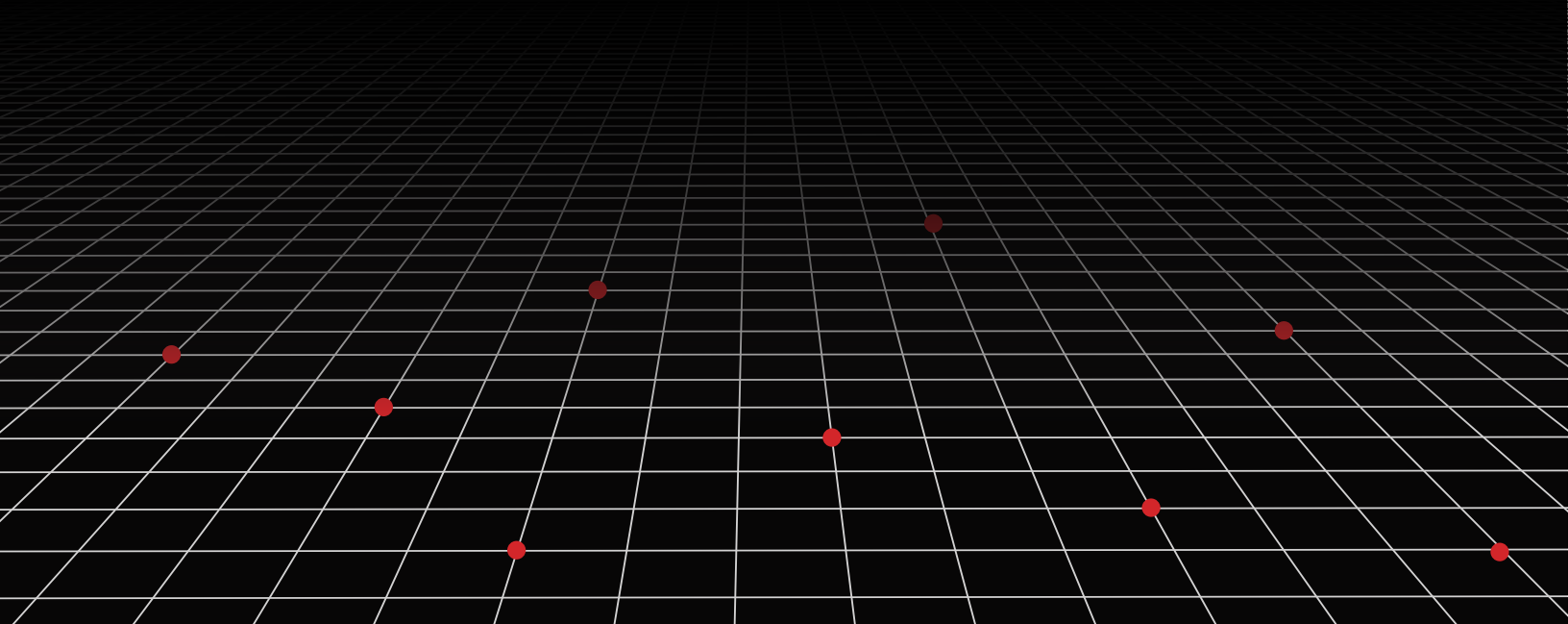
fastly

Fastly Security Research Report

Cybersecurity at the Crossroads

How Australia and New Zealand can strengthen cybersecurity in an era of escalating threats and digital disruption



