

WHITEPAPER

Securing the Future:

Asia Pacific Cybersecurity
Readiness Survey



Content

3	Executive Summary
4	Methodology
5	Navigating a complex threat environment
6	Frequency of cybersecurity incidents rising
11	Competing priorities in advancing preparedness
13	Budgets stepping up to the challenge
14	Bolstered spending does not mean greater results
15	The price of failing to prepare
17	Recommendations
18	Glossary



Executive Summary

In this study, we set out to build a better understanding of the threat landscape facing Chief Information Security Officers (CISOs) and their teams across the vast and varied territories of Asia Pacific and the actions driving positive results and outcomes. The results are both illuminating and worrying.

Amid a grappling for control, we see organizations of every size, in every industry, and every market in the region facing a rising number of cyber threats. Over three-quarters (78%) of the more than 4,000 cybersecurity professionals we interviewed from 14 markets across the region experienced at least one cybersecurity incident in the past 12 months. Almost the same number (76%) said that the number of incidents had risen. Of these, 80% reported experiencing four or more incidents, and half experienced more than 10.

Web attacks emerged as the number one threat across most markets surveyed, with bad actors primarily aiming to plant spyware. However, the number of threat vectors continues to multiply in our increasingly hybrid working world.

In this environment, diligent CISOs and their teams have clearly stepped up their preparations, which was evident with nearly nine out of ten reporting reduced time to resolve incidents. However, this study finds that overall perceptions of cybersecurity preparedness are still lagging, with only 38% of respondents describing their organizations as 'highly prepared' for cybersecurity incidents, with user protection as the area most lacking in preparedness.

Cybersecurity architectures continue to remain a patchwork for many, with a small proportion reporting 'mature' deployment, and many rating themselves as only 'somewhat prepared' to tackle incidents. Many are resolving this by increasing the number of products they use, with mixed results. In fact, this study finds that increasing the number of solutions in the face of growing threats does not appear to be an effective response.

Other pressing challenges include the talent crunch, which is a key issue for most respondents (60%). Insufficient funding also remains an issue, although there are signs that increasing executive visibility on these is positively affecting budgets with many reporting increased investment for the year ahead.

Given the talent crunch, financial resources, and time required to manage an array of solutions, and the indication that less may be more, organizations with simpler security architectures are likely to be more agile and effective in handling attacks.

Smarter allocation of resources is further needed to mitigate losses. Our findings show that the vast majority of respondents' organizations saw financial losses of at least US\$1M over the past 12 months, as well as accompanying reputational loss.

As we look to achieve a more secure future, my hope is that this report will provide useful reading and inspiration for CISOs and cybersecurity teams in the region looking to achieve a better understanding of the cybersecurity risks at play, and how to achieve greater outcomes for their organizations.

Yours Sincerely,

Grant Bourzikas
SVP & Chief Security Officer

Methodology

The report is based on the findings of a double-blind survey conducted in July 2023 of 4,009 leaders responsible for cybersecurity in their organizations, including executive leadership, security leadership, security management, and technical leadership for cybersecurity.

The respondents interviewed were based in 14 markets across Asia Pacific: Australia, China, Hong Kong SAR, India, Indonesia, Japan, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Taiwan, Thailand, and Vietnam.

They were drawn on a roughly equal basis from small (150 to 999 employees), medium (1,000 to 2500 employees), and large (more than 2,500 employees) organizations across a wide range of industries: Business & Professional Services; Construction & Real Estate; Education; Energy, Utilities & Natural Resources; Financial Services; Gaming; Government; Healthcare; IT & Technology; Manufacturing; Media & Telecoms; Retail; Transportation; Travel, Tourism & Hospitality.

By country:		number of respondents	
309	Australia	426	China
302	Hong Kong SAR	403	India
211	Indonesia	303	Japan
207	Malaysia	230	New Zealand
203	The Philippines	297	Singapore
291	South Korea	349	Taiwan
224	Thailand	228	Vietnam

Navigating a complex threat environment

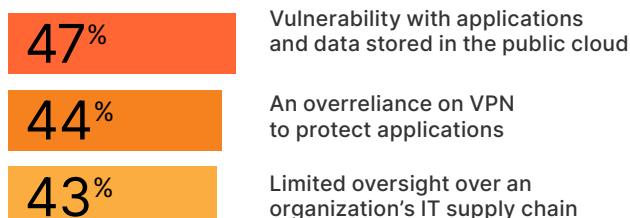
CISOs and their teams are operating in an increasingly complex and changeable environment. Our study finds that the top three challenges for cybersecurity leaders in the region are now: securing a hybrid workforce (51%); defending against cyberattacks (48%); and deploying Zero Trust architectures (42%).

