CLOUDFLARE

Navigating the New Security Landscape: Asia Pacific Cybersecurity Readiness Survey

Content

Executive summary

As the Chief Security Officer at Cloudflare, I have the privilege of speaking with many of my peers, CEOs, and board members across various industries. In our discussions, one question always comes up: "Are we secure?"

It is a simple question that is nearly impossible to answer. One way is to liken cybersecurity to personal wellbeing. While someone might be healthy today, they may not be healthy tomorrow. Similarly, while a company's cybersecurity posture may not be compromised today, that might not be the case tomorrow.

It is also clear from these discussions that the same type of cybersecurity issues continue to comprise the operational 'health' of many organizations in this region. A year on from the publication of our inaugural Asia Pacific Cybersecurity Readiness Survey, the findings of our latest study show that 41% of the 3,844 respondents experienced a data breach between 2023 and 2024, with 76% reporting an increase in the number of breaches their company had sustained during the same time period. Those respondents representing IT & Technology, Media & Telecoms, Retail, and Financial Services reported the greatest increase in attacks over the last 12 months.

Added to this growing number of cyberattacks is a 29% decrease in the percentage of respondents who felt prepared to defend against them. This is a worrying prospect, particularly when 51% of respondents reported a financial loss of more than USD 1 million due to data breaches.

The combination of financial losses, budgetary pressures, the responsibility of securing technology for business transformation, managing an expanding list of IT vendors and solutions, and emerging risks like AI-powered attacks has plunged organizations into a crisis of complexity.

In fact, 86% of respondents revealed that complexity is making their organization more vulnerable to attacks. This complexity is evidenced by survey findings revealing that 49% of respondents had deployed more than 20 security tools, with 82% adding more vendors and tools this year alone.

To effectively address complexity, something needs to change.

Firstly, organizations need to double down on AI, lest they risk becoming obsolete. 87% of respondents said AI has been used either to facilitate an increased number of attacks on their organisations, or is making attacks more sophisticated. However, only 28% believe they are highly prepared to mitigate AI-powered attacks. While AI has given rise to new cyber-related threats, it is also a key driver for business transformation, productivity, and growth. Organizations must look ahead, today, and map out what advantages emerging AI technologies could potentially bring to their cybersecurity strategies in the future.

Secondly, driving towards operational resilience is vital to the success of any organization, and it goes hand in hand with robust cybersecurity plans. Resiliency has to be baked into any cybersecurity strategy well ahead of any mandates put in place by regulators. Recent global cybersecurity events have brought into sharp focus the challenges that can come with not having modern, resilient infrastructure or a well-thought out plan in the case of any crisis.

Finally, it is important to act now to drive out complexity. With nearly 90% of respondents reporting that complexity is making their organization more vulnerable to attacks, the need to act with urgency is critical. Consolidate your security and technology stack, streamline processes and modernize IT architectures, shift resources to ensure business outcomes, and start to transform your cyber workforce to enable the deployment of AI-powered solutions. This is how we will change the historical outcomes our industry has faced over the past 20 years.

I hope this report helps my peer CISOs and their teams manage the challenges of the next 12 months, as well as provide guidance on how to seize new opportunities. The insights gleaned from this report should ideally help CISOs identify roadblocks when navigating the complexity in cybersecurity stacks, make more informed decisions on how to tackle the emerging paradigm of AI-powered threats and opportunities, strategically recalibrate resources to overcome talent constraints, and figure out how to best navigate the web of regulations. There is much to be done to keep organizations safe from increasingly sophisticated attacks so the learnings from others in similar positions may provide much-needed inspiration to prepare you to answer that all important question: “Are we secure?”.