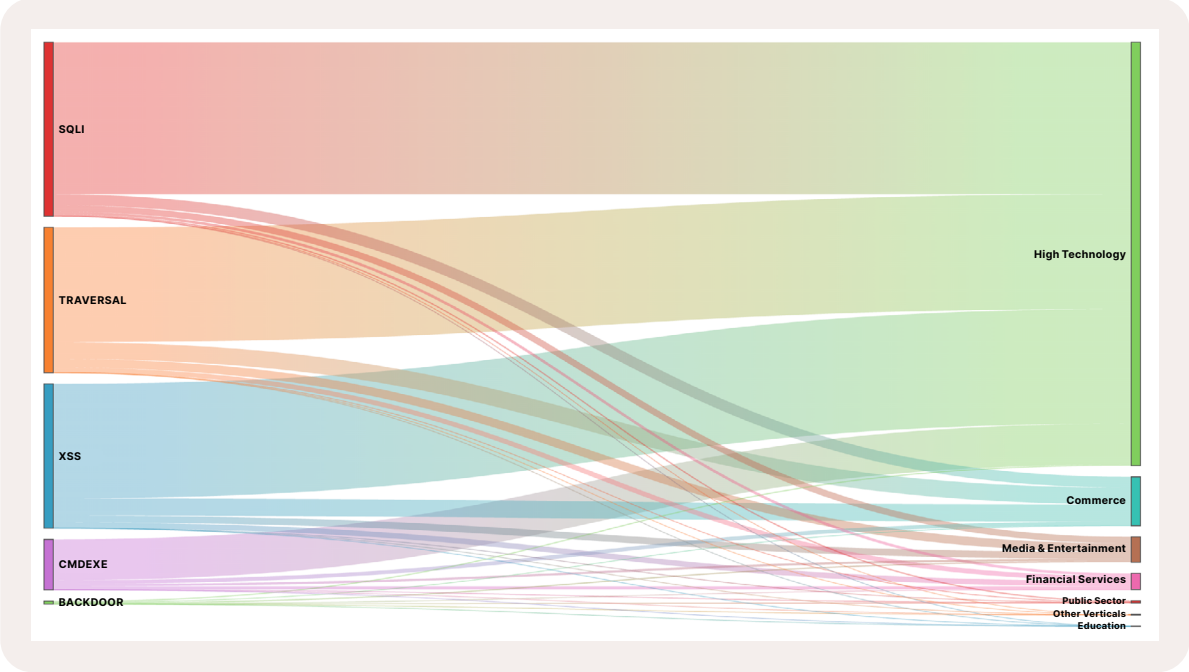
Executive Summary

Over the past year, cybersecurity risks escalated significantly. A global outage caused by a misconfigured update disrupted millions of Windows systems, underscoring the fragility of even well-established security tools.

While international cybersecurity incidents often dominate global headlines, Australia and New Zealand face their own significant challenges, highlighting the urgency of regional resilience. The high-profile breaches at Optus and Medibank served as stark reminders that local organizations are not immune to sophisticated attacks, nor to the reputational and operational fallout that follows.

These events underscored vulnerabilities in critical infrastructure and consumer data protection, prompting increased regulatory scrutiny and elevating cybersecurity to a board-level priority across both public and private sectors. As threat actors become more targeted and persistent, regional leaders must adopt a proactive, well-resourced security posture that reflects the scale and complexity of the risks at hand.

Against this backdrop, the need for more cybersecurity and digital resilience is greater than ever - yet a closer look at the last 12 months finds security programs in a precarious position. The headwinds facing cybersecurity initiatives are more significant now than they were previously. Many of these are non-technical, covering issues such as budget scrutiny and confusion over who is responsible for cybersecurity in organizations.



The largest attacks observed in Australia and New Zealand by Fastly, and the industries they targeted the most in the past 365 days (May 2024 - May 2025)

As mentioned in our earlier global security report, online security is at a crossroads. To gain more insight into how corporations are dealing with key cybersecurity issues and where the industry is headed, in late 2024, Fastly worked with business and consumer market research agency Sapio to survey 1800 worldwide IT decision makers, all with an influence in cybersecurity. This report, focused specifically on Australia and New Zealand, offers deep insights into the regions cybersecurity challenges and how they plan to overcome them. Here are some of the key findings:

- **Security initiatives are on a knife-edge.** While more IT decision makers (87%) expect cybersecurity investment to increase over the next year, the results from this spending will be under intense scrutiny. Security teams face an uphill struggle as they try to convince senior executives to continue budgeting in ways that make effective defense strategies possible. The C-suite has plenty of other priorities to address, especially in areas such as digital transformation and IT modernization, and they feel that cybersecurity initiatives slow them down.
- **Organizations face challenges scaling their cybersecurity operations.** As they struggle to justify their function to the board, there are also worrying signs of inefficiencies in cybersecurity. Over a third of respondents felt that they had no clear idea of where they should allocate cybersecurity resources, which correlates with a feeling of over-investment.
- **The market is not providing the talent that companies need.** There are also signs of an inability to scale cybersecurity efforts as capacity and complexity demands increase. Traditionally, companies have invested in more talent to try to keep up with burgeoning cybersecurity needs, but this year sees a deep dissatisfaction with the available talent pool. That calls for a rethinking of skills management practices to cope with evolving cybersecurity needs.
- **Technology complexity is holding back cybersecurity efforts.** The technology organizations use to fight cyber threats are also an issue as companies look to scale their cybersecurity initiatives. Businesses are also still laboring under complex, overlapping toolsets that make cybersecurity operations such as incident response more difficult. 2024's CrowdStrike outage has thrown security products and services into the spotlight, as security leaders begin to question the risks and benefits of their cybersecurity tooling.

