SOPHOS
Cybersecurity evolved.

The Future of Cybersecurity in Asia Pacific and Japan

2nd Edition

"A TRA Report sponsored by Sophos"

CONTENTS

INTRODUCTION

In 2019 Sophos and TRA collaborated to launch the first edition report of the Future of Cybersecurity in Asia Pacific and Japan.

That report revealed that organisations in APJ faced a series of cybersecurity obstacles in the areas of education, company culture, skills, budgeting, and operational management. At the time, the key themes centred on creating stronger education and awareness of security threats and issues, underpinned by more efficient adoption and usage of new cybersecurity tools and solutions.

What's changed?

Well, not much and a great deal. The COVID-19-driven 2020 mass migration to a work from home/ remote work environment imposed considerable stresses on organisations' technology and cybersecurity capabilities. Broadly, whilst where we work changed substantially, the digital transformation agenda continued its acceleration and security maturity, education and capabilities that we saw in 2019 continue to be problematic.

Our survey of senior IT and security decision makers in 900 companies in Australia, India, Japan, Malaysia, Philippines and Singapore highlighted that:

- The COVID-19 pandemic had a positive impact on cybersecurity with 69% of companies across our survey agreeing with the sentiment that "*The outbreak of COVID-19 was the strongest catalyst for upgrading our cybersecurity strategy and tools in the past 12 months*."
- Cybersecurity budgets remained largely unchanged as a percentage of revenue between 2019 and 2021, however there was a marked push to exert more centralised control and oversight with 64% of companies consolidating cybersecurity budgets within their IT groups, an increase of 14% over 2019.
- Cybersecurity in its current form is a known factor – meaning the market is familiar with the threats and solutions available. For the most part, while there is still some element of "playing catch up" with new threats, new tools patterns, the focus is on operational excellence through improving culture, education and the optimisation of the technology.
- Asia Pacific organisations say they are becoming more mature with cybersecurity, but they continue to be hit by a number of attacks –with 56% suffering from a successful attack in 2021 up from 32% in 2019.
- Skills, budget, and organisational apathy are the top challenges. Most also say they cannot keep up with the pace of security developments. Comparisons between 2019 and 2021 data show that companies are increasing their reliance on managed service providers in 2021 to alleviate some of the pain associated with skills shortages, cloud migrations and increased threat activity.

As with our first edition, this report comprises four sections – the research results, individual country insights, a list of steps to consider when reviewing/implementing cybersecurity strategies, and the view of the report sponsor, Sophos.

> "Before 2020 our employees didn't have access if they were outside the office. In 2020 we moved from 400 office branches to 3,000 home 'branches' with no LAN, different end-user control and Wi-Fi restrictions. Zero Trust security and a secure edge strategy were critical."
>
> Angel Broking Ltd, India

RESEARCH FINDINGS

The research results are presented in three sub-sections (Maturity and Strategy, The Skills Challenge and Incidents and The Future Outlook), each with important data and findings highlighted.

Maturity and Strategy

In 2019 we wrote, "*it is evident that perceived security maturity remains low*". At that point in time only 2% of surveyed companies self-assessed themselves at the top 'optimised' cybersecurity maturity level.

Today that number stands at 18% (see Figure 1 following). A significant improvement over two years and undoubtedly many organisations made tremendous progress in improving their security posture. (For more detail regarding the categorisations, please see the "Demographics, Definitions and Methodology" section at the end of the report.)

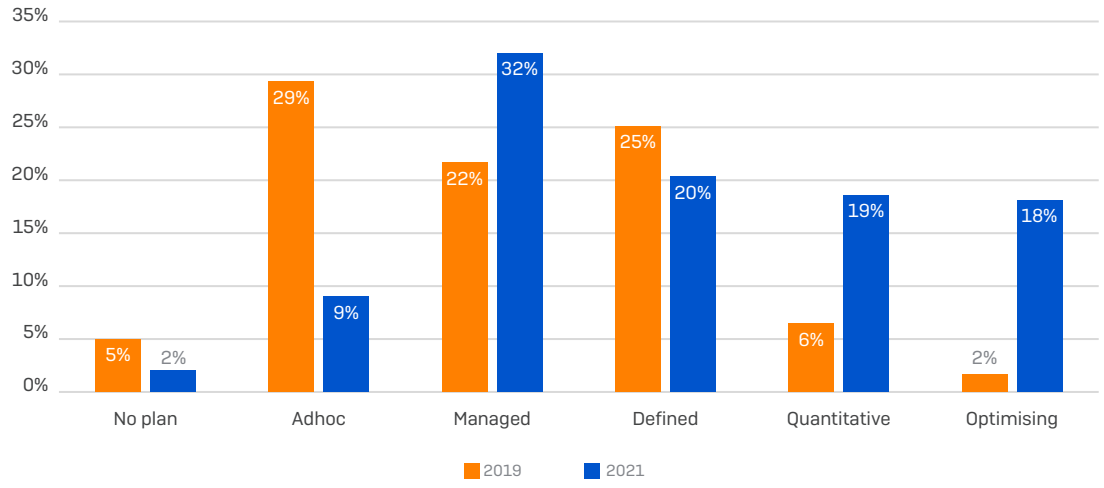


Figure 1: "How would you define your company's cybersecurity maturity?'