Yours sincerely,

Grant Bourzikas
SVP & Chief Security Officer

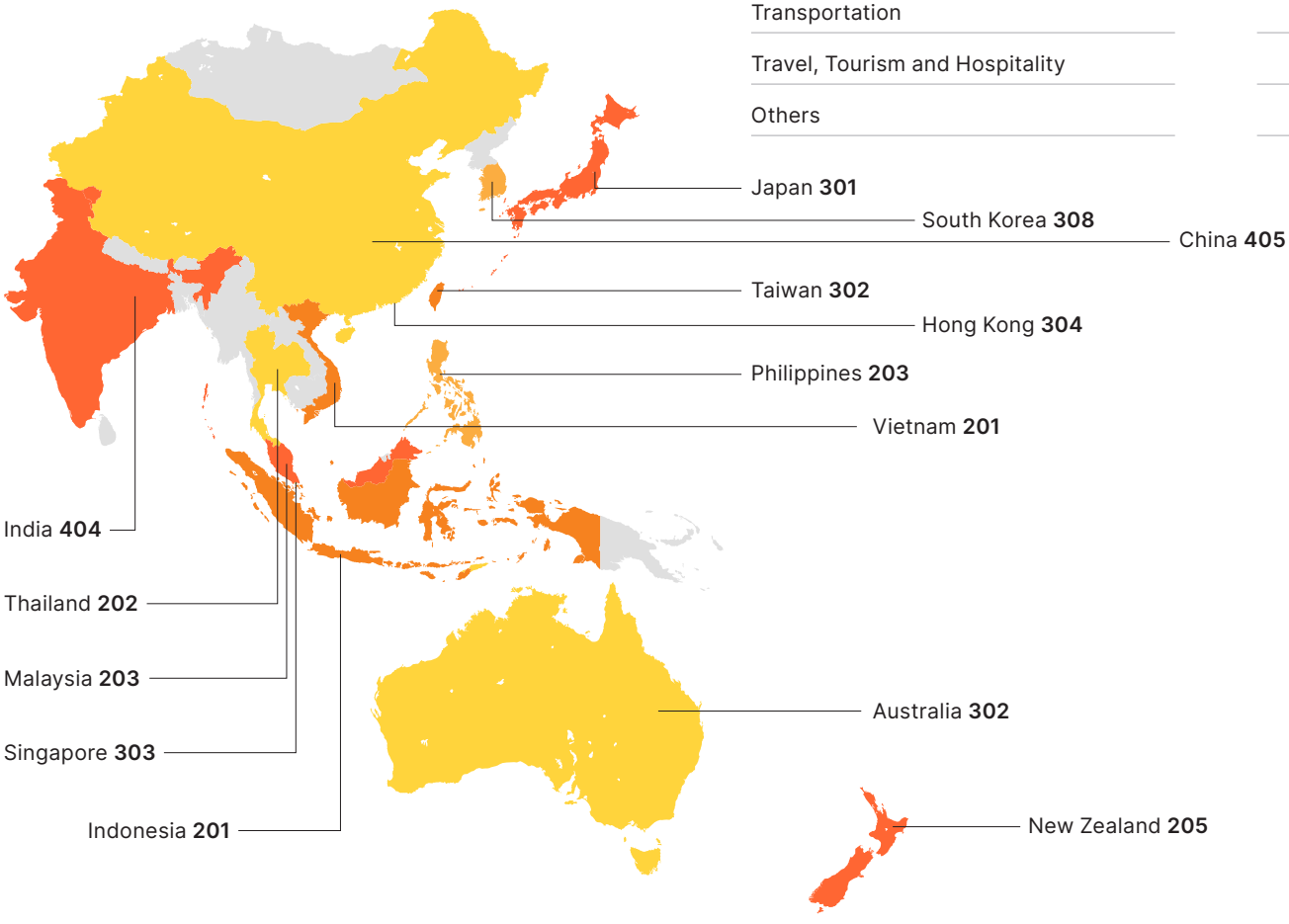
Methodology

The report is based on the findings of a double-blind survey conducted in June 2024 of 3,844 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.

This year's survey honed in on the cybersecurity challenges faced by Asia Pacific's enterprises, with a minimum respondent organization size of 250 employees and a weighting towards larger organizations. Respondents from smaller organizations (250-999 employees) represented 18% of the sample, with those from medium and large organizations making up 27% and 55% of our participants, respectively.

Distribution of respondents



The participants span a range of sectors

Industry	Number of respondents
Business and Professional Services	371
Construction and Real Estate	355
Education	204
Energy, Utilities and Natural Resources	347
Financial Services	349
Gaming	65
Government	263
Healthcare	254
IT and Technology	368
Law/Legal Services	4
Manufacturing	352
Media and Telecoms	163
Retail	342
Transportation	151
Travel, Tourism and Hospitality	236
Others	9

Organizations overwhelmed by data breaches

It's been 12 months since our last report and cybersecurity leaders in Asia Pacific continue to grapple with a complex threat landscape. While the number of respondents that experienced incidents in the past 12 months stands at 68%, this year's report delves deeper into how these incidents played out. Our study reveals that of those that experienced cybersecurity incidents, 61% suffered data breaches[1].

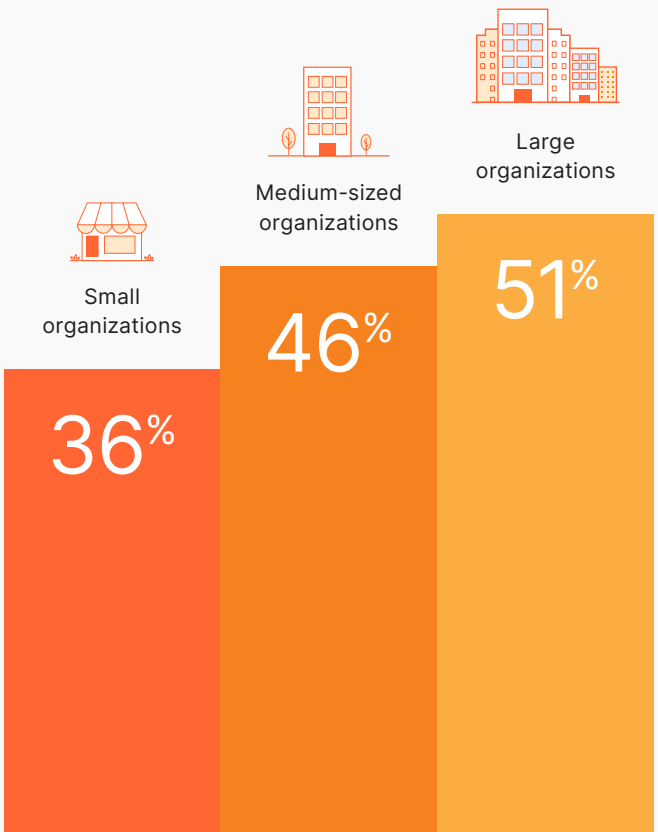
Many with exposed vulnerabilities are being struck repeatedly before they can plug holes in their defenses. 47% of respondents reported that their organization experienced more than 10 data breaches in the 12 months leading up to this study. Attackers appear to be eyeing larger organizations in particular. The organizations most likely to experience 10 or more data breaches in the past year are Construction and Real Estate, Travel Tourism and Hospitality, and Financial Services.

