers over exaggerate threats and issues
3. Our executives assume our company will never get attacked

Board Level Understanding of Cybersecurity

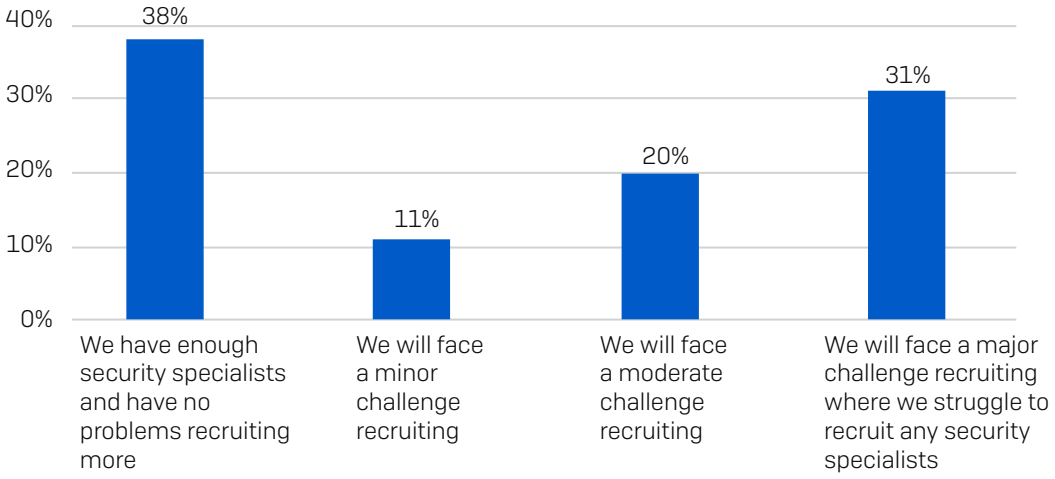
Perceived Board Level Understanding of Security – Philippines

How well do you think your company board understands cybersecurity issues?



Cybersecurity Professional Recruitment Difficulty Level

What is your view on the availability of skilled security employees for your organisation in the next 24 months? Philippines



Top skills in demand:

1. Knowledge of cloud security policies/architecture
2. Software vulnerability testing
3. Staying up to date with the latest threats

Top attack vectors:

1. Phishing and whaling
2. Weak or compromised credentials
3. Malicious employees

Top rated threats in 2022:

1. Phishing
2. Poorly designed systems
3. Malware
4. Encryption backdoors
5. AI/ML attacks

Rated threats 2021-2022

2021	2022
Phishing and whaling	Phishing and whaling
Malware	Poorly designed systems
Ransomware	Malware
Corporate espionage	Encryption backdoors
Malicious employee	AI/ML attacks
AI/ML attacks	Corporate espionage
Poor systems	Malicious employees
Employee error	Employee error
Partner/3rd party error	Nation state
Zero-day vulnerabilities	DDoS
Backdoors	Social engineering
Social engineering	Zero-day vulnerabilities
Nation state	3rd party error
DDoS	Ransomware

Adoption of threat hunting:

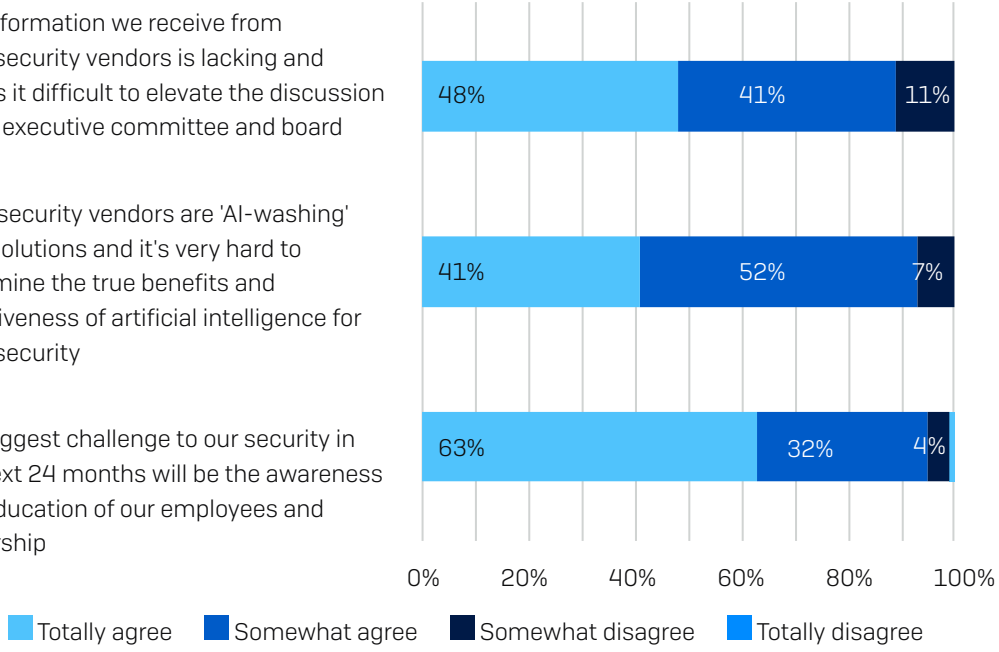
24% of companies do in-house, 69% use an external partner, 8% no/unsure

Please rate your agreement with the following statements – Philippines

The information we receive from cybersecurity vendors is lacking and makes it difficult to elevate the discussion to the executive committee and board level

Cybersecurity vendors are 'AI-washing' their solutions and it's very hard to determine the true benefits and effectiveness of artificial intelligence for cybersecurity

The biggest challenge to our security in the next 24 months will be the awareness and education of our employees and leadership

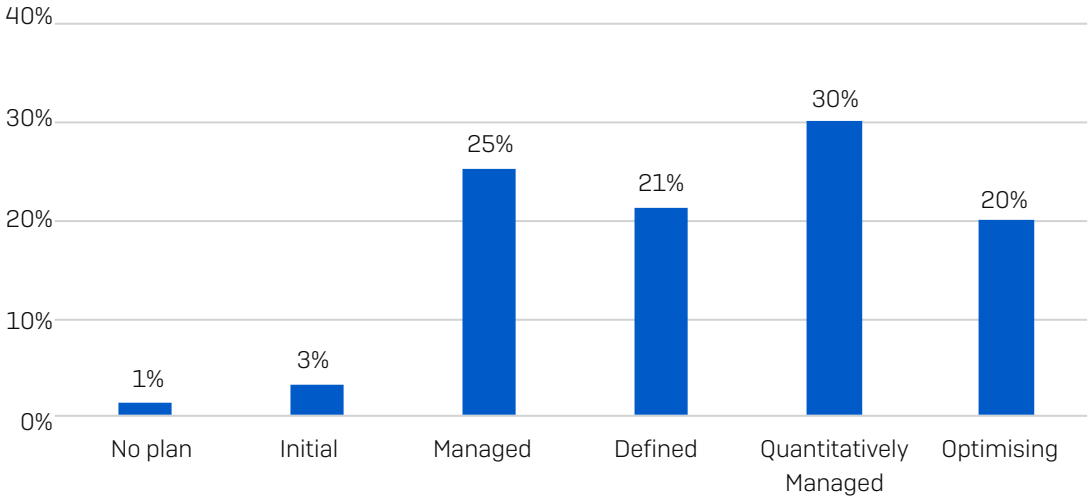


Cybersecurity in Singapore

Spend on cybersecurity as percentage of total technology budget: 11.23%

Cybersecurity Maturity Profile

Cybersecurity Maturity Rating – Singapore



Who leads cybersecurity strategy?