Top challenges for Asia Pacific cybersecurity leaders:



This is amplified by a myriad of issues that must be navigated to develop a resilient and fit-for-purpose cybersecurity posture. Respondents rate the top issues with their cybersecurity architecture as vulnerability with applications and data stored in the public cloud at 47%; an overreliance on VPN to protect applications at 44%; and limited oversight over an organization's IT supply chain at 43%. These issues highlight, among other things, an interesting challenge for CISOs and a potential headache for businesses, with cybersecurity shifting beyond its traditional silo to become a truly cross-organization discipline.

Top issues with current cybersecurity architecture:



Bad actors are all too aware that common IT practices driven by CIOs open up vulnerabilities, creating significant and ongoing security headaches. This is an urgent issue, not just for CISOs, but for organizations at large.

Frequency of cybersecurity incidents rising

These challenges are amplified in an increasingly high-intensity threat landscape. A year on from the end of the pandemic across Asia Pacific, with post-pandemic working patterns becoming more established, the study finds that the frequency of cybersecurity incidents in the region continues to grow.

Over three-quarters (78%) of our respondents experienced a cybersecurity incident of some kind in the past 12 months with those working for medium-sized organizations the most likely to be affected.

% reporting cybersecurity incident in the past 12 months

78%

experienced a cybersecurity incident in the past 12 months.

By organizational size:

77%

Small organizations



81%

Medium organizations



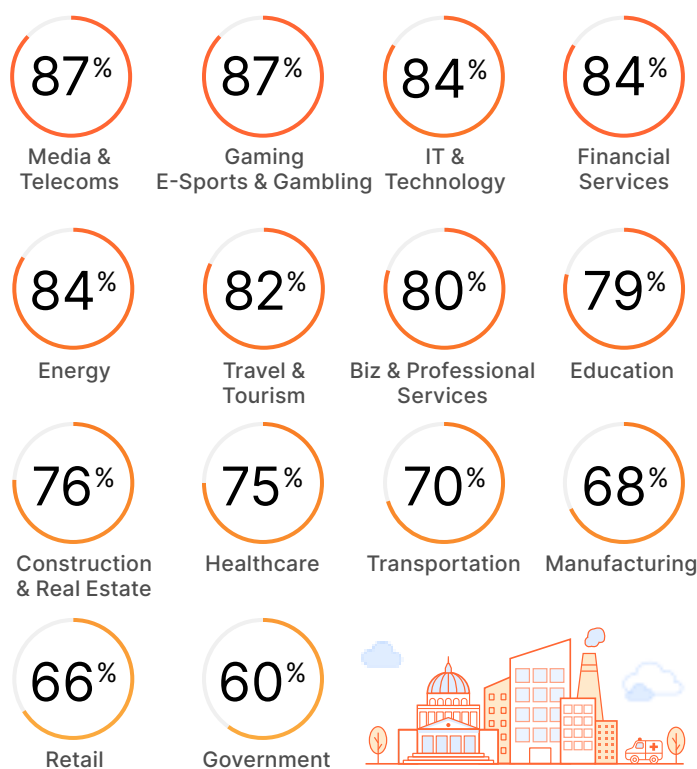
74%

Large organizations

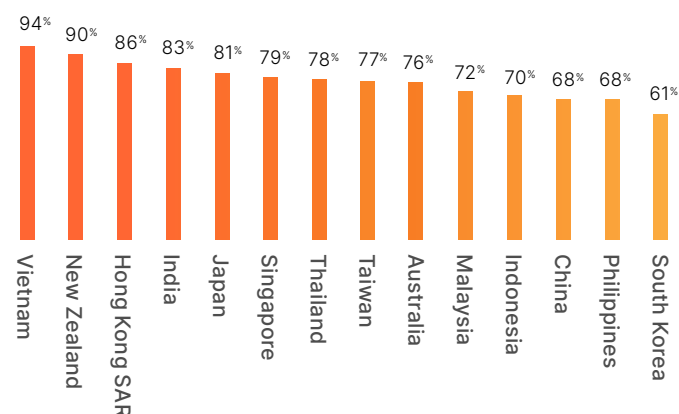


There are significant disparities across industries and our survey shows that technology-led industries – such as Gaming and Media & Telecommunications – are those most vulnerable to incidents, which is a trend seen throughout this report.