76% of those that experienced a data breach in the past year say the frequency of data breaches has increased. 58% believe they will see an even higher number over the next 12 months. In addition, 70% of all respondents either experienced a data breach over the past year, or believe they will fall victim to one in the year ahead. Respondents from Vietnam (86%), India (82%), Malaysia (80%), and Singapore (80%) were most likely to report

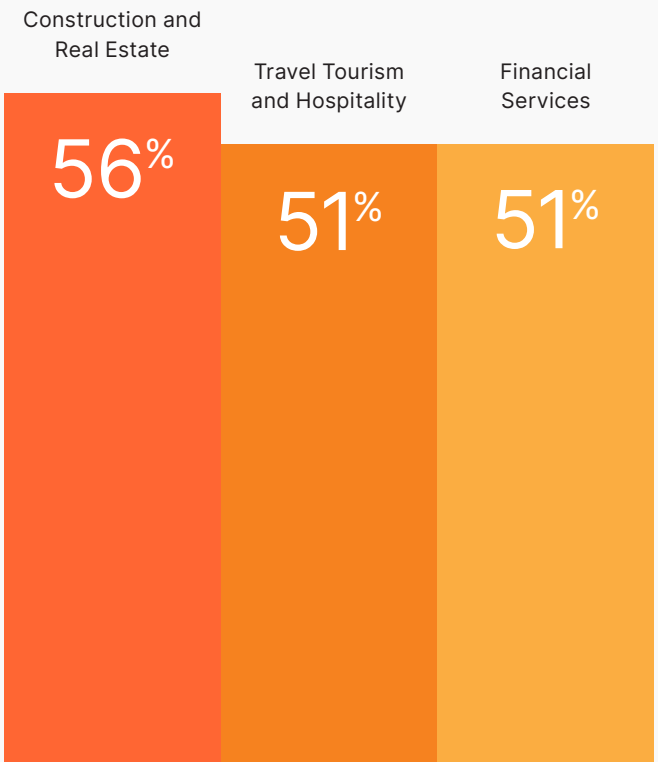
1. A data breach is an incident in which attackers gain unauthorised access to an organisation's applications, data and networks, whereas incidents are actions that can potentially compromise system integrity.

% of respondents reporting cybersecurity incidents in the past 12 months

By organization size



Most frequently targeted industries



an increase in data breaches over the last 12 months. 51% of respondents report combined losses of more than USD 1 million due to data breaches, with 27% of respondents reporting losses of more than USD 2 million. Financial loss is by no means the only impact to affected organizations. For organizations that have experienced data loss, customer data is most frequently targeted, with 67% of respondents indicating the theft of such data. Likewise user access credentials (58%) and financial data (55%) are also commonly stolen.

For those who have suffered data breaches, the financial losses incurred also include additional expenses that are not covered by cybersecurity insurance policies and the year-on-year financial burden of rising insurance premiums. Medium-sized organizations, which may not have robust insurance policies in place, but are also targeted by sophisticated attacks, often bear the brunt of additional expenses.

Web attacks, malware (viruses, worms, Trojans etc.), and phishing continue to top the list as the most common attack vectors leading to data breaches over the past year.

Annual premium increase (USD)

Small organizations	Medium-sized organizations	Large organizations
80,381	566,107	437,865

Additional expenses in most recent data breach (USD)

Small organizations	Medium-sized organizations	Large organizations
103,361	705,610	152,674

Top five most commonly experienced cyberattack vectors

Web Attacks 57%

Malware 49%

Phishing 44%

Supply Chain Attack 35%

Business Email Compromise 33%

Nearly all (92%) of organizations faced further business impact beyond the immediate data breach as a result of data loss, with the top issues being regulatory action (26%), further attacks using the data (17%), and reputational damage (16%).

According to the Cloudflare Q2 DDoS Threat Report, Distributed Denial of Service (DDoS) attacks have increased 20% year-on-year to hit 4 million, with 55% of them being Layer 3/4 DDoS attacks. Our data reflects this current landscape with 67% of respondents indicating their organization had experienced DDoS attacks. The majority of those attacks were either Layer 4 (47%) or Layer 3 (41%), while API or Layer 7 attacks accounted for only 26% and 18% of incidences, respectively. The key impacts of DDoS attacks are financial loss (55%) and service disruption (54%).

Another factor likely to be worrying many IT leaders is response times. 76% of respondents said their organizations took, on average, more than 12 hours to identify a data breach while 74% took more than half a day to contain the incident.

Unsurprisingly as a result, only 27% of respondents currently believe their organizations are highly prepared to prevent data breaches.