> "Our approach is to ratify our strategy annually and it's critical to understand the business goals so you know where to invest rather than just doing the same thing. We also understand it's impossible to do everything and it was important for us to get the senior management on board about the importance of protecting our 'crown jewels'."
>
> National Aged Care Provider, Australia

Our research suggests this growth in recognition of the importance of the cybersecurity issues facing companies has been driven by:

- Continued developments in regulatory requirements, especially personally identifiable information (PII) initiatives as well as movement in mandatory breach disclosure legislation.
- The acceleration of digital transformation activities and the move to establish work from home/remote business operations throughout 2020 due to the COVID-19 pandemic. Indeed, 53% of companies agreed with the statement "*We were unprepared for the security requirements driven by the sudden need for secure remote working caused by COVID-19.*"
- The sustained adoption of cloud-based technology, either infrastructure-as-a-service or software-as-a-service solutions.

Of the companies surveyed, those in Australia, India and Philippines showed higher levels of maturity relative to the overall sample whilst those in Japan, Malaysia and Singapore indicated above average percentage of companies with an 'adhoc' approach.

However, company self-assessment results can sometimes be influenced by a sense of complacency or over-accomplishment and our data tends to suggest the maturity reality may be a little different.

Let's consider the issue of keeping the cybersecurity strategy up to date.

In 2019, 51% of companies stated they last reviewed their strategy more than 12 months ago. With maturity capabilities increasing significantly in 2021, our expectation was that companies had moved to a more continuous improvement approach with their cybersecurity strategy.

We were wrong.

Whilst only a small increase of 3%, the 2021 data showed that 54% of all companies had not updated their cybersecurity strategies in the last 12 months. This comes during a time of rapid digitisation and remote work initiatives.

In 2019 we concluded that "*maturity levels can be highly subjective unless properly quantified and regularly tested*" and that sentiment is still valid. We explored the issue of maturity and capability in a series of survey questions focusing on skills, budgets and technology deployments and, in many instances, there was little noticeable improvement between 2019 and 2021.

For example, the top 3 frustrations companies experience relating to cybersecurity in 2021 are:

1. "*Our executives assume cybersecurity is easy and we over exaggerate cybersecurity threats and issues*" (2019 rank: 3rd)
2. "*There is not enough budget for cybersecurity*" (2019 rank: 2nd)
3. "*We can't employ enough cybersecurity professionals*" (2019 rank: 1st)

These frustrations are the same ones we wrote about in 2019 (albeit in a slightly different order).

> "One of our challenges is managing people and making sure they understand the risks. We have to make sure management understand it's more complicated than just buying a product to fix a problem. We're lucky we have good support at senior levels."
>
> National Electrical Engineering Company, Australia

We also asked organisations if they had a cybersecurity team in place that could detect, investigate and respond to threats. In 2019, 50% of organisations answered 'no', in 2021 that increased to 52%.

The reality is that organisations typically find it hard to achieve and maintain a consistent focus on security. Like many other company initiatives, culture, capabilities, enthusiasm, education, etc all vary. There is no 'constant state', rather companies move along a sine wave, sometimes above the curve, sometimes below.

> "A lot of companies are upgrading their cybersecurity technology and maturing. Hackers are also maturing faster and upgrading faster. Hackers are targeting the human weaknesses more than technology."
>
> Tanglin Trust School, Singapore, Singapore

When companies were asked if they had challenges in keeping up to date with cybersecurity in their organisation, comparisons show a modest improvement of 5% from 72% agreeing in 2019 to 67% in 2021. (See Figure 2 following).