CISO: 33%, CIO/CTO: 36%, Shared Group Responsibility/Other: 31%

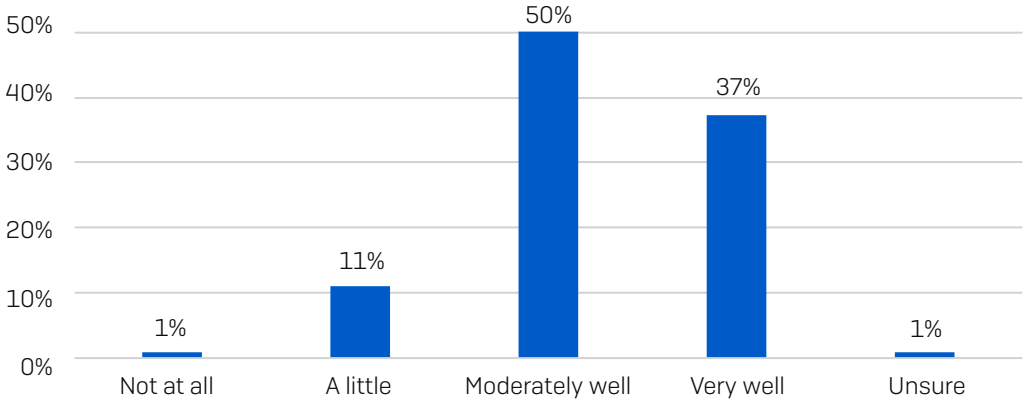
Top frustrations of cybersecurity professionals:

1. Our executives assume cybersecurity is easy and me/my cybersecurity peers over exaggerate threats and issues
2. There's too much 'fear and doubt' messaging that makes it hard to talk accurately about cybersecurity
3. Cybersecurity is frequently relegated in priority

Board Level Understanding of Cybersecurity

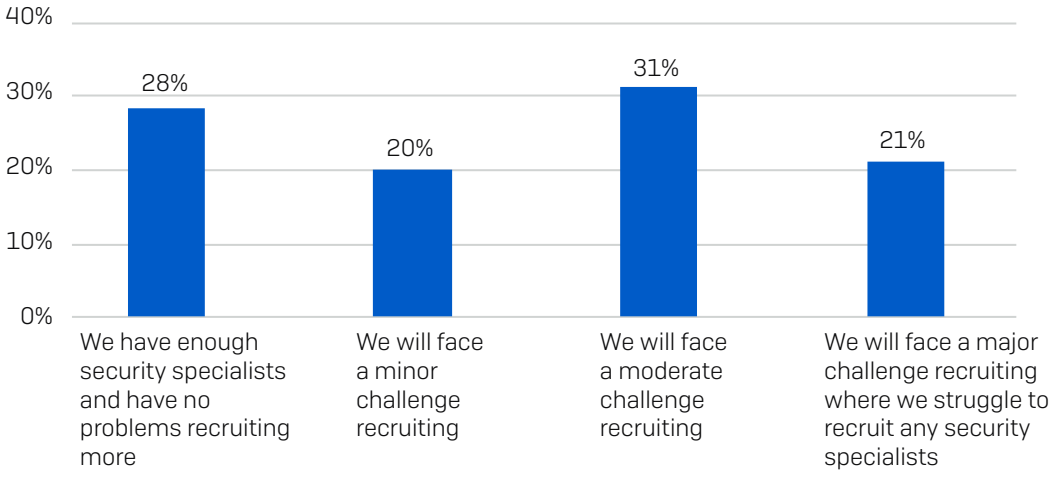
Perceived Board Level Understanding of Security – Singapore

How well do you think your company board understands cybersecurity issues?