AI is changing the threat landscape

Artificial Intelligence (AI) has dominated discussions across various industries in recent years. However, in the context of cybersecurity, our respondents express a predominantly negative view, with 87% indicating AI has either contributed to more frequent attacks or empowered attackers to become more sophisticated.

Despite widespread concern about the impact of AI on cybersecurity, confidence around keeping pace with the threat is high, with 83% of respondents saying their cybersecurity teams can stay ahead of threat actors leveraging AI to power cyberattacks in the future. However, should an organization be targeted by an AI-powered data breach, only 28% of respondents feel their organization is highly prepared, highlighting a gap between confidence and actual readiness — until critical capability upgrades are made.

Respondents in Engineering and Automotive (45%) and IT and Technology (42%) feel best prepared to prevent these types of data breaches. This contrasts with those in Law & Legal Services (25%) and Education (21%) where lower levels of confidence prevailed.

Looking ahead, our respondents believe the threat from AI will grow, as threat actors work out how to use the technology more effectively. Specifically, 50% of our respondents anticipate that AI will be employed to crack passwords or encryption codes. Additionally, 47% believe it will enhance phishing attacks and social engineering techniques, while 44% expect AI to advance DDoS attacks. Lastly, 40% believe AI will play a role in creating deepfakes and facilitating privacy breaches.

As a consequence of these new and diverse threats, 70% of respondents said their organizations are changing their ways of working. The areas seen as most likely to be affected by changes due to AI are governance and regulatory compliance (40%), strategic direction of cybersecurity teams (39%), and vendor engagement (36%).

Cybersecurity leaders are also equipping themselves to combat threats posed by AI. Every respondent expects to deploy at least one new AI-related security tool, technology or measure in the future. The hiring of generative AI analysts (45%), further investment in threat detection and response systems, and security information and event management (SIEM) systems (both at 40%) are ranked as top future measures. IT vendors will continue to play an important role, as 66% of respondents have already sought AI-related solutions from them.

Approaches to ransomware attacks evolving as paying ransom proves ineffective

Ransomware and consequent ransom demands are on the rise globally, and the Asia Pacific region is no different.

Our survey shows that 22% of all respondents who experienced a data breach were targeted by ransomware attacks. Of those that were impacted, 62% eventually paid ransoms. This widespread payment of ransoms starkly contrasts with the fact that 70% of impacted organizations have made pledges against doing so.

There are significant variations across the region, though, with organizations in India (69%), Hong Kong (67%), Malaysia (50%), and Indonesia (50%) most likely to pay, while those in South Korea (19%), Japan (19%), and New Zealand (22%) least likely to give in to ransom demands.

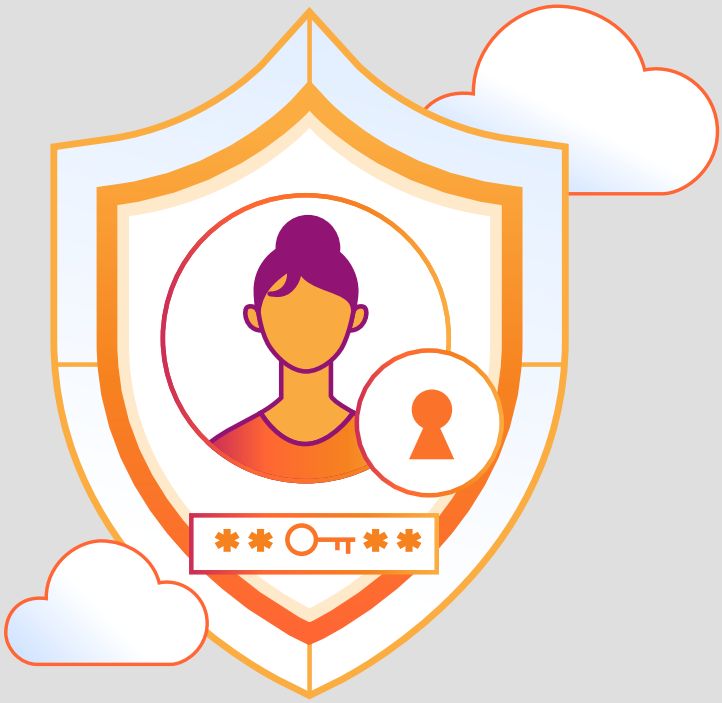
There are a variety of factors at play in agreeing to the extortion, but most common are concerns over the legal repercussions of data loss (39%), the benefits of restoring the data easily (25%), the fear of prolonged downtime (22%), and ethical repercussions (13%).

Almost every organization which ended up paying regretted it, with 96% of respondents who paid finding there were one or more consequences to their decision:

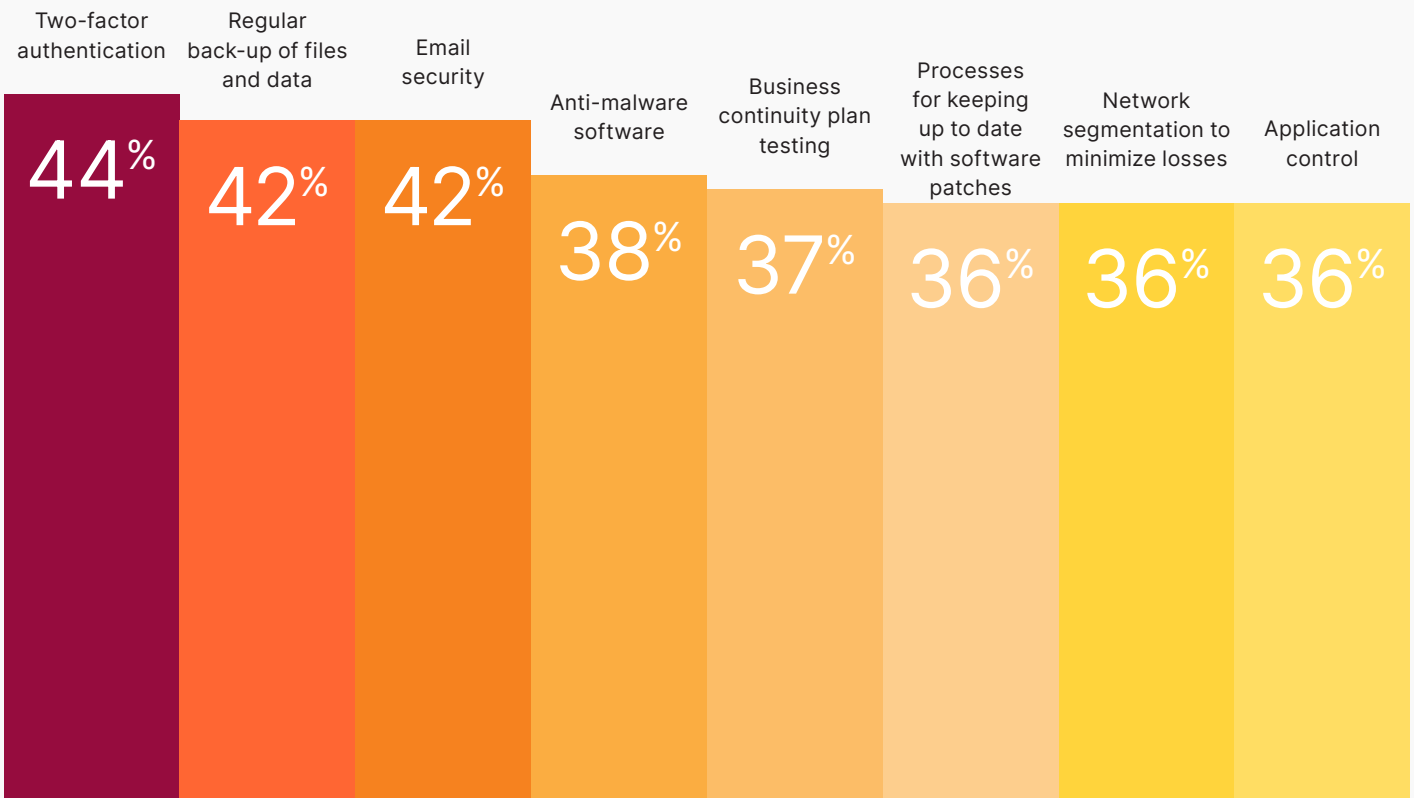
- Ransom attacks from new sources increased after the payment was publicized (63%)
- Attackers did not delete stolen data and sold/disclosed it at a later date (56%)
- Attackers did not honor the agreement to restore systems and return data (53%)
- Only some of the stolen data was restored (50%)
- The same attackers returned with further ransom demands (46%)

According to our respondents, the most common entry point for these attacks was a compromised Remote Desktop Protocol or VPN servers. These account for 47% of all cases, but is an outsized risk for medium-sized companies where it accounted for 61% of ransomware attacks. The second most common entry point was unpatched vulnerabilities in web applications or servers (39%).

These weaknesses underpin our respondents' focus on the measures they can implement to prevent ransomware attacks. Common tenets of Zero Trust architecture, such as network segmentation and regular data backups, can limit the leverage of ransomware perpetrators, yet our data show significant room for improvement in these areas.



% of respondents with "very mature" (76-100%) deployment of anti-ransomware measures

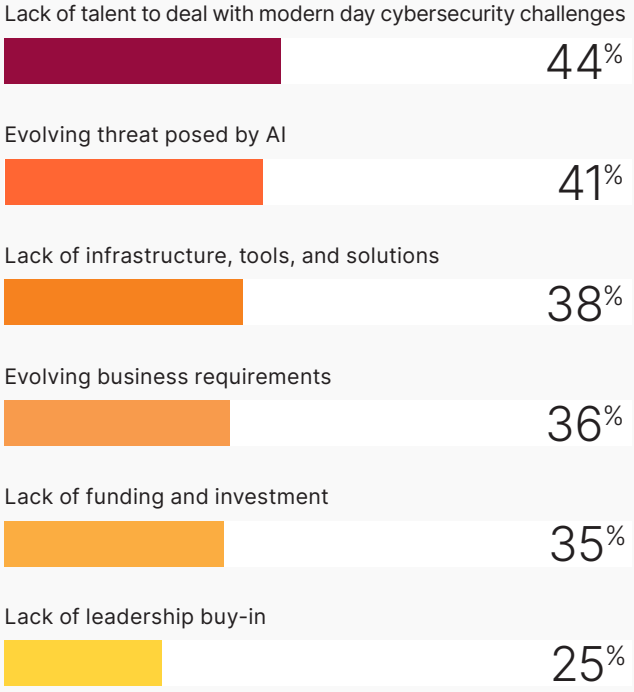


More is being asked of cybersecurity teams with less investment available

With only 21% of respondents believing their organization's cybersecurity posture is very mature, several key factors are holding organizations back.