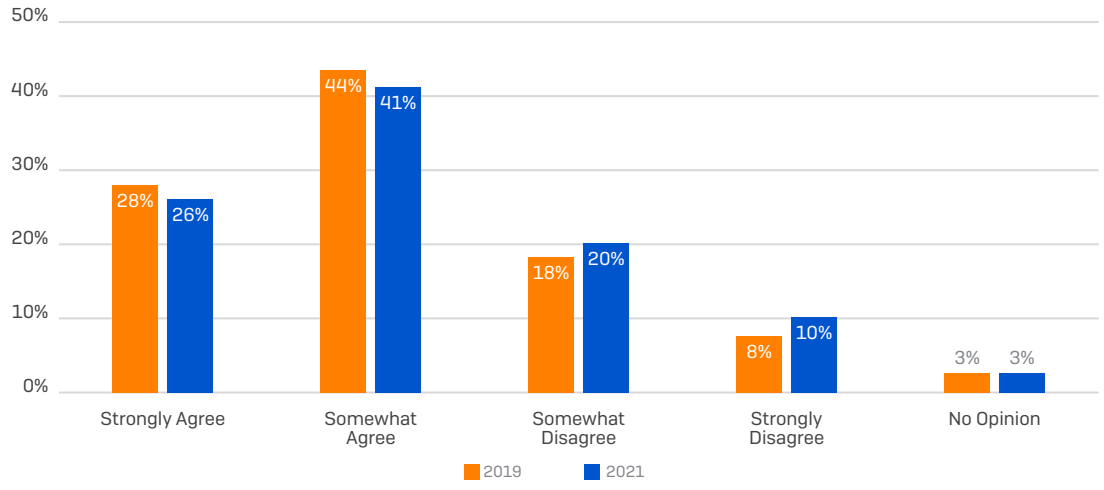


Figure 2: "Staying up to date with cybersecurity technology is a challenge for my organisation"

Overall, despite improvements made, progress remains slow, reinforcing our belief that cybersecurity is never 'finished' and requires a constant focus, both from technological and cultural viewpoints.

The Skills Challenge

In 2021, we found that 67% of companies are having difficulty staying up to date with their cybersecurity environment and in-house skills are an important consideration in helping organisations tackle this issue. Unfortunately, 59% of businesses agree that their company's "*lack of cybersecurity skills is challenging for their organisation*", a marginal 3% improvement from 2019's 62%.

Companies are confronted with dual blockers when attempting to improve their in-house skills; a lack of suitable staff and budget constraints:

- In 2019, 67% of companies struggled to recruit people with the necessary cybersecurity skills. In 2021, this had marginally improved, dropping 5% to 62%.
- Reflecting the law of supply and demand, the relative scarcity of suitable people has seen pressure on hiring companies to increase their budgets. Yet in 2021, 59% of businesses stated that their cybersecurity budget is below where it needs to be, the same percentage it was in 2019. (See Figure 3 following).

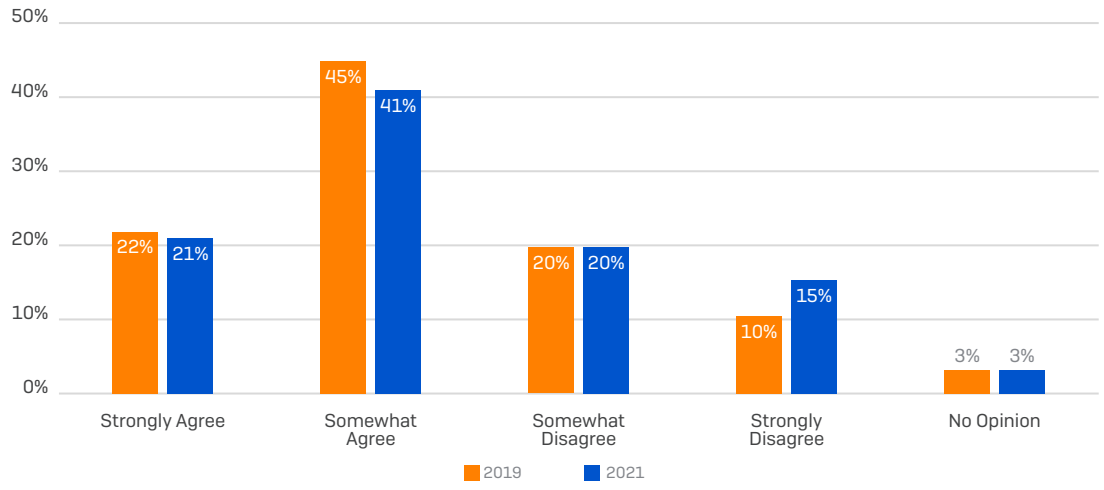


Figure 3: "My organization struggles to recruit people with the cybersecurity skills we need"

Exploring this issue a little more reveals a persistent trend.

Many organisations are looking to third parties to help plug the gaps in skills shortages. Unlike 2019 where the majority of organisations kept most capabilities in-house across all facets of cybersecurity strategy and management, our research data showed a consistent trend of companies moving away from this to either a fully outsourced or blended (i.e. a mixture of in-house and third party) model. This trend shows clearly from 2019 to 2021 as well as in our respondents' 2023 plans.

Whilst some activities such as creating and maintaining cybersecurity strategies or providing training to all employees only showed relatively slight increases in an outsourced or blended approach, the more operational and process areas of cybersecurity showed larger movements towards less in-house and more with third parties.

> "We have to rely on partners moving forward as we will never be able to get the required staff."
>
> Melanoma Institute, Australia

For example, data management and compliance activity showed an increase from 43% to 50% of companies following an outsourced/blended model between 2019 and 2023.