Cybersecurity Professional Recruitment Difficulty Level

What is your view on the availability of skilled security employees for your organisation in the next 24 months? Singapore



Top skills in demand:

1. Knowledge of cloud security policies/architecture
2. Software vulnerability testing
3. Staying up to date with the latest threats

Top attack vectors:

1. Phishing and whaling
2. Misconfigurations
3. Man in the middle

Top rated threats:

1. Malware
2. Phishing
3. DDoS
4. Social engineering
5. Ransomware

Rated threats 2021-2022

2021	2022
Ransomware	Malware
Malicious employee	Phishing and whaling
AI/ML attacks	DDoS
Malware	Social engineering
Backdoors	Ransomware
Phishing and whaling	Nation state
Nation state	Corporate espionage
Zero-day vulnerabilities	Employee error
Corporate espionage	3rd party error
Poorly designed systems	Malicious employees
DDoS	Poorly designed systems
Employee error	Encryption backdoors
Partner/3rd party error	Zero-day Vulnerabilities
Social engineering	AI/ML attacks

Adoption of threat hunting:

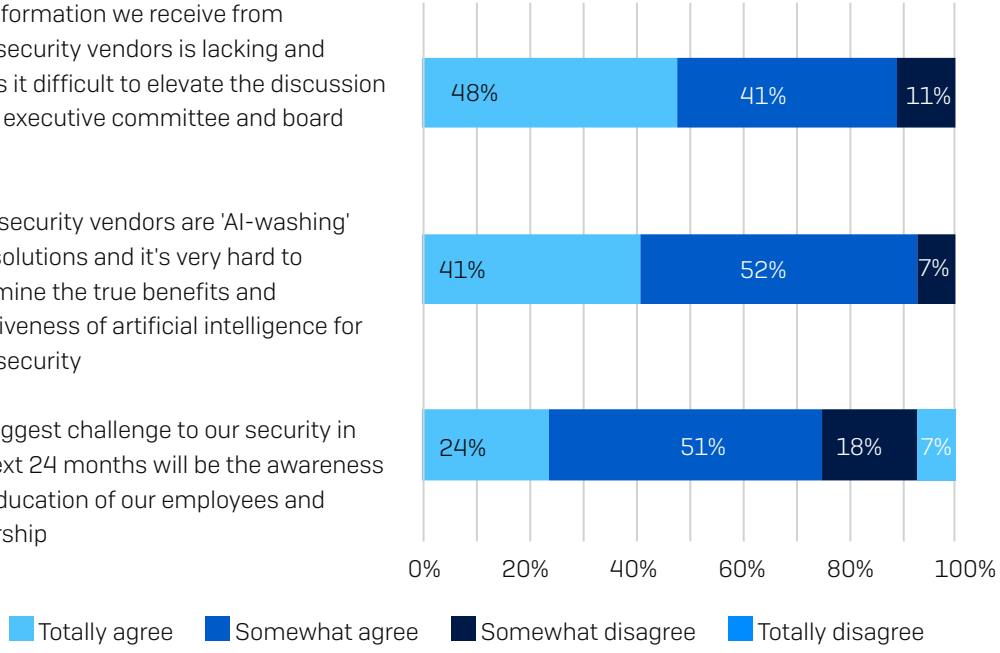
23% of companies do in-house, 61% use an external partner, 16% no/unsure

Please rate your agreement with the following statments – Sinagpore

The information we receive from cybersecurity vendors is lacking and makes it difficult to elevate the discussion to the executive committee and board level

Cybersecurity vendors are 'AI-washing' their solutions and it's very hard to determine the true benefits and effectiveness of artificial intelligence for cybersecurity

The biggest challenge to our security in the next 24 months will be the awareness and education of our employees and leadership



A View from Sophos

These latest results from TRA indicate that that the tide may have turned this year and APJ organisations really are taking cybersecurity more seriously – hopefully this sentiment is now the new-normal.

While you may scoff at the thought that those outside your organisation think you don't take cybersecurity seriously, historically though, it was the reality. And with more organisations moving up the self-ranked cybersecurity maturity charts, it's a clear indicator that there was room for the improvements that were desperately needed.

But how much of that self-ranked maturity will translate into preparedness you can rely on when something goes inexplicably wrong?

Evaluations and self-ranking aside, very few organisations put into practice and validate their resilience when faced with a real cybersecurity incident.

"Everyone has a plan until they're punched in the nose."