Is cybersecurity spending falling behind?

Nothing happens without appropriate investment, and the same is true of cybersecurity. As attackers proliferate and become more sophisticated, defenders must commit funds to protecting their assets. While intentions are good, reality highlights some glaring problems.

Back in 2023, three-quarters of those surveyed planned to invest more in cybersecurity. A year on, half of all companies feel that they have underinvested in key areas of cybersecurity and worry that this has left them vulnerable to attack. Looking globally, at 61%, this fear is strongest among companies in the U.S, which is natural as they experienced the highest number of attacks.

Companies generally feel that they're investing in the right cybersecurity areas, with 71% reporting alignment between their investments and their cybersecurity strategy. So why do so many companies still feel underinvested in security?

Investments are hard to justify

The disconnect extends beyond a simple lack of cybersecurity awareness, which would be simpler to solve. Instead, cybersecurity is seen as an obstacle to other priorities, with 45% of respondents' senior executives worrying that it slows down innovation. IT modernization is a significant component in digital transformation efforts, and 43% of people feel that cybersecurity investments hinder this initiative.

Cybersecurity professionals must justify their costs to a C-suite facing these priorities, but 44% fail to do so. While 72% of respondents feel their investments have supported revenue and growth goals, confidence that they have quantified the ROI from cybersecurity spending is moderate, at 62%. Part of the problem is understanding where to spend those resources; 36% said they had invested far too much, with no clear plans on where to allocate resources.

Those making cuts are likely the last ones that should

On the upside, at 88%, more organizations than last year plan to increase their investment in cybersecurity. However, given that 76% of companies planned to invest more in cybersecurity in 2023, and that half still feel under-invested this year, intentions might not reflect reality.

Maybe not surprisingly, only 4% plan to reduce their cybersecurity investment, which might not mean reducing functionality. As competition increases, those looking to make cuts are likely moving to cheaper solutions, consolidating contracts for cost efficiencies, or even looking at open-source options. There's nothing wrong with making each dollar do more, but this cost-cutting group's relatively poor performance raises concerns. They suffered 68 security incidents on average over the past year, which is 70% more than the overall average of 40.

Risk analysis: a key component of investments

Companies can achieve a lot by investing in the preventive and response efforts that have the right impact. This takes a mature approach, both to risk analysis, understanding the most impactful cyber risk for a specific company, and concentrating investment in those mitigations.

Risk is a language the C-suite understands. Cybersecurity professionals can speak this language by surfacing top-level risk mitigation metrics that prove to busy decision makers how cybersecurity makes innovation and business transformation safer. They can also work with production teams to introduce security measures earlier in the development cycle using automation, where possible, to make these measures more effective and less disruptive.

Recovery time

There's no denying that 2025 is off to a turbulent start as far as the international political climate goes, and the tone in the raging debates is often uncompromising, and lines get drawn fast. That alone might be enough to keep CISOs up at night, proving that they work for a company that can find itself in the crosshairs of public opinion. It's a short distance from "all is well" to "we're under attack".

There is nothing that points towards the amount of online attacks getting smaller. It doesn't really matter whether you look at it in terms of the number of attacks, the damage they create, and the amount of time it takes to mitigate them, clean up, and try to prevent them from happening again. Online attacks remain an often-used strategy to hurt businesses where they feel it the most: reputation and revenue.

We asked participants from Australia and New Zealand how long to typically takes to fully recover from online attacks. On average, they estimated 7.01 months. This is approximately one week longer than the global estimate of 7.34 months. But we should also point out that 30% of the global respondents said they'll have cleaned up within an impressive 1-3 months. 17% saw attacks that took more than a year to recover from.

So why the large delta? One answer is undoubtedly that recovery times rise as cybersecurity investment falls. We saw a direct correlation between those companies that expect to spend less in the next 12 months and those expecting recovery time exceeding eight months. The gap between perception and reality continues to grow - companies planning to reduce cybersecurity investments take nearly 11 months to recover from incidents, about a third longer than they anticipate. In contrast, organizations that maintain or increase their cybersecurity spending recover significantly faster.

Preventive measures top the list of recovery tactics

For Australia and New Zealand, the two most common responses around preventive measures are implementing stronger security (51%) and revising security policies and procedures (43%) - reflecting a focus on "lessons learned" and prevention of future attacks. Both are higher than the worldwide results - 43% and 41% respectively. While there is nothing unusual in the response with the highest priority, some may find that it's surprising to see revision of security policies this high. We believe there are two reasons for this: companies are still adjusting their security procedures to accommodate a flexible culture when it comes to where you work. Secondly, social engineering is increasingly being used as the hunting ground for inroads, and with work being conducted all over the place, training on how to be more vigilant is needed.