Other functions such as cybersecurity reporting, testing, incident response, investigation and remediation also showed relatively large increases in the use of third parties between 2019 and 2023, as can be seen in the following table:

Table 1: Use of third parties between 2019 and 2023

ACTIVITY	2019 % OUTSOURCED/BLENDED	2023 OUTSOURCED/BLENDED
Reporting	46%	57%
Testing	54%	61%
Incident response	50%	62%
Incident investigation	56%	61%
Incident remediation	56%	61%

> "It just makes sense to use partners however there are always some intricacies within the business that partners can't know so the ideal mix is both partners and internal staff to create a team."
>
> National Aged Care Provider, Australia

Of course, even with a trend to more third-party engagement, it's important to maintain in-house education and training and this is actually one of the more significant challenges that businesses face. In 2019 we observed that 60% of businesses struggle to provide effective cybersecurity education to their employees.

That's increased by 22% to 82% today.

To help manage the complexity of their environments, alongside the growing use of third parties, companies are also looking to more efficient technology solutions that incorporate automation, machine learning and artificial intelligence. In this context both AI/ML-driven solutions and reliance on public cloud were cited as the top two technology approaches that will have the biggest impact on companies' cybersecurity capabilities (and, ironically, we expect their cybersecurity posture as well).

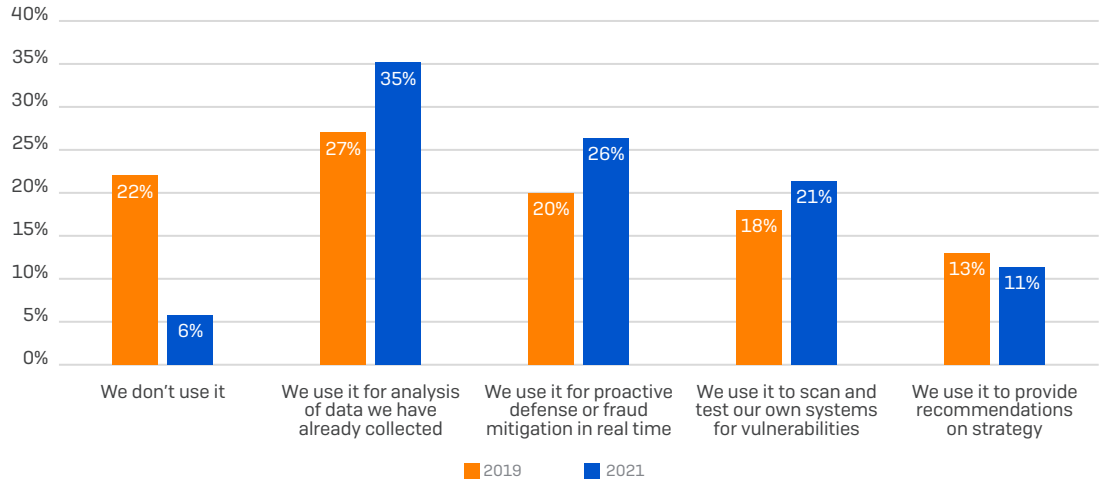


Figure 4: What is the role of AI and machine learning in your organisation's approach to security today?

> "We are always challenged to keep our staff as cybersecurity skills are in such high demand. We've reduced the negative impact of this by moving much more towards automation."
>
> Philippines Government Agency CISO, Philippines

Incidents and the Future Outlook

Raise a metaphorical hand if you've been attacked since the start of 2021. Thought so.

Keep your hand raised if the attack was successful and you lost data.

If it's still raised, you're not alone.

68% of those surveyed in 2021 stated they had been successfully breached by some form of cyber-attack. That represents a significant increase of 36% over 2019 data when 32% of companies stated they had fallen victim to an attack.

Of these successful breaches, 55% of companies rated the loss of data as either 'very serious' (24%) or 'serious' (31%)(see Figure 5 following) and although we didn't ask the question in 2019, in 2021 the frequency of attacks showed that 17% of companies were subject to more than 50 attacks per week with expectations of increased activity to come.

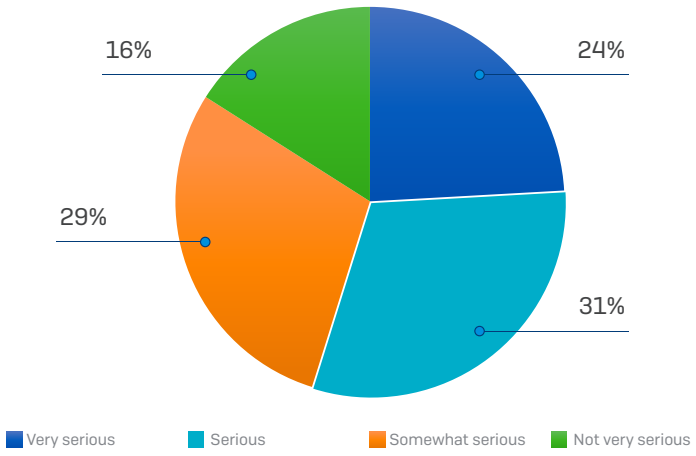


Figure 5: How serious was the cybersecurity breach loss?