The TRA research shows that organisations that do have plans, might not have fully tested them against a serious attack scenario. In some cases where a real incident has unfolded, plans and response actions have been bespoke. Sometimes plans can't be retrieved as they're on the desktops and servers that have just been ransom(war)ed!

Much of this murkiness in cyber resilience is attributed to issues of comprehension of the threats and diversification of cybersecurity roles and responsibilities within an organisation. Comprehension is the primary reason organisations across APJ fail to live up to their own expectations when it comes to adequately planning for a cyber incident because board and executive levels often do not understand how cyber issues can disrupt and eviscerate the bottom line.

Don't leave the door open for attackers to take advantage of you – as they likely will.

Even though we've all witnessed high impact vulnerabilities take main stage and threat actors wreak havoc across businesses of all sizes from all industries – employing everything from ProxyShell to Log4J – by stealing corporate data and using extortion tactics, it's not just the big oh-days that we should be looking to mitigate. Basic cybersecurity hygiene is still problematic for many organisations with unpatched applications and operating systems allowing attacks to easily unfold, and even simplistic phishing and credential harvesting operations giving cyber-criminal groups access far and wide.

Looking for solutions to solve these very complex and deeply rooted issues isn't an overnight thing, and don't expect a single piece of software or policy control to be a silver bullet. Once again, the human element comes into play with phishing and user interaction still common ways attackers make their way through the front door. Understanding the threats we face on an almost daily basis and how to deal with them – regardless of whether you're a C-suite executive or working in the mail room – is essential to protect the organisation. Bottom line – everyone needs the same level of insight and training on how to spot and deal with fraudsters attempting to infiltrate the business.

On the diversification of cybersecurity roles and responsibilities front, mitigating controls are technical even though theoretically autonomous. These types of extremely technical controls need expertise to make sense of and to action the items that are important. This is why having a diverse team with different skill types within your cyber resiliency ranks will bolster how your organisation responds to an incident.

By addressing comprehension and diversification, you will be one step closer to successfully detecting and remediating an attack before it gets its hooks into you, your employees, your business and the information you hold dearest.

Appendix

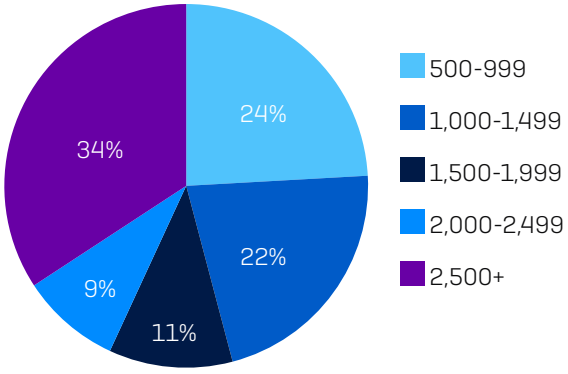
Definitions for the Cybersecurity Maturity Model:

- 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.

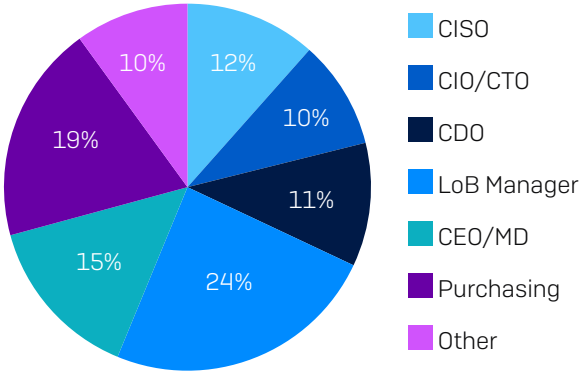
Demographics and Methodology

In January 2022, 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.