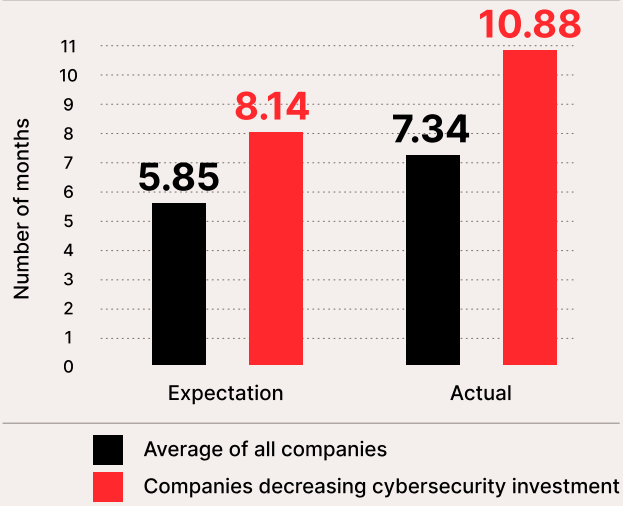
More companies in Australia and New Zealand are prioritizing specific actions that aid incident recovery, such as restoring from backups (40% - up from 38% worldwide) or communicating with stakeholders (29% - down from 34% worldwide). Forensic analysis - critical for pursuing legal action against malicious insiders or external attackers and for regulatory reporting - is the least commonly cited, at just 23%, just shy of the 25% worldwide. On a positive note, 36% of respondents from Australia and New Zealand are allocating additional budget toward incident response playbooks and supporting tools, up from 32% worldwide.

When surveyed, most regional businesses rely on internal resources for recovery, with 66% turning to their IT teams. 41% engage external cybersecurity firms for support. Fewer than one in three respondents opted to use cyber insurance to offset costs, a number we expect to continue to decline, as the average cost of a data breach in 2024 reached an all-time high of $4.88 million.

Finally, Australia and New Zealand show less loyalty than the rest of the world when it comes to their EDR vendors. 26% of respondents said that in light of recent security events, they are considering changing vendors. Still, many keep using their existing tools and instead look for ways to better utilize or optimize them. At 53%, more than half of the respondents in these two countries answered that this was their preferred approach.

Figure 1

Recovery time after cybersecurity incidents



Confidence vs. Reality: Are Organizations Overestimating Their Infrastructure Security?

Security incidents have long been a part of everyday life for IT professionals, and almost every company has experienced them. For both Australia and New Zealand, as well as worldwide, only 14% of those polled did not have any security incidents. Worldwide, the response was 10%. In the past year, on average, the organizations we polled had 40 known incidents. American businesses were the ones most affected; they experienced one incident per week, and with 64 incidents over a 12-month period, larger organizations were even more exposed owing to their greater attack surface and possibly the reach of their brand.

It bears repeating that an incident isn't necessarily the same as an online attack. In fact, of those asked, 27% of the Australian and New Zealand businesses answered that they had incidents due to misconfigurations, with software bugs coming in at an astounding 42%! Yet, patches and IT changes often arrive too slowly, creating security gaps for 25% of the companies polled. Embracing Secure DevOps (SecDevOps) can help prevent bugs upfront and accelerate fixes for vulnerabilities that slip through.

An additional key issue is the tension between manual and automated processes. Manual steps contributed to 28% of incidents, with 14% of respondents reporting problems due to reliance on employees manually enforcing security policies, rather than embedding security into their technology solutions.

Cyber incidents wreak financial havoc

No matter who or what is the cause of a cyber incident, everyone polled ended up with significant revenue losses. 23% of those asked in Australia and New Zealand could see the effect on the bottom line. Worldwide, companies lost an average of 2.5% of revenue when there were financial losses. Although it's less measurable in terms of cost, downtime is another big consequence, closely followed by data loss.

It's important to remember that online security incidents pose significant legal and regulatory risks. 14% of the combined respondents in Australia and New Zealand reported compliance violations, while 16% indicated that customer accounts had been compromised, which could lead to breaches of privacy laws.

Reputational damage is also a major concern, affecting 27% of the combined organizations in Australia and New Zealand. Additionally, 21% experienced a decline in customer trust, and similarly, 21% noted a decrease in customer satisfaction. These issues have a direct impact on customer retention, with 14% of organizations reporting an increase in customer churn following an incident.