The data also showed that larger organisations with 500+ employees were only marginally more likely to be attacked suggesting that even smaller and mid-market companies need to contemplate an 'enterprise-grade' level of security with manufacturing, technology, banking and financial services, professional services, health and government agencies the most frequently targeted sectors.

> "We're rigorous with incident response. We keep hard and soft copies of our IR playbooks and encourage the team to do the same. We run trials frequently to ensure we're learning and continually refining our process. It's fundamentally important that everyone understands their roles and responsibilities."
>
> University of Newcastle, Australia

Unsurprisingly, the threat landscape continues to evolve.

For the lead up to 2021, respondents told us that overall, the top 3 security threats were:

1. Ransomware
2. Malware
3. Phishing

The view looking forward to 2023 is a little "same, same but different". In part reflecting the concerns triggered through supply chain vulnerabilities (i.e. where a security vendor or other technology provider has been unknowingly breached, allowing threat actors to target downstream customers of the vendor) the expected top 3 threats in 2023 are expected to be:

1. Phishing
2. Malware
3. Poorly designed/vulnerable supplier systems

Technology tools obviously have a direct influence on companies' cybersecurity stance and in 2019 we cited artificial intelligence and machine learning, digital transformation programs, IT and OT convergence, and the shift to cloud computing as having the most impact on an organisation's security.

Our most recent data reveals only slight changes in that top 5 list as seen in the following table:

Table 2: Technologies having the most impact on an organisation's security

TECHNOLOGY TOP 5	2019	2021
1	Artificial intelligence and machine learning	Artificial intelligence and machine learning
2	Digital transformation	Digital transformation
3	Workflow automation	Workflow automation
4	IT and OT convergence	IoT devices
5	Cloud computing	Agile development

TRA data shows that the adoption of AI and ML in cybersecurity operations has surged between 2019 and 2021 (See Figure 6 following). There is a clear shift towards adopting AI and ML for security approaches, particularly for data analysis, pro-active defence and fraud mitigation, and scanning systems.

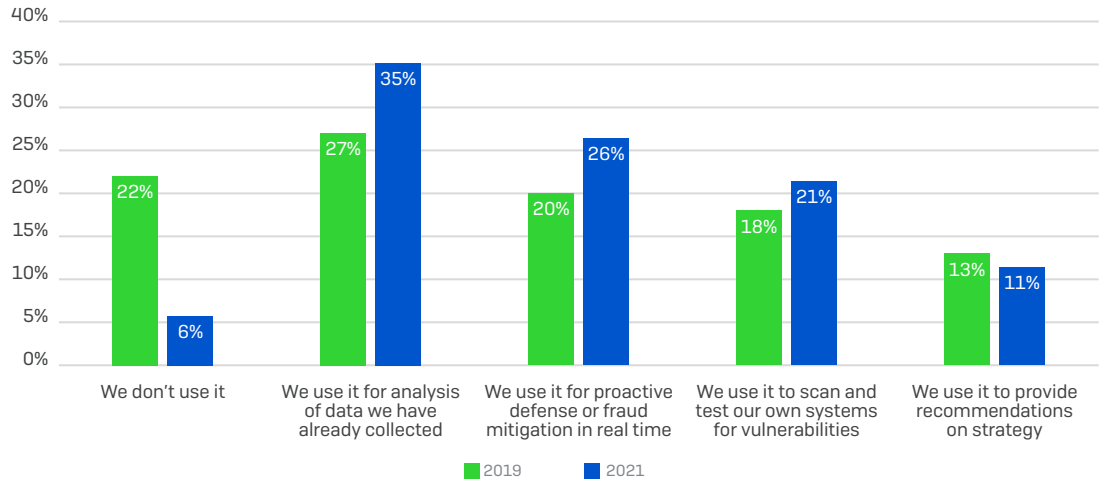


Figure 6: What is the role of AI and machine learning in your organisation's approach to security today?

> "We get attacked more than 15,000 times a day. Recent high-profile attacks have made us strengthen our zero-trust approach."
>
> Philippines Government Agency CISO, Philippines

In Closing

What's different since the first edition of this report in 2019?

The cybersecurity rate of change has increased.

Attacks are coming more frequently, across multiple threat vectors and, according to our data, are becoming more successful. COVID-19 provided an added impetus for companies to refresh their cybersecurity strategies yet the transformational shift to remote working also exposed additional weaknesses. Businesses have transformed their workplace environments, undergone an accelerated period of digitisation and moved to cloud yet continue to confront the same, systemic cybersecurity issues they experienced two years ago, namely, executive apathy, lack of budgets and a dearth of skilled cybersecurity professionals.