A lack of talent remains the most pressing challenge (44%), while only 33% of organizations are investing in leadership team cybersecurity training. The majority (83%) of our respondents face at least two of the following challenges with cybersecurity preparedness.

% of respondents that indicated at least 2 of the following challenges amongst their top 3 cybersecurity challenges:



The expanding threat of data breaches is on the agenda of many senior leadership teams, with 80% of our respondents indicating they are expected to report on data breaches to their boards at least monthly, while 22% are required to do so weekly.

In terms of budget allocation, 84% of respondents said their organizations spent more than 10% of their total IT budget on cybersecurity in the past 12 months, while 30% spent more than 20%. Despite the challenging market conditions across Asia Pacific, budgets are expected to remain relatively stable over the coming year.

This will be critical as cybersecurity leaders wrestle with the ongoing talent crunch. Many recognize that finding new staff is a challenge and are therefore investing in upskilling their team members (48%). A similar number (45%) is investing in the restructuring of teams and processes, with 36% outsourcing cybersecurity functions to managed service providers (MSPs). While new hires are not ruled out entirely, only 31% are investing in additional staff, despite recognizing the talent shortage in addressing cybersecurity threats.

More solutions do not make organizations safer

There are certain holdovers which persist from the rapid digitalization and digital transformation efforts brought on by the pandemic. Notably, many products and solutions were hastily implemented as teams grappled with the complexities of managing a large, remote workforce.

Overall, 86% of our respondents who report complexity arising from a multitude of solutions and IT vendors say this has made their organizations more vulnerable to attacks. Beyond the difficulty of defending against attacks, complexity in cybersecurity architectures leads to over-stretched talent and delays in addressing successful attacks.

Challenges arising from managing multiple IT vendors

	Experienced more than 30 data breaches in past 12 months (among those with data breaches)
Organizations with less than 10 IT vendors	4%
Organizations with 11-20 IT vendors	6%
Organizations with 21-30 IT vendors	24%
Organizations with more than 30 IT vendors	45%

Challenges arising from managing multiple IT vendors

Talent challenges (existing manpower too stretched, insufficient manpower, excessive manpower)	52%
Challenges with integration with other solutions/software in place	49%
Too much time spent on repetitive tasks/ non-critical cybersecurity functions	49%
Too many solutions to navigate to remedy a cyberattack	48%
Cyberattacks take longer to be remedied	47%
Overlapping capabilities mean some solutions are redundant	46%
Too many rigorous protocols and processes to adhere to	44%

Almost all respondents (92%) experienced at least two of these issues, with 67% of respondents indicating their organizations purchased solutions from more than 10 IT vendors, while 40% of organizations are serviced by more than 20 IT vendors. Despite this, the increase in the array of vendors continues unabated, with 82% respondents saying the number of IT vendors they work with has grown in the last two years.

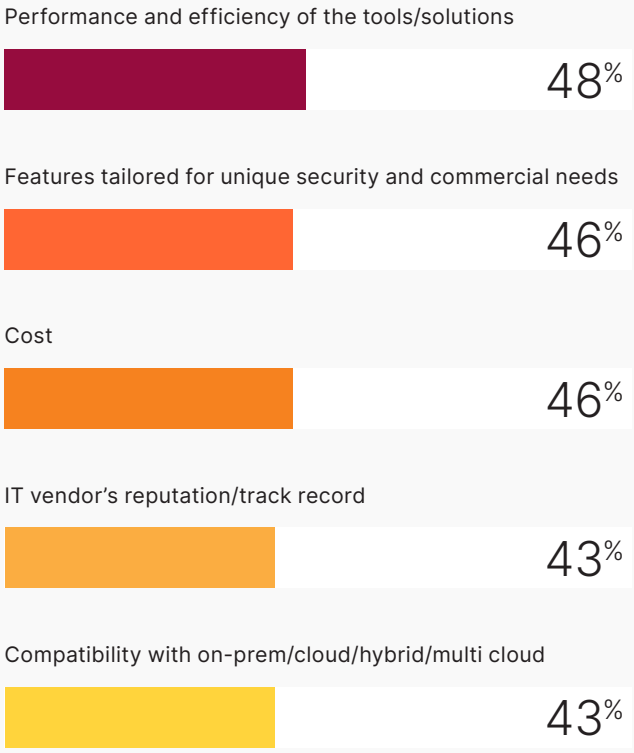
Purchasing solutions from a myriad of IT vendors does not make organizations safer. Organizations with fewer IT vendors are less likely to be attacked. Only 4% of organizations with less than 10 IT vendors experienced more than 30 data breaches in the past year, compared to 45% of those with more than 30 IT vendors.

The increased complexity of keeping an organization safe is not the only problem caused by the ever-expanding number of IT vendors; costs are spiraling too. Our survey reveals a direct link between the number of IT vendors and budget allocation. 22% of organizations with 30 or more IT vendors allocate over 30% of their IT budget to cybersecurity, compared to only 5% among those with fewer than 10 IT vendors spending this portion.