Confronting the Next Wave of Threats

Concern over cyber threats remains high. The rise of automated attackers is particularly troubling, with 43% of respondents saying it keeps them up at night. Many question whether their current security tech stack can keep pace: 32% cite a lack of automation in their defenses, while 21% are held back by sluggish change management processes. In fact, automating cybersecurity is the second-highest security priority over the next 12 months, identified by 27% of the respondents. The anxiety is casting a shadow over innovation. While digital transformation promises growth, 44% worry that expanding their software footprint and digital infrastructure will increase their exposure to attacks, especially since 33% are concerned they don't have the experience to secure modern and complex architectures. More broadly, 52% believe they are unprepared to face sophisticated threats, and 33% say their internal cybersecurity technologies aren't strong enough to protect them.

DDoS in Depth

They may be a quarter-century old, but distributed denial of service (DDoS) attacks are still a perennial threat. They are a worry for 23% of companies in the coming year.

Damage from downtime was a problem for 62% of companies suffering DDoS attacks in 2024, and over half (52%) report significant revenue loss, with 70% suffering a spike in operational costs.

Paradoxically, DDoS protection ranks just ninth as an investment priority, at 25%, yet 45% of those citing DDoS as a threat next year feel unprepared. There are plenty of mitigations to take. The most popular, at 71%, is to enlist cloud-based DDoS protection, while 56% call upon their ISPs for help. On-premises mitigation is a solution for 54%. Web application firewalls (WAFs) can work in the cloud or on-premises, accounting for the popularity of this measure, at 66%.

Is Cybersecurity Spend Keeping Pace with Rising Risk?

Effective cybersecurity doesn't happen without appropriate investment. As threats multiply and adversaries grow more sophisticated, organizations must continue to commit meaningful resources to the defense of their online storefronts and infrastructure. Yet despite strong intentions, the data we see reveals critical shortfalls.

In 2023, 75% of respondents indicated plans to increase cybersecurity spending. One year later, half reported underinvesting in key areas. In their own words, this is raising concerns about exposure to threats. This sentiment is particularly acute in the U.S., where 61% of organizations acknowledge gaps, correlating with the region's high incident volume.

Interestingly, worldwide, 71% say their current investments align with strategic objectives. For Australia and New Zealand, the number is an impressive 79%. So why do so many still feel underinvested in online security?

Investments Are Hard to Justify

Tight budgets aren't the only reason respondents have trouble securing funds earmarked for protecting against online threats. The answers given to us revealed that cybersecurity is often seen as an obstacle to working on other priorities. An astonishing 43% of respondents' senior executives worry that this very issue could slow down innovation. IT modernization is a significant component in digital transformation efforts, and 35% feel that investments in cybersecurity hinder that initiative.

Cybersecurity professionals must justify their costs to the C-suite, but 49% fail to do so. While 60% of the respondents feel their investments have supported revenue and growth goals, confidence that they have quantified the ROI from cybersecurity spending is better than most, at 42%. Part of the problem is understanding where to spend those dollars; worldwide, 36% said they had invested far too much, with no clear plans on where to allocate resources. The number for Australia and New Zealand was 31%.

Trimming Security Budgets Is a Shortcut to Exposure

On a positive note, an astonishing 82% of respondents plan to increase their cybersecurity investment this year. However, given that half of the companies this time around say they're still under-invested, intentions alone may not translate into reality.

It's also good to see that only 9% of organizations expect to reduce cybersecurity spending. While that number might seem high, this doesn't mean that those respondents will scale back their level of protection. Those companies may be shifting to lower-cost solutions, consolidating vendor contracts, or exploring open source alternatives.

Optimizing spend is sensible. But the data shows that this cost-cutting cohort may be paying the price: Those expecting to scale back budgets experienced an average of 68 security incidents in the past year - 70% more than the overall average of 40. That raises important questions about the hidden costs of cutting corners.

Risk Analysis: The Foundation of Smart Cyber Investment

Maximizing the impact of cybersecurity spending starts with a mature approach to risk analysis. By identifying the most significant threats to their specific environment, organizations can target investment toward preventative and response efforts that deliver meaningful protection.

Risk is a language the C-suite understands. Cybersecurity leaders can bridge the gap by highlighting high-level risk mitigation metrics that clearly demonstrate how security enables safe innovation and business transformation.

Collaboration with engineering and production teams is

also key. Embedding security earlier in the development lifecycle - particularly through automation - can make protections more effective, less disruptive, and easier to scale.