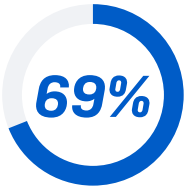
Are we running fast to stand still? Possibly. Yet there are also signs of progress around industry engagement, partnering with cybersecurity experts to help reduce risks and a growing move to harness the power of emerging technologies, especially artificial intelligence and machine learning that suggests organisations are strengthening their capabilities whilst continuing to focus on education and awareness.

As we did with 2019, in the pages following we have provided more insights into the individual country data sets as well as a checklist of issues to consider as you develop your cybersecurity strategy. The report sponsor, Sophos, also shares some compelling perspectives from its position as one of the region's premier cybersecurity solution providers and we hope you find its viewpoint thought provoking.

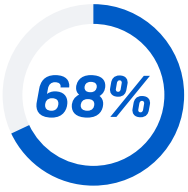
CYBERSECURITY IN AUSTRALIA

Have you been breached?

Australian organisations say they fell victim to a successful cybersecurity attack in the last 12 months



Say this was serious or very serious



Say it took longer than a week to remediate

61% of Australian organisations claim to have a proactive or better security capability in place today, while 10% have no plan or just an ad hoc one.

The number of organisations planning to have a Chief Information Security Officer (CISO) lead their strategy will increase from 37% today to 43% in the next 24 months.

63% agree "My organisation struggles to recruit people with the cybersecurity skills we need."

28% say the number of external security partners they use will increase significantly in the next 12 months.

What is the top mistake your security-related providers make when selling to you? 70% say "not understanding the business problem."

There is an expected increase in the median percentage of technology budgets spent on cybersecurity from 6% today to 9% in the next 24 months.

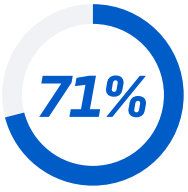
The top technologies or issues Australian organisations think will impact their security in the next 24 months are:

- Artificial intelligence and machine learning
- Public cloud computing
- IT and OT convergence

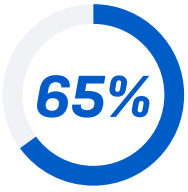
CYBERSECURITY IN INDIA

Have you been breached?

Indian organisations say they fell victim to a successful cybersecurity attack in the last 12 months



Say this was serious or very serious



Say it took longer than a week to remediate

Two thirds of Indian organisations say they have at least a proactive capability when it comes to cyber security: the largest percentage of any country in this research.

The number of organisations planning to have a Chief Information Security Officer (CISO) lead their strategy will increase from 33% today to 40% in the next 24 months.

60% agree "My organisation struggles to recruit people with the cybersecurity skills we need."

27% say the number of external security partners they use will increase significantly in the next 12 months.

What is the top mistake your security-related providers make when selling to you? 75% say "not understanding the business problem."

There is an expected increase in the median percentage of technology budgets spent on cybersecurity from 9% today to 10% in the next 24 months.

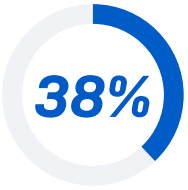
The top technologies or issues Indian organisations think will impact their security in the next 24 months are:

- Artificial intelligence and machine learning
- IT and OT convergence
- IoT devices and blockchain

CYBERSECURITY IN JAPAN

Have you been breached?

Japanese organisations say they fell victim to a successful cybersecurity attack in the last 12 months



Say this was serious or very serious

Say it took longer than a week to remediate

18% of Japanese organisations admit they have no cybersecurity plan or only an ad hoc capability. In contrast, 7% say they have the highest maturity level.

The number of organisations planning to have a Chief Information Security Officer (CISO) lead their strategy will increase from 13% today to 17% in the next 24 months.

60% agree "My organisation struggles to recruit people with the cybersecurity skills we need."

Only 4% say the number of external security partners they use will increase significantly in the next 12 months.

What is the top mistake your security-related providers make when selling to you? 72% say "not understanding the business problem."

There is an expected increase in the median percentage of technology budgets spent on cybersecurity from 5% today to 9% in the next 24 months.

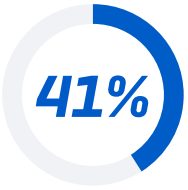
The top technologies or issues Japanese organisations think will impact their security in the next 24 months are:

- Artificial intelligence and machine learning
- Public cloud computing
- IoT devices

CYBERSECURITY IN MALAYSIA

Have you been breached?

Malaysian organisations say they fell victim to a successful cybersecurity attack in the last 12 months



Say this was serious or very serious

Say it took longer than a week to remediate

1 in 10 Malaysian organisations say they have no plan or just an ad hoc one when it comes to cybersecurity. And 33% only have a basic plan in place today.