By industry: % reporting at least one cybersecurity incident in past 12 months



By market: % reporting at least one cybersecurity incident in past 12 months

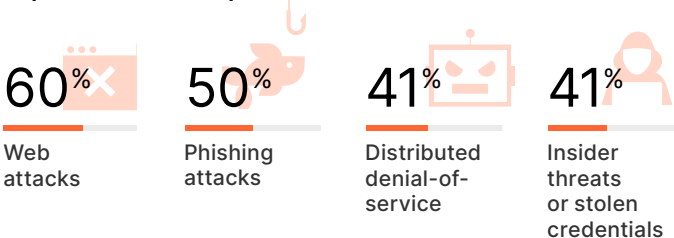


Our study further reveals that cybersecurity breaches are not one-off incidents. Among respondents from organizations experiencing incidents in the past year, 80% reported four or more cybersecurity episodes, while 50% have experienced 10 or more. Smaller businesses are slightly less likely to be affected than their larger peers but, as we discuss later, this is potentially a consequence of less sophisticated cybersecurity architectures being less able to detect attacks. Respondents in New Zealand (68%), Hong Kong SAR (67%) and Vietnam (64%) reported more than 10 incidents in the past 12 months.

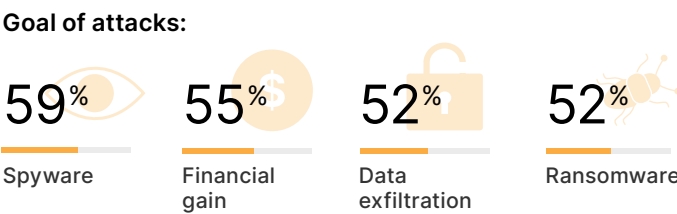
Organization size	4+ incidents	10+ incidents
Total	80%	50%
Large	80%	51%
Medium	81%	54%
Small	77%	46%

When looking at the types of incidents occurring, web attacks are now the most common form of attack, replacing phishing as the key vector shown in other surveys. Respondents most commonly report web attacks (60%), followed closely by phishing attacks (50%).

Types of cybersecurity attacks experienced in the past 12 months:



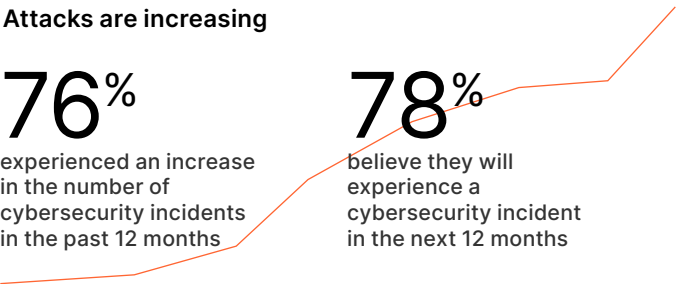
For most respondents, the goal of most attacks is to plant spyware. This occurred in well over half of the attacks (59%) in the past year, no doubt laying the groundwork for future assaults. Financial gain (55%), data exfiltration (52%), and planting ransomware (52%) made up the rest of the top four objectives for bad actors.



Top aim	Industries where this was the top aim	Top industries impacted
Planting spyware	Education, Energy, Government, IT & Technology, Manufacturing, Media & Telecommunications, Retail, Travel & Tourism	Media & Telecoms (72%), Energy (69%), Travel & Tourism (69%)
Financial gain	Business & Professional Services, Construction & Real Estate, Energy Financial Services	Energy (69%), Financial Services (68%), Media & Telecoms (67%)
Ransomware	Gaming (E-sports and Gambling)	Gaming (65%), Media & Telecoms (63%), Construction & Real Estate (57%)
Data exfiltration	Government, Healthcare, Transportation	Healthcare (64%), Transportation (62%), Construction & Real Estate (57%)

*Government = spyware + data exfiltration joint top; Energy = spyware + financial gain joint top.

This trend looks set to continue as we consider the rest of 2023 and into 2024; over three-quarters (76%) say the number of incidents have risen in the past 12 months.



Respondents from New Zealand (89%), Thailand (87%), and Vietnam (86%) were most likely to report an increase in incidents in the past 12 months. Interestingly, while there are significant variations from industry to industry, the industries reporting increased cyber incidents vary from the previous analyses. This indicates perhaps that malign actors are looking for rich pickings when they identify their targets – opportunities to maximize returns from an attack.

By industry: Percentage by industry reporting at least one cybersecurity incident in 12 months.



Looking ahead, CISOs and their teams across the region see significant challenges on the horizon, with nearly eight in ten (78%) believing their organization will experience some kind of cybersecurity incident in the next year. Those in what we have already seen to be vulnerable industries – Gaming, Media & Telecommunications – are most likely to express pessimism, while only two-thirds of respondents in Government believe they will experience an attack in the next 12 months.