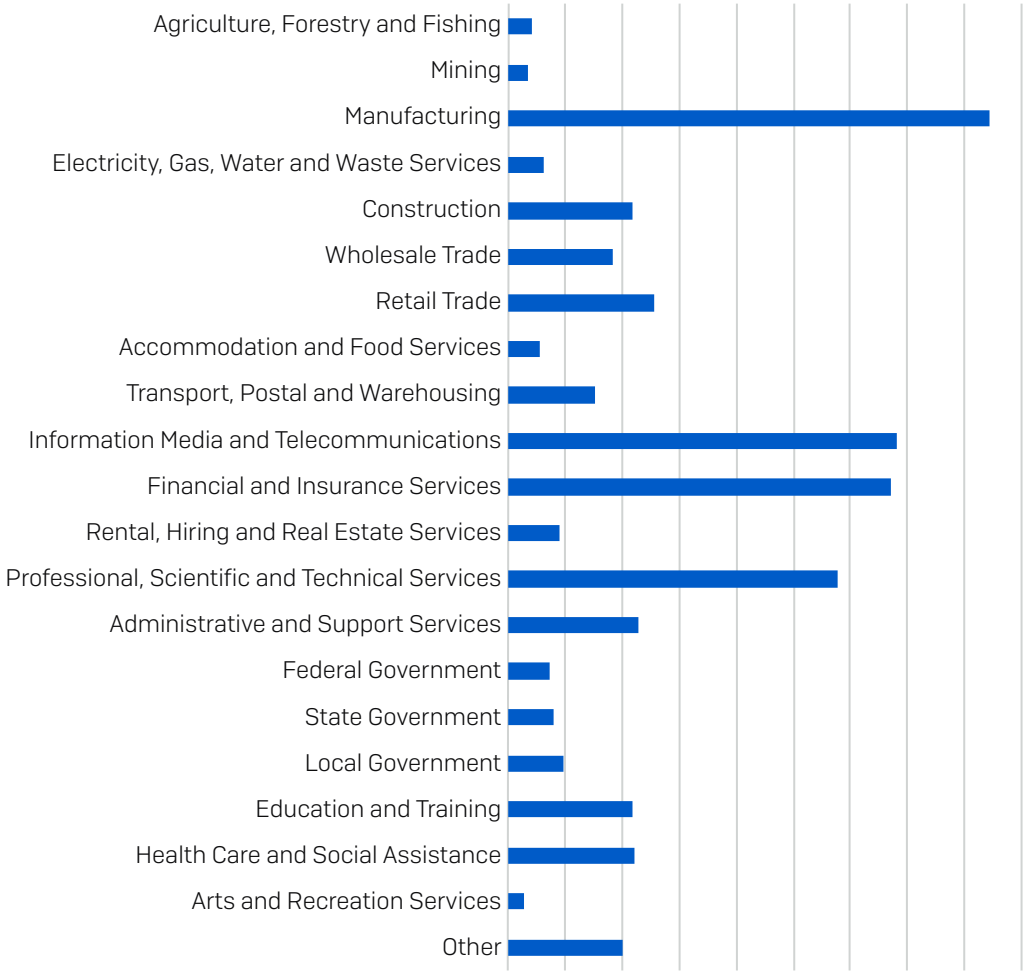
Employee Size



By role



Industry



About Sophos

Sophos is a worldwide leader in next-generation cybersecurity, protecting more than 500,000 organisations and millions of consumers in more than 150 countries from today's most advanced cyberthreats. Powered by threat intelligence, AI and machine learning from SophosLabs and SophosAI, Sophos delivers a broad portfolio of advanced products and services to secure users, networks and endpoints against ransomware, malware, exploits, phishing and the wide range of other cyberattacks. Sophos provides a single integrated cloud-based management console, Sophos Central – the centerpiece of an adaptive cybersecurity ecosystem that features a centralised data lake that leverages a rich set of open APIs available to customers, partners, developers, and other cybersecurity vendors. Sophos sells its products and services through reseller partners and managed service providers (MSPs) worldwide. Sophos is headquartered in Oxford, U.K. 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

For more information on how to protect your business from cybersecurity threats visit www.sophos.com

2022-03-31 (WP-NP)

SOPHOS