The number of organisations planning to have a Chief Information Security Officer (CISO) lead their strategy will increase from 41% today to 43% in the next 24 months.

54% agree "My organisation struggles to recruit people with the cybersecurity skills we need."

14% say the number of external security partners they use will increase significantly in the next 12 months.

What is the top mistake your security-related providers make when selling to you? 75% say "not understanding the business problem."

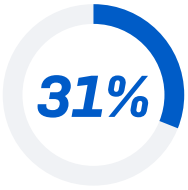
There is an expected increase in the median percentage of technology budgets spent on cybersecurity from 7% today to 10% in the next 24 months.

The top technologies or issues Malaysian organisations think will impact their security in the next 24 months are:

- Artificial intelligence and machine learning
- Public cloud computing
- IoT devices

CYBERSECURITY IN PHILIPPINES

Have you been breached?



Philippines organisations say they fell victim to a successful cybersecurity attack in the last 12 months

Say this was serious or very serious

Say it took longer than a week to remediate

The Philippines has the largest percentage of organisations (30%) claiming to have the highest level of cybersecurity maturity out of all countries in this research.

The number of organisations planning to have a Chief Information Security Officer (CISO) lead their strategy will increase from 37% today to 38% in the next 24 months.

44% agree "My organisation struggles to recruit people with the cybersecurity skills we need."

28% say the number of external security partners they use will increase significantly in the next 12 months.

What is the top mistake your security-related providers make when selling to you? 86% say "not understanding the business problem."

There is no expected increase in the median percentage of technology budgets spent on cybersecurity sitting at 10% today and the same in the next 24 months.

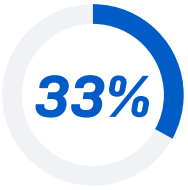
The top technologies or issues Philippine organisations think will impact their security in the next 24 months are:

- Artificial intelligence and machine learning
- IT and OT convergence
- Digital transformation programs

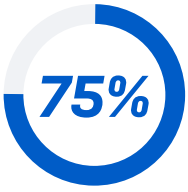
CYBERSECURITY IN SINGAPORE

Have you been breached?

Singaporean organisations say they fell victim to a successful cybersecurity attack in the last 12 months



Say this was serious or very serious



Say it took longer than a week to remediate

53% of Singaporean organisations say they have only an ad-hoc or basic level security strategy in place today.

The number of organisations planning to have a Chief Information Security Officer (CISO) lead their strategy will increase from 25% today to 38% in the next 24 months.

61% agree "My organisation struggles to recruit people with the cybersecurity skills we need."

10% say the number of external security partners they use will increase significantly in the next 12 months.

What is the top mistake your security-related providers make when selling to you? 73% say "not understanding the business problem."

There is an expected increase in the median percentage of technology budgets spent on cybersecurity from 7% today to 8% in the next 24 months.

The top technologies or issues Singaporean organisations think will impact their security in the next 24 months are:

- Artificial intelligence and machine learning
- Blockchain
- Public cloud computing

CYBERSECURITY CHECKLIST

TRA offers the following questions to help your organisation on its cybersecurity journey. It is intended as a starting point and should not replace due diligence efforts.

People and Culture

- **Have you assessed what the customer, employee, and partner experience is like when it comes to security in your organisation?** If you do not have a firm grasp on what the lived experience is for both your customers and employees then you will struggle to implement a successful security culture.
- **Does your organisation have up-to-date knowledge of security vulnerabilities, privacy, and ethics?** Are you able to say confidently that all leaders and appropriate employees are frequently updated in this area?
- **Are you providing training and security skills to all employees in a "just in time" and ongoing fashion?**
- **Do you have the right security leaders and teams in place?** Are they available and helpful to all your business units and know how and why the organisation operates the way it does?
- **Do you provide investment so that employees can obtain the best security certifications?** Including external training with official vendors and certifying organisations.

Policy, Process, and Practice

- **Do you have a trusted partner to audit your processes and create service blueprints and/or journey maps so that you know what binds your organisation together?** This helps with knowledge sharing and gives you a starting point with which to manage the environment.
- **Have you taken the time to observe the actual practices your employees undertake in each process?** Do they match your assumptions or expectations and are they are creating security risks?
- **Are you adopting an agile, sprint-by-sprint, blueprint for improving, digitising, and automating your processes?** Be prepared to adjust the blueprint as circumstances change and make sure you deliver early wins to keep people enthusiastic.
- **Are your security experts (internal and external partners) involved at the start of any attempts to improve or change a process or to create a new one?** Avoid having to retrofit security into already designed processes.
- **Does your organisation already support agile development and/or similar agile approaches for team collaboration or are you heading in this direction?** If so, investigate what peers have done to ensure the workflow has a balance between security and speed.
- **Do you have a robust auditing, penetration testing, and compliance check process?**

Places and Location

- **Do you understand how a workplace is designed and the way security can be enhanced by the way the floor plate (or plan) is laid out?**
- **Have you identified the most likely physical spots where data or document leakage is likely to occur and taken measures to mitigate risk?** Data centres are the obvious starting point but there are many vectors to address including mobile working locations and home offices.
- **How agile and digital are your occupational health and safety efforts?**
- **What is your long-term plan for addressing the convergence?** Physical security is converging with digital and information security – i.e. with machine learning algorithms such as image recognition being combined with CCTV.