The proportion of respondents describing the probability of attacks as “very likely” in Vietnam dwarfed that in other markets at 75% compared to a 23% regional average.

By industry: Percentage by industry expecting at least one cybersecurity incident in next 12 months.



Most respondents are worried about malware attacks in the next 12 months. This ranks as the top concern for 37% of respondents, with ransomware and spyware the second most worrying attack vector (ranked number one by 15%). Despite phishing accounting for the second highest number of incidents in the previous 12 months, this form of attack ranks third as a concern when looking ahead for the next 12 months.

Preparedness remains low

Despite the increasing frequency of cybersecurity incidents, less than half (38%) count themselves as ‘highly prepared’, and just over half believe they are ‘somewhat prepared’.

Preparedness remains low

Less than half of organizations are highly prepared for cybersecurity incidents:

38% Overall cybersecurity	40% Network security
42% Data security	38% Application security
41% Device security	37% User security

Perhaps in response to the greater threat vectors, CISOs in technology-led industries tend to be better prepared than their counterparts in other industries. The industries most likely to report high levels of preparedness are Retail (44%), Media and Telecommunications (44%), IT (40%), and Transport (40%). This contrasts with those in Healthcare (16%), Education (13%), Government (10%), and Tourism (10%) who are most likely to report they are 'unprepared' to withstand an attack. It is worth noting, though, that these industries also often face budgetary challenges, or have to deal with legacy systems.

The proportion of respondents reporting high preparedness differs significantly across markets. Only 20%, 21% and 24% of those surveyed in South Korea, China and Taiwan claimed to be highly prepared. Despite the aforementioned high levels of reported attacks in Vietnam, respondents there are by far the most likely to describe their organizations as highly prepared (78%), compared with an average of 38% across markets.

Data is the security pillar where preparedness is the highest, likely due to the potential cost of weak endpoint security, while preparedness around users is lowest.

42% are highly prepared for securing their data. (40% of small organizations vs 44% of large organizations)

41% are highly prepared when it comes to their devices.

40% are highly prepared when it comes to their networks.

38% are highly prepared when it comes to their applications.

37% are very prepared when it comes to their users.

While these levels are perhaps not where every organization would want them to be, there are positive signs though, with 46% having started their journey.

As may be expected, larger organizations are better prepared across the key pillars of cybersecurity in comparison to their smaller counterparts. This is perhaps unsurprising, given the relative size of cybersecurity budgets, although larger organizations have a more complex operating environment, which can lead to delays in rolling out measures.

CISOs face a difficult task when it comes to deciding which area of cybersecurity to prioritize. They know attacks are coming from numerous directions, but budgetary constraints, as well as limited expertise and time mean they need to optimize focus, and for many that focus is around networks. 90% of our respondents claim to have deployed solutions around this area, notably higher than data (85%), users (85%), devices (84%), and applications (83%).

Again, our respondents from the Healthcare industry lag behind their peers with around a quarter saying they do not have solutions deployed in each of the five areas of cybersecurity.

24% have no solutions currently deployed to secure networks

23% have no solutions currently deployed to secure applications

27% have no solutions currently deployed to secure devices

23% have no solutions currently deployed to secure data

28% have no solutions currently deployed to secure users

However, more than three-quarters of healthcare respondents that do not have solutions deployed have plans to rectify this in the next 12 months.

One side-effect of increased cybersecurity preparedness is that many respondents report an increased volume of incidents over the last 12 months. It appears that with preparedness, cybersecurity teams tend to be more capable of detecting intrusions, hence the higher number of reported incidents.

The link between preparedness and detection is clearly seen in the incidence of various attacks reported by the highly prepared, prepared and unprepared over the last 12 months, particularly looking at DDoS, insider/ stolen credentials, and supply chain attacks:

Attack type detected	Highly prepared	Somewhat prepared	Unprepared
Phishing	50%	51%	40%
Web attack	60%	62%	53%
Distributed Denial-of-Service (DDoS)	45%	39%	38%
Insider threat / stolen credentials	46%	37%	38%
Public facing application(s)	40%	35%	27%
Zero Day exploit	29%	25%	20%
Supply chain attack	38%	30%	22%
Business email compromise	32%	29%	30%
Exploit of disclosed vulnerability	13%	12%	11%

Competing priorities in advancing preparedness

For most CISOs, the key to preparedness is to ensure they are covering major holes in their security architecture. Around a fifth of our respondents say they do not have MFA (19%), CASB (19%), or browser isolation solutions (19%).