The Cybersecurity Skills Gap: A Growing Threat in itself

Professional skill shortages continue to be a major obstacle in cybersecurity, and Australia and New Zealand is no exception. More than one-third (37%) of organizations cite a lack of the necessary expertise to address modern security threats. Compounding the issue, 42% of those in the region acknowledge underinvestment in cybersecurity talent, both in terms of hiring and compensation. As a result, training and talent acquisition have become the top priority for 34% of organizations when looking at the coming twelve months.

The consequences of a cybersecurity talent shortage can be severe. Organizations not only become more vulnerable to cyberattacks, but also face longer response times and higher costs when incidents occur. These challenges place additional strain on existing teams and can hinder ongoing preventive efforts.

Guy Brown, Fastly's Staff Enterprise Security Architect, often hears similar feedback when meeting prospects and customers: "The cybersecurity talent gap is not a future concern - it's a present and pressing reality. Our customers are navigating this challenge every day. Organizations must make a choice: cultivate talent from within or compete in a highly saturated market for external expertise. The real question for leadership is -what is your strategy to attract, retain, and empower the security talent your business needs to stay resilient?"

A significant contributor to the gap may be a misalignment between where companies are searching for talent and where qualified professionals actually reside. A little less than half (43%) of the organizations polled report that the talent pool lacks the specific skills they require, but at the same time, 13% say they are not facing major issues in hiring for cybersecurity roles.

As many in the industry can attest, the development of security talent is not immediate. Turning recent graduates or entry-level hires into effective team members requires considerable time and effort. These individuals must not only acquire technical expertise with the organization's tools and systems but also develop a nuanced understanding of internal workflows and company culture.

These challenges are expected to become more pronounced as organizations grow. Operating in larger, more complex environments adds pressure, particularly for less experienced hires. 19% of respondents identified "inexperience with large-scale technology infrastructures" as a significant barrier to success within security teams.

Addressing these issues requires a deliberate and sustained focus on nurturing talent pipelines, investing in upskilling programs, and aligning recruitment strategies with actual organizational needs.

Alternatives to External Recruitment

Companies should direct their skill development efforts toward internal improvement, given the existing challenges. There are several options:

Upskilling. The existing workforce can learn new responsibilities because they already understand your company culture and have a basic understanding of your operational systems and processes.

Mentoring. Junior employees learn valuable skills through on-the-job training provided by experienced staff members, which helps them develop into successful professionals.

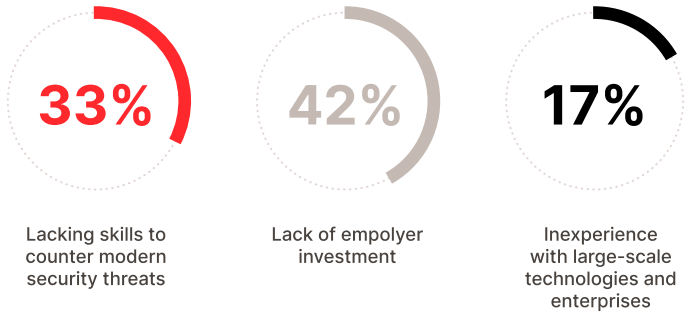
Cross-functional collaboration. Security teams that communicate better with IT, compliance, support, and product development teams will develop employees who understand security's role within different organizational functions. The organization should consider implementing secondments within this framework. The ultimate goal

should be to expand both skillset and responsibilities into non-security teams. The integration of security knowledge between product development teams enables them to implement secure-by-design principles during their development process.

Internal recruitment of staff who work across different functions provides multiple benefits. Such a practice demonstrates that every employee must contribute to security responsibilities. The initiative helps organizations advance their digital transformation goals. An integrated security culture supports the digital transformation process while addressing the security concerns of 43% of companies who believe their vulnerability to attack will rise during this period.

Figure 2

Shortcomings in the current talent pool



Mapping the shift in accountability

When a cyber incident happens, who gets held responsible? Regulators now direct their accountability judgments to the chief information security officer (CISO). In October 2023, the USA-based SEC prosecuted not just SolarWinds but also its CISO, Timothy G. Brown, with fraud and internal control failures. Although most charges were later dismissed, the regulatory bodies have used new language to define the liability of CISOs explicitly.

An Empty Response to CISO Liability

Most organizations have implemented policy modifications to reflect the changing accountability structures, according to 94% of respondents. Numerous organizations implement changes that lack genuine substance. The most commonly implemented measure, which grants CISOs attendance rights at strategic discussions, stands as an unremarkable development (41%).

Some measures are defensive or box-ticking exercises. The 41% of organizations that plan “increased scrutiny of security disclosure documentation from supervisory agencies” are simply committing to rule compliance. The same proportion of organizations plan to provide legal defense to their cybersecurity employees for potential agency investigations. Among the surveyed group, only 22% of respondents stated that CISOs face legal obligations for cybersecurity standards.