Data and Technology

- **Are you planning for an edge-to-cloud world where your security ranges from on-premises environments through to multiple cloud services?**
- **Have you determined what data and documents are critical and need top tier security measures?** You will need to really test your assumptions and make hard decisions.
- **What is your security maturity today?** Aim to exceed the various security maturity frameworks that are available to evaluate your current efforts.
- **Do you have a security and privacy ethics framework?** Make sure you are meeting every one of the legal and ethical obligations around data and documents. This can not only make or break the brand, but also individual careers.

THE SOPHOS VIEW

We can't stress enough the importance of what it means to be cyber resilient. Modern computing platforms, high speed internet links, a heavily distributed workforce and the accelerated adoption of cloud-based technologies has put a massive strain on everybody. While technology administrators need to understand the tools they have deployed and users need to learn how to use them, everyone needs to work together to keep these essential systems as secure as possible to reduce the risk of a cybersecurity incident.

This research by TRA highlights a disturbing attitude that needs to be tackled head on – executives claiming that cybersecurity incidents are exaggerated. This is the biggest hurdle faced by IT leaders when trying to manage cybersecurity. It is confounding that this attitude prevails even when the end of 2020 showed us just how bad a global supply-chain attack could be. If that wasn't enough, the more recent zero-day vulnerabilities in widely deployed email platforms demonstrates the desperate need for unification when it comes to cyber resilience. Everybody needs to play a part. And to play a part, we all need to understand the risk.

Although staff education of the risks through simulated phishing attacks and tabletop exercises that emulate a cyber hack have incrementally increased awareness within most organisations, there is still a gap between cybersecurity maturity and risk acceptance.

Tackling the perceived exaggeration of cybersecurity risk at the board and executive level requires not only a highly skilled and knowledgeable group of people, it also heavily mandates trust. However, trust is seldom granted on demand; it takes time to establish a level of trust where a conversation around cybersecurity maturity and the actions needed can be positively adopted and driven from the top down. This is where cybersecurity professionals, working in the capacity of a provider to an organisation, can have a great influence on how a business should constantly evaluate its cybersecurity maturity and put in place actions to bring it up a level.

Observationally, many organisations need or want help or, at the very least, guidance on whether the things they're doing are the right things. As the saying goes, many hands make light work, and although some organisations have outsourced to a specialised detection and response cybersecurity provider, there are some that assume that these services are excessive. Challenge yourself as a cybersecurity professional to provide the advice to change these assumptions and to reinforce that the risk to the organisation of doing nothing and assuming that things can't be 'that bad' is significant. Too many organisations have fallen victim to high-profile extortion and data theft leaving them with a long and costly road to recovery – if, in fact, they recover at all.

DEMOGRAPHICS, DEFINITIONS AND METHODOLOGY

In preparing this report we followed a blended methodology of quantitative survey research and qualitative virtual CXO roundtable engagements to ensure we had a holistic view of the cybersecurity issues.

The research was conducted throughout December 2020 and January 2021 with the survey sampled from IT and cybersecurity executives and decision makers in 900 companies across Australia, India, Japan, Malaysia, Philippines and Singapore. Only companies with 150+ employees were eligible to participate.

The virtual roundtables were held in Australia, India, Japan and Singapore (with ASEAN representation) with senior representatives from a diverse range of organisations spanning everything from financial services, utilities, manufacturing through to health, professional services and retailing.

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.

About Sophos

As a worldwide leader in next-generation cybersecurity, Sophos protects more than 400,000 organizations of all sizes in more than 150 countries from today's most advanced cyber threats. Powered by SophosLabs and SophosAI – a global threat intelligence and data science team – Sophos' cloud-native and AI-powered solutions secure endpoints (laptops, servers and mobile devices) and networks against evolving cyberattack techniques, including ransomware, malware, exploits, data exfiltration, active-adversary breaches, phishing, and more. Sophos Central, a cloud-native management platform, integrates Sophos' entire portfolio of next-generation products, including the Intercept X endpoint solution and the XG next-generation firewall, into a single "synchronized security" system accessible through a set of APIs. Sophos has been driving a transition to next-generation cybersecurity, leveraging advanced capabilities in cloud, machine learning, APIs, automation, managed threat response, and more, to deliver enterprise-grade protection to any size organization. Sophos sells its products and services exclusively through a global channel of more than 53,000 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. 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

2021-03-26 EN (PC)

SOPHOS