For many, a key element of their preparation is fully implementing SASE, and here, there are encouraging developments, with 80% of respondents reporting they are at a 'developing' or above stage of rollout, and only a small proportion (4%) are at an early stage, or are yet to start their SASE journey.

These implementation numbers also align with the strategic intentions of security leaders. A quarter (25%) rank moving towards a SASE architecture among their top three priorities.

Implementation levels of processes and tools are very similar across businesses of all sizes with 40% reporting 'mature' implementations for Zero Trust, endpoint protection platform (EPP) and data encryption rollouts. The one notable exception is extended detection and response (XDR), where just 29% of respondents report maturity in their implementation compared to other solutions.

Although encouragingly, nearly half (49%) are part way through their rollouts indicating a maturing of adoption.

	Mature implementation	Partial implementation
Browser isolation	36%	43%
Cloud access security broker (CASB)	38%	43%
Data encryption	44%	38%
Endpoint protection platform (EPP)	36%	42%
Extended detection and response (XDR)	29%	49%
Multi-factor authentication (MFA)	38%	43%
Zero Trust Network Access	33%	48%

As noted, Zero Trust deployment is a key priority for many organizations, and while the technology is new, it is rapidly growing. Zero Trust Network Access had the highest rate of partial deployment among all solutions, indicating that deployment levels will eventually catch up with other solutions. 42% of respondents also ranked the deployment of Zero Trust as one of top three strategic priorities for their organizations.

The talent crunch

Grand ambitions may, however, continue to be hampered by execution challenges. A lack of talent was cited by 60% of respondents when discussing challenges to cybersecurity preparedness. These figures are particularly high in Japan (72%), along with Malaysia and Vietnam (71% each). Respondents citing a lack of talent as a key barrier also reported a greater number of incidents over the past 12 months.

The talent crunch



Lack of talent is a barrier to greater cybersecurity preparedness for 60% respondents, and correlates with experiencing more incidents and a reduced ability to resolve them quickly.

Sufficient talent Insufficient talent

10+ incidents in past 12 months

47% 54%

Able to resolve a cybersecurity incident within 12 hours

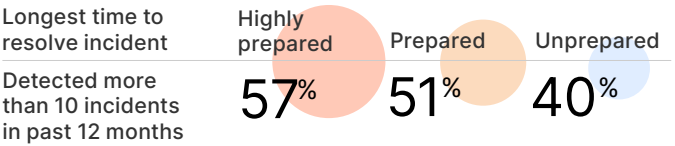
80% 77%

Clearly, the war for talent in cybersecurity is having an impact but not just on preparation. This talent crunch intensifies once an organization begins to multiply its cybersecurity solutions. Our findings show clearly that the more solutions an organization has in its architecture, the more likely they are to experience a talent crunch. In fact, two-thirds (65%) of organizations with 15 or more cybersecurity solutions are likely to report talent shortages compared to three in five (60%) of those with fewer than 15.

The case is clear — preparedness is driving results

Solution rollouts are also a critical part of CISO preparation, and our study shows this clearly ,with a strong correlation seen between preparedness and better security outcomes across the major areas of cybersecurity. For many respondents, preparation really is key to effective performance. The findings reveal that preparedness correlates with a greater ability to detect and manage cybersecurity incidents and attacks, and to resolve them sooner.

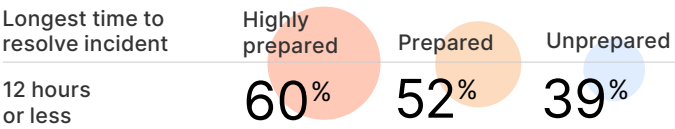
Preparedness level vs cybersecurity incidents detected:



Preparedness level vs cyberattacks detected:

Attack type detected	Highly prepared	Prepared	Un prepared
Phishing	50%	51%	40%
Web attack	60%	62%	53%
Distributed Denial-of-Service (DDoS)	45%	39%	38%
Insider threat / stolen credentials	46%	37%	38%
Public facing application(s)	40%	35%	27%
Zero Day exploit	29%	25%	20%
Supply chain attack	38%	30%	22%
Business email compromise	32%	29%	30%
Exploit of disclosed vulnerability	13%	12%	11%

Preparedness level vs longest time to resolve an incident:



Budgets stepping up to the challenge

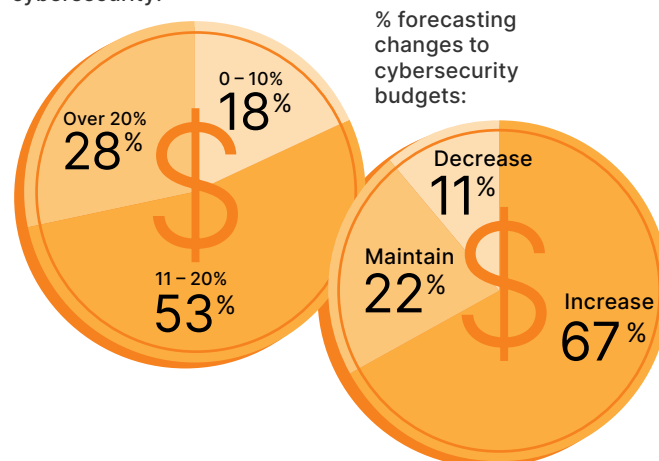
For many, preparation is no doubt helped by investment. In the past 12 months, more than half (53%) spent between 11% and 20% of their organization's entire IT budget on cybersecurity, while a further 28% spent 21% or more. Less than a fifth (18%) spent under 10% on their cybersecurity preparedness. Organizations in Vietnam, the Philippines (43% each) and Japan (40%) indicated that their organizations allocate more than 21% of IT budgets to cybersecurity. As we have seen elsewhere in this report, size does matter, and cybersecurity preparation is no different. Over a third (35%) of large organizations spent more than a fifth of their IT budget on cybersecurity products, solutions, and staffing. This is an order of magnitude higher than those in medium-sized and small organizations where just 26% spent more than a fifth of their IT budget on cyber preparedness.

Interestingly, given the state of preparation across industries, Healthcare was one of the three types of organizations spending the most, alongside Transportation and Finance, demonstrating that higher budgets do not necessarily equate to higher states of readiness. By contrast, organizations in Education, Gaming, Government, and Manufacturing are those most likely to have spent between 1% and 10% of IT budgets on cybersecurity preparations. Looking ahead, two-thirds (67%) of all respondents expect bigger budgets in the next 12 months and another fifth (22%) expect to maintain their current expenditure levels. Industries that might be considered critical to daily life – Finance, Healthcare, and Transportation – foresee higher spending thresholds, while those that may be more negatively impacted by the economic environment – such as Retail and Manufacturing – forecast budget reductions.

For many, there are significant budget increases ahead. Of those who thought their budget would rise over the next 12 months, nearly half predicted an increase of between 11% and 20%. As you might expect, 37% of respondents from large organizations believe they would be on the receiving end of this type of windfall, compared to just 27% of their peers in small businesses.

Budgets stepping up to the challenge

% of IT budgets spent on cybersecurity:



And the key drivers of budget increases? Three in five (60%) respondents say the rate of cybersecurity incidents is the most significant factor, while 55% believe it is the financial impacts of previous incidents. Making up the top three factors is an assessment of the current cyberthreat landscape, which is a factor for 45% of respondents. Among the minority of organizations expecting to see a decrease in budgets, most think the cuts will fall between 11% and 20%. Organizations in Manufacturing (48%), Retail (50%), and Transportation (54%), in Asia Pacific will most likely be the hardest hit with budget cuts of more than 20%.

Bolstered spending does not mean greater results

The challenges faced by CISOs have led to a mosaic of products and solutions for many cybersecurity teams with most saying they now have between six and 15 products in their architecture. Larger organizations tend to have a more complex array of products though, with almost twice as many having more than 20 in their architecture compared to their medium-sized peers. Interestingly, medium sized businesses are less inclined to use more products than their larger counterparts. Our research shows that large firms – those with over 2,500 employees – are more than twice as likely to have 20+ solutions. This may stem from larger budgets for product acquisition as well as the resources to hire teams to implement and manage them. Juggling multiple cybersecurity solutions has somewhat negatively impacted cybersecurity effectiveness – hinting that organizations should be looking for more simplicity.

Purchasing and managing a larger number of solutions is generally more costly. Organizations already dealing with the aforementioned talent crunch will be even more hard-pressed to find staff to manage often-overlapping solutions. 65% of organizations with more than 15 cybersecurity solutions reported talent shortages, compared to 60% of organizations with less than 15 solutions.

Yet a common response to recent cybersecurity incidents is to increase the number of solutions deployed, indicating a mismatch in priorities. Nearly a third (31%) of respondents from organizations which had experienced incidents within the past three months reported that their organizations would significantly increase the number of cybersecurity solutions within the next 12 months, compared to 21% of the overall respondent group.

Marked differences in performance are seen in those with more and less solutions. Those with less solutions performed better:



Using budgets judiciously – increased or not – is a challenge for every CISO. For many, there are three clear criteria they use when they bring in third parties to provide tools or solutions.