Looking more broadly at the financial implications of the growing number of IT vendors, our respondents report that, on average, spending on tools and solutions increased by an average of 18%. Those who had reduced IT vendor numbers only saw costs rising by 6%.

With so many solutions to choose from, cybersecurity decision makers have had to put in place a variety of evaluation criteria to ensure they are making choices based on more than just cost. Our respondents told us, perhaps unsurprisingly, that performance and efficiency were most important with tailor-made solutions and cost in a close joint second.

Factors in selecting new solutions



Calculations requested of IT vendors demonstrating ROI

Reduced time to respond to data breaches due to centralized threat detection and response	64%
Cost savings arising from time saved to manage fewer solutions	64%
Cost savings arising from replacement of multiple subscriptions to other solutions	52%
Reduced risk of security gaps caused by siloed solutions and human error	50%
Automation and streamlining cybersecurity protocols	31%

There are clear advantages for organizations in consolidating the number of solutions or IT vendors in their stack, not least of which is better security outcomes. As businesses increasingly recognize this reality, they are putting pressure on IT vendors chosen to implement consolidation drives. From man-hours saved to incident response times, the table on the left illustrates the top five requests made of IT vendors.

There is also a shift in the way organizations assess the effectiveness of the tools they choose to deploy, with a focus on performance rather than the impact of data breaches.

Top factors when selecting new cybersecurity tools and solutions

56% Time taken to respond to cyberattack	55% Time taken to detect cyberattack	55% How effectively they detect advanced threats
46% Volume of data lost	44% Financial loss incurred	43% Time between upgrades

Zero Trust solutions play a critical role in cybersecurity

In the midst of an intensifying threat landscape, Zero Trust has gained significant traction.

Approximately 88% of respondents have invested in, or plan to invest in, Zero Trust solutions. Among those who have deployed these solutions, 33% are fully deployed, while 42% are partially deployed, primarily emphasizing data encryption and multi-factor authentication (MFA). Additionally, 80% of respondents report at least partial deployment of secure web gateways and firewall-as-a-service. Several key reasons are driving the shift to a Zero Trust architecture:

- It reduces the impact of user credential theft and phishing by requiring multiple authentication factors;
- By segmenting user access, Zero Trust ensures that users can only access specific resources without exposing the entire network. This approach is critical for limiting the severity of ransomware attacks;
- The Zero Trust framework reduces the risk posed by vulnerable IoT devices, which are often difficult to secure and update; and
- It delivers continuous monitoring and validation of connected users and devices.

When those that have made the shift to Zero Trust were asked about resulting efficiency gains for organizational processes, 84% of respondents said that bottlenecks for remote workers were eased through VPN replacement or augmentation. Conversely, onboarding new employees saw the least efficiency gains.

Moving to a Zero Trust framework is not a straightforward process though. 83% of respondents told us that migrating to a Zero Trust architecture using a SASE model is a ‘complex’ (65%) or a ‘highly complex’ challenge (18%). The change must also be managed from a people standpoint, with 23% of end users not supportive of the move. Cybersecurity teams, with their specialist expertise, are almost universally (89%) supportive.

88% of respondents name mapping out transaction flows of all jobs that require access to sensitive data stores,necessary systems, and applications as the most challenging task in preparing for the shift to Zero Trust.

Increased regulation is a core concern

There are mounting regulatory requirements for cybersecurity teams that are taking considerable time and resources to manage. Our survey shows that 43% of respondents spend more than 5% of their organization's IT budget on compliance and certification issues.

48% spend 10% or more of their work week - half a day - staying abreast of changing regulatory and certification requirements. The challenge is most evident in the Gaming industry where 62% of organizations spend increased time on regulatory compliance.

Almost all (99%) have seen more time commitment required for regulatory compliance over the past two years – with 47% reporting that the weekly time spent on this area has grown by 20% or more.

Local cybersecurity regulations are most likely to have contributed to the increased complexity of organizations' cybersecurity architecture in the past two years. This accounts for increased time spent (64%), while international data privacy regulations (57%), local data privacy regulations (55%), and international cybersecurity regulations (49%) account for time spent on other forms of regulation.

Respondents in Hong Kong (75%), Taiwan (70%), and Indonesia (70%) are most likely to report increased complexity arising from local cybersecurity regulations, while the industries most affected are Transportation (73%) as well as Energy, Utilities and Natural Resources (72%), potentially due to the high public sector exposure of those industries.

The consequences of adhering to greater regulatory and compliance changes in the past two years are real. Every single one of our respondents had experienced at least one of the following issues with 77% experiencing at least two:

- Affected organization's ability to deliver technology and data to customers: 46%
- Affected the cybersecurity teams' ability to meet business goals: 46%
- Affected the cybersecurity teams' ability to deliver to the CIO and CISO: 44%
- Affected the overall functioning of the business: 40%
- Has forced the organization to deploy physical IT equipment in each market: 39%
- Prohibits the use of non-certified IT vendors: 37%

Amidst the negative impact of heightened regulatory requirements, respondents also highlight positive effects. All of our respondents reported they had seen at least one of the following, and 79% had seen at least two:

- Improving organization's baseline privacy and/or security levels: 59%
- Improving the integrity of the organization's technology and data: 57%
- Improving organization's reputation and brand: 53%
- Increasing private sector sales opportunities: 42%
- Increasing public sector sales opportunities: 39%

There are questions about whether more stringent certifications are yielding a positive return on the time spent adhering to them. Only a minority of respondents believe any of the common certifications have had a positive impact on their organization's security, brand or business opportunities, with the United States Federal Risk and Authorization Management Program (FedRAMP) the most positively received at 42%.