“These security measures are nice, but little more than self-preservation”, says Fastly CISO Marshall Erwin. “Those aren’t actually improving your security posture.”

Who Does the Buck Stop With?

A major problem stems from an unclear distribution of cybersecurity incident responsibility among different parties. The organization lacks an explicit cybersecurity leader because multiple staff members at various levels demonstrate minor accountability responsibilities. According to the survey results, the CISO ranks third in accountability at 12%, with security engineers taking first place with 27%. Security managers come in second at 20%.

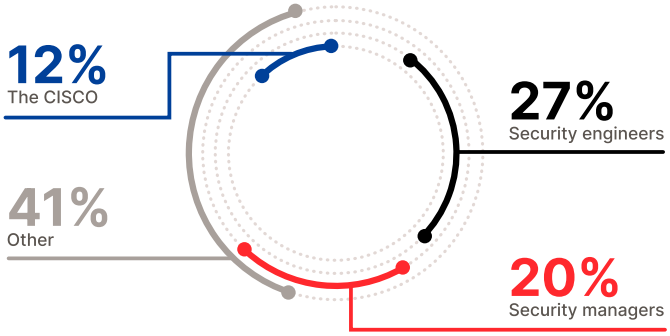
Some positive indicators exist. The increasing number of teams taking on cybersecurity accountability demonstrates that incident responsibility now extends past traditional security roles, which include application developers (11%), site reliability engineers (10%), and SOC analysts (7%).

These theoretical results would create universal responsibility among all individuals. In practice, it means no one is. Only 44% of respondents clearly identify roles and responsibilities for cybersecurity.

This leaves more than half with no clear ultimate responsibility. 45% experience unclear cybersecurity incident accountability. At the end of the day, someone needs to take responsibility.

Figure 3

Who is responsible for cybersecurity incidents



Employees in the Cross Hairs

The entire organization needs to understand security as an organization-wide responsibility while providing employees with the authority to execute policy. Social engineering attacks stand as the most feared security threat for the upcoming year, according to 34% of respondents. The transition to hybrid work environments has created new security challenges because 66% of organizations expect their remote workers to become attack targets.

The majority of organizations (78%) confirm they properly explain cybersecurity compliance to their entire workforce. The approach appears successful because 79% of employees outside IT state their work affects cybersecurity, and 72% of staff members comply with cybersecurity rules. The main challenge stems from insufficient cybersecurity education, which 50% of the Australian and New Zealand organizations face.

The ability to follow established rules depends on having sufficient resources to do so. An impressive 79% of companies say they provide those resources, meaning that only just more than 20% do not. Reporting procedures are not always clear. The majority of respondents (73%) confirm that incident reporting follows a clear process accessible to all staff, but non-IT employees lack confidence in identifying and responding to security threats (65%).

Choosing the Right Tools for a Shifting Landscape

Cybersecurity threats require continuous evolution, which demands corresponding updates to our defensive tools.

34% of the Australian and New Zealand organizations polled identify social engineering as their a significant security concern. This encompasses other common threats like phishing, which is a crucial step in attacks such as business email compromise and ransomware. (Lack of relevant technical skills was the top priority at 37%.)

Multiple security threats converge into an intricate environment, which complicates the situation further. The threat of account takeover identified by 22% of respondents originates from phishing attacks. Data exfiltration (a worry for 35% of those asked) is a common outcome of ransomware compromise.

As mentioned earlier, the SolarWinds hack as well as the Kaseya ransomware attack have led organizations to identify third-party compromise as a significant security concern, according to 27% of respondents.

Investing for Protection

The broad investment of organizations into protection measures includes strategic purchases of products and services aimed at countering threats. Organizations show positive investment trends toward contemporary authentication systems, which rank as the third-most important investment at 40%. Identity and access management tools, together with multi-factor authentication, will help organizations fight against social engineering attacks that serve as the foundation for many other security threats.

The growing danger of API exploitation makes many organizations reconsider their security measures through API gateway security investments, which reached 41%. A total of 31% of organizations have purchased web application firewalls. The investment in WAF products exceeded the 24% of organizations that expressed concern about web application exploitation, yet these products serve as standard defensive measures against multiple attack types, including small DDoS events. Web application and API security solutions receive an average yearly investment of $1.58 million from organizations.

We were surprised to find DDoS investments in eighth place, at 27%, and bot mitigation near the bottom at 18%. Bots serve as primary instruments in credential stuffing attacks, which frequently lead to account takeover incidents.