Of these, the most important (59%) is choosing vendors with whom they already have a relationship or have had one in the recent past. Naturally, best-in-breed products rank high as a selection criteria for 53%, as is their ability to choose their own products (52%), rather than have them preselected by others in the organization. Cybersecurity teams in larger organizations seem to have more latitude to choose the products they want, with 55% of respondents reporting that they were given responsibility for product choice rather than having to choose best-in-breed products.

The price of failing to prepare

The US' Federal Bureau of Investigation ("FBI") received more than 800,000 reports of cybercrimes in 2022¹ – that's around one every minute and a half. It is no wonder that the cost of cyber incidents is rising exponentially every year, a fact endorsed by our respondents with 63% reporting the financial impact on their organizations was at least US\$1M during the past 12 months. It is not just large organizations that experience these significant losses. 61% of small and 72% of medium sized businesses lost at least a million dollars through cyber incidents. Respondents from organizations in Hong Kong (91%), New Zealand (83%) and South Korea (81%) are most likely to report financial impacts of greater than US\$3M over the past 12 months. Around one in seven of all respondents (14%) suffered a loss of more than US\$3M, with larger businesses naturally experiencing this at a greater rate (21%), compared with medium (14%) and small (8%) businesses.

The price of failing to prepare

Financial impact of cybersecurity incidents over the past 12 months by organization size:



	Total*	Small	Medium	Large
US\$1M <	31%	39%	28%	26%
> US\$1M	63%	54%	69%	65%

*Remaining respondents indicate they are unsure about financial impact

While the financial cost is clearly the most direct impact, it is not the only effect. 16% of respondents rated reputational damage as the biggest impact while 21% rated loss of data or Intellectual Property (IP) as the most important outcome. In fact, data loss is the most frequently cited outcome of a cybersecurity incident for organizations over the past 12 months, and it can have dramatic consequences.

For example, 30% reported layoffs as an outcome of data loss, while 26% had legal action brought against them. Regulators too have much to say about data loss. Around a third (33%) of respondents say their organization reported breaches to the relevant authorities. Just over a quarter (26%) ended up paying a fine and the same number faced legal action.

	Overall	Small	Medium	Large
Data impact				
Customer and client data	58%	60%	57%	58%
Employee data	58%	57%	61%	54%
Proprietary data	53%	49%	54%	56%
Financial data	50%	49%	53%	50%
Business impact				
Loss of reputation	29%	29%	25%	35%
Lost revenue	28%	30%	25%	30%
Lost employees	10%	11%	8%	12%
Lost customers	17%	18%	15%	19%
Business response actions				
Forced layoffs	30%	30%	29%	30%
Business plans on hold	40%	39%	41%	40%
Temporary suspension of operations	35%	33%	38%	34%
Reduced or restricted hybrid work	42%	39%	44%	44%
Legal and regulatory consequences				
Paid fine(s)	26%	26%	25%	28%
Disclosed incident(s) to authorities	33%	31%	34%	33%
Experienced legal action	26%	26%	26%	25%

¹ <https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-in-2022-fbi/>

As we saw earlier, the majority of CISOs feel they are at least somewhat prepared to tackle cybersecurity incidents. These efforts are contributing to resolution times with nearly nine out of ten (87%) reporting they were able to deal with incidents more quickly in the past 12 months. These decreased response times are the result of a range of different factors.

Factors responsible for opportunities and challenges:

60%	Better security culture	55%	Right talent
52%	A clear attack playbook	51%	Investment in technology
46%	Better coordination with stakeholders	38%	Better monitoring and detection platform

However, it is not all positive news when it comes to incident response, and notably, three-quarters of our respondents say dwell times have increased, with more than a fifth (22%) saying dwell times have gone up significantly. This is most evident in Media & Telecommunications, where 88% of organizations experienced an increase in dwell times, with IT & Technology not far behind at 79%. Government (61%) and Retail (66%) were least likely to have experienced increased dwell times.

It is not only the incidence of dwell times that should concern CISOs, it is the average dwell times reported by respondents. Two-thirds said bad actors had access to their systems for 12 or more hours and 42% experienced an average dwell time of 24 hours. This resulted in significant downtime for many, with 83% reporting an impact on their organization’s functional ability of more than three hours. One in six (17%) said their organization was affected for nine hours or more.