It is not a universal picture, however, and some markets welcome the greater levels of scrutiny. Respondents in Vietnam (62%), the Philippines (58%), and Thailand (57%) welcome FedRAMP and believe it has a positive impact.

Among organizations which handle customer credit card data, 66% are fully compliant with the new Payment Card Industry Data Security Standard 4.0 (PCI DDS 4.0) framework and a further third (31%) are partially compliant. Respondent organizations appear to be significantly more developed in encryption and protection of data (at 71%) compared to other areas of the framework.

Recommendations

Cybersecurity teams are navigating an increasingly sophisticated threat landscape with the potential of AI-powered attacks. At the same time, leaders are balancing budget constraints, navigating regulatory requirements, and continuing to compete for top security talent. The challenges of this dynamic environment are exacerbated by the complexity of legacy solutions across multiple vendors.

What recommendations can we make to support CISO success?

1. **Streamlining solutions to reduce complexity:** In last year's report, we suggested streamlining security architecture through SASE. This year, not only does that suggestion remain, but the evidence is clear: more solutions and IT vendors does not correlate with risk reduction. Organizations should be considering a more measured approach to minimize the number of solutions deployed and consolidate the number of IT vendors they obtain their solutions from.

2. **Strengthen the weakest link in the chain:** In today's global and interconnected environment, every organisation relies on the software supply chain. Applications are built on open-source code, APIs, and third-party integrations are all part of the increasing attack surface. This expansion of our attack surface is why onboarding a new partner means choosing to trust its entire development ecosystem, rather than just the tool itself. Moving from a perimeter-based security model to a Zero Trust model that trusts no one, assumes that attackers are within the network already, assesses users, devices and workloads based on identity and context can reduce risk associated with a breach in your supply chain. Look for partners who are committed to secure by design principles.

3. **Limit the leverage for ransomware attackers and make plans for demands:** Ransomware attacks are on the increase and CISOs and their Boards need to have a plan in place. Looking at the evidence of this study, that plan should not include paying the ransom because in almost every case, organizations that have done so have regretted their course of action. We recommend a strategy of minimizing lateral movement should a breach occur, leveraging Zero Trust capabilities. In addition, a robust resiliency program will reduce the leverage of an attacker's demands. Assurance begins with regular data backups, tested to ensure efficacy and completeness, of your most critical systems and data. Regular disaster recovery testing is critical to identify gaps and build the muscle to restore operations and reduce impact.

4. **Prepare for AI fuelling a multiplication and intensification of attacks:** AI will be used by attackers and CISOs need to have AI defensive strategies in place. Cybersecurity leaders should be wary of simply outsourcing the problem but there is definitely a case for examining talent models, governance frameworks, compliance requirements and monitoring usage. A key action all can take now is to review the terms of engagement with third party vendors to ensure their use of your data, in their AI models, is understood and aligns with your requirements. How do your current security tools combat an increase in AI attacks? Many Cloudflare products leverage our massive global network of threat intel to combat new threats proactively.

5. **Shift investment from capital to operating expenditure:** Budgets for most are under pressure and cybersecurity leaders need to be good fiscal stewards. Look at upskilling existing team members to align with your future state, reduce complexity and streamline processes. Explore opportunities to reorganize roles to maximize effectiveness while also reducing lag time. It is worth looking at outsourcing some of the functions to MSPs, shifting investment from a capital expense to an operating expense.

6. **Get used to more scrutiny:** Cybersecurity leaders are facing increasing scrutiny internally and externally, adding to their already-significant pressures. This scrutiny will continue and CISOs need to be diligent in seeking opportunities to comply with changing regulations (local or international) as well as being able to meet the needs of board members. Ensure your audit commitments are negotiated to clear scope and timelines to reduce tasks that don't add value to your customers nor reduce risk.

Move to a connectivity cloud

Cloudflare plays a crucial role in providing security everywhere by offering a new category of service, called the connectivity cloud, that connects and protects a company's people, apps, and networks. Through Cloudflare's broad portfolio of security offerings, such as application, API and network security, Zero Trust, and global threat intelligence, organizations can fortify their digital infrastructure against cyberattacks. An organisation can ensure the security of their online data and intellectual property, and protect the integrity of their brand.

These security services are built on Cloudflare's unified platform of programmable global cloud network services, which connects and protects a massive percentage of the world's Internet traffic and stops an average of 182 billion threats per day. This global cloud network minimises the risk of downtime and ensures high availability by providing redundancy and resilience against network outages and infrastructure failures.

To learn more about Cloudflare's platform of solutions and request a demo or POC from a sales representative, please visit:

cloudflare.com

We will evaluate your existing security posture and create an action plan to strengthen cybersecurity for your people, applications, devices, networks, and data.

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com