The investment went toward incident response services to manage cybersecurity incidents. Risk transfer stands as one possible approach, which shares the top investment rank with modern authentication at 42%, along with cyber insurance. Organizations choose to prevent cyber threats and respond to incidents through managed security services companies, since a staggering 34% of respondents have adopted this approach.

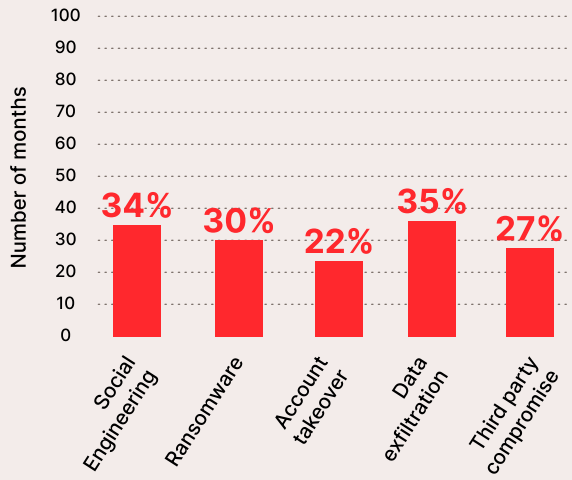
Organizations that choose security outsourcing often work with multiple service providers, since 24% of all survey participants adopted this approach, while 28% placed their security response under a single external service provider. 23% of organizations choose to unite their security response activities under internal teams, while 23% split their security response activities between internal teams and external partners.

The Current Security Tools Remain Difficult to Integrate With Each Other

The use of duplicate tool sets creates difficulties for respondents. On average, organizations make use of 7.85 network and application security solutions, while Australia and New Zealand combined reported 7.65 solutions. Among those polled, there's a 33.5% tool redundancy rate.

Figure 4

Primary reason for wanting to consolidate tools



Rewriting the Security Playbook: Centralized and Built-In from Day One

If there's one key takeaway from our latest survey, it's this: businesses are caught between escalating cyber threats and limited cybersecurity budgets. While 81% of those polled recognize cybersecurity as essential, almost half (46%) admit they still feel vulnerable due to underinvestment. Many plan to increase spending, but history shows that intent doesn't always lead to action. A major hurdle? Justifying the cost to senior leadership, who often see greater value in directing those funds elsewhere.

The reliance on fragmented and overlapping tool sets exacerbates this problem because these cybersecurity franken-stacks are both expensive and complex to integrate and maintain. They are also a natural consequence of reactive cybersecurity strategies that evolve piecemeal over time to track a changing threat landscape.

Time for Security by Design

Organizations must innovate to tackle burgeoning security risks more efficiently while stopping costs and complexity from spiraling out of control. This demands a standard mechanism of identifying and mitigating threats that they can apply across the whole business.

Toolset consolidation is a key component of this mechanism, as it helps to reduce complexity and cost. It requires mature risk management, mapping tool functions to risks based on each risk's impact and probability. This will vary based on factors such as sector and company size.

The other requirement is a set of universal principles for security, and the will to apply them in the development of everything from customer-facing products and services through to internal workflows. Applied from the design stage onward, this will strengthen security from the inside out.

Implementing this security by design concept into software architecture is a priority for just 17% of our respondents, ranking sixth among other mitigations. That's understandable, because it's a cultural change as much as a technical one, and those are difficult to engineer.

We also face another problem: 36% of our respondents feel that cybersecurity is a waste of time and budget that would be better spent elsewhere. Those feeling that way are far more likely to decrease their cybersecurity investment (55%).

Lack of cybersecurity visibility among senior executives is a problem here, warns Fastly's CISO Mashall Erwin. "If your security program is effective, then you are mitigating a lot of risk and reducing the likelihood of compromise or incident. However, your leadership will not see that value directly," he says.

This attitude will be more difficult to change, but mapping a direct line between cybersecurity investments and quantifiable risk-based outcomes is the first step.

About Fastly

Fastly's powerful and programmable edge cloud platform helps the world's top brands deliver online experiences that are fast, safe, and engaging through edge compute, delivery, security, and observability offerings that improve site performance, enhance security, and empower innovation at global scale. Compared to other providers, Fastly's powerful, high-performance, and modern platform architecture empowers developers to deliver secure websites and apps with rapid time-to- market and demonstrated, industry-leading cost savings. Organizations around the world trust Fastly to help them upgrade the internet experience, including Reddit, Neiman Marcus, Universal Music Group, and SeatGeek. Learn more about Fastly at https://www.fastly.com, and follow us @fastly.