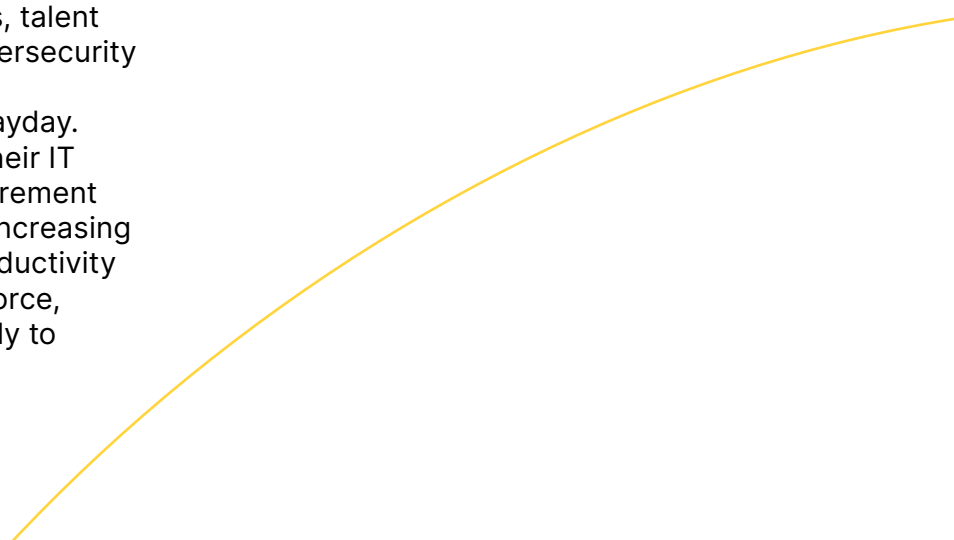
Recommendations

1. The right preparation is everything. Organizations should strategically invest in consolidated solutions and respond to an increasingly complex threat environment through approaches such as Zero Trust.
2. Less is more when it comes to the number of solutions deployed – streamlining security architecture through SASE allows organizations to mitigate the impact of the industry-wide talent crunch and improve cybersecurity outcomes.
3. Spend time enhancing the security culture among the board and the rest of the company. Strong understanding and awareness should be the first line of defense in enhancing preparedness.
4. Through building a strong security culture, CISOs will no longer have to wait for incidents to occur to make the business case for boosting preparedness, empowering them to proactively mitigate the risk of grave financial loss.
5. Cybersecurity must not exist in a silo. Senior executives should view cybersecurity as mission critical, and organizations should take a holistic approach in ensuring their staff, suppliers, and clients adhere to best practices.

Cloudflare can help your organization adapt to the cybersecurity challenges of today, regardless of where your organization is when it comes to the implementation of cybersecurity measures or the levels of preparedness amongst your security teams. Cloudflare's platform can help organizations of any size, at any stage of implementation, and with any level of preparedness to simplify cybersecurity, compensate for talent constraints, and robustly defend against any type of cyber threat.

To learn more about Cloudflare's suite of solutions and request a demo or POC from a sales representative, please visit: <https://www.cloudflare.com>. We will help evaluate your existing security posture and collaborate towards an action plan for how Cloudflare can help you strengthen your cybersecurity for your people, applications, devices, networks, and data.

The study has revealed that many organizations in Asia Pacific are facing and will continue to face numerous challenges across the spectrum – be it budgetary constraints, talent shortage, an increasingly complex cybersecurity landscape, or the growing audacity of cybercriminals looking for their next payday. Many organizations have invested in their IT infrastructure as a result, but the requirement to protect the organization from ever-increasing external threats, while maintaining productivity and dealing with a more remote workforce, means that investment for many is likely to continue.



Glossary

Cybersecurity roles

Security Leadership = involved in defining organization's security posture

Security Management = involved in running day-to-day of security team

Technical = involved in providing technical support expertise in areas such as engineering, architecture, response and intelligence

Implementation stages

Full implementation = 100%

Advanced implementation = 76-99%

Developing implementation = 51-75%

Partial implementation = 26-50%

Early stage implementation = 25%<

Maturity (Zero Trust examples)

Infancy = implemented MFA

Developing = no more VPN, enhanced endpoint protection

Mature = segment network access, using Internet for branch connectivity

Very mature = Protect applications from Layer 7 attacks (DDoS, injection, bots, etc), have dedicated Zero Trust practitioners, CZTO, etc.



© 2023 Cloudflare Inc. All rights reserved.
The Cloudflare logo is a trademark of Cloudflare. All other
company and product names may be trademarks of the
respective companies with which they are associated.

1 888 99 FLARE | enterprise@cloudflare.com | [Cloudflare.com](https://cloudflare.com)

REV:BDES-4859.2023AUG22