Global Security Research Report

Cybersecurity at the crossroads

Why companies face a cybersecurity dilemma - and what to do about it

fastly

Table of Contents

01 Executive Summary

02 Reality isn't meeting expectations when it comes to cyber incident recovery

03 How confident are organizations in their security infrastructure, and how confident should they be?

04 Is cybersecurity spending falling behind?

05 Mapping the shift in accountability

06 Rethinking the cybersecurity talent gap

07 Choosing the right tools for a shifting threat landscape

08 Why it's time to consolidate, centralize, and bake in security from the beginning

10 About the research

Executive Summary

The last year has seen the cybersecurity stakes continue to grow. Thieves stole call data for almost all AT&T's customers[1]. An attack on UnitedHealth saw the exposure of personal health information that could be owned by "a substantial proportion of people in America"[2]. Chinese hacking group Salt Typhoon is said to have targeted Donald Trump and his colleagues by hacking US telecommunications networks[3]. The world suffered what was arguably the most significant cyber outage to date as a misconfigured CrowdStrike update took millions of Windows PCs offline.

Against this backdrop, the need for more cybersecurity and digital resilience is greater than ever - yet 2024 finds security programs in a precarious position. The headwinds facing cybersecurity initiatives are more significant now than they were last year. Many of these are non-technical, covering issues such as budget scrutiny and confusion over who is responsible for cybersecurity in organizations.

Cybersecurity is at a crossroads. To gain more insight into how corporations are dealing with key cybersecurity issues and where the industry is headed, in September 2024 Fastly worked with business and consumer market research agency Sapio to survey 1800 IT decision makers with an influence in cybersecurity. This report offers deep insights into their 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 people (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 part with that budget. That's because the C-suite has plenty of other priorities to address, especially in areas such as digital transformation and IT modernization. They feel that cybersecurity initiatives slow these 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 and 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.

---

1 Whittaker, Zack. "AT&T says criminals stole phone records of 'nearly all' customers in new data breach | TechCrunch." TechCrunch, 12 July 2024, techcrunch.com/2024/07/12/att-phone-records-stolen-data-breach.

2 UnitedHealth Group. "UnitedHealth Group Updates on Change Healthcare Cyberattack." UnitedHealth Group, 22 Apr. 2024, www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html.

3 Barrett, Devlin. "What to Know About the Chinese Hackers Who Targeted the 2024 Campaigns." N.Y. Times, 26 Oct. 2024, www.nytimes.com/2024/10/26/us/politics/salt-typhoon-hack-what-we-know.html.

Reality isn't meeting expectations when it comes to cyber incident recovery

2024 was a milestone year for cyber incidents. The CrowdStrike incident, which crashed approximately 8.5m Windows systems globally[4], sparked business disruptions in sectors ranging from finance to air travel and manufacturing. Outages like these are bound to occur at some point and unavoidable, but how well prepared are we to cope with them?

Organizations are not as good at recovering from cyber incidents as they think. On average, they expect recovery to take 5.85 months. In practice, it takes around 25% longer, at 7.34 months.

Recovery times rise as cybersecurity investment falls. Companies that plan to spend less during the coming year expect recovery to take over 8 months. The gap between perception and reality also rises, with recovery among companies planning to invest less in cybersecurity taking a third longer than they expect at nearly 11 months. Companies committed to cybersecurity spending recover more quickly from cybersecurity incidents compared to those who plan to cut their cybersecurity spending.

Preventative activities top the list of recovery measures

The top two actions taken in response to cyber incidents - implementing stronger security measures (43%) and offering additional training to employees (41%) - fall into the 'lessons learned' category as preventative actions to avert future incidents. Respondents are also more focused on software patches, with 86% changing their approach to patch testing or deployment after the CrowdStrike event.

Fewer companies cite specific activities to help with incident recovery such as restoring from backups (38%) and stakeholder communication (34%). Forensic analysis - useful when building a legal case against malicious insiders or external attackers, or reporting to regulators - is least popular at 25%. Positively, 32% of respondents are committing extra money for incident response playbooks and supporting tools. *(Figure 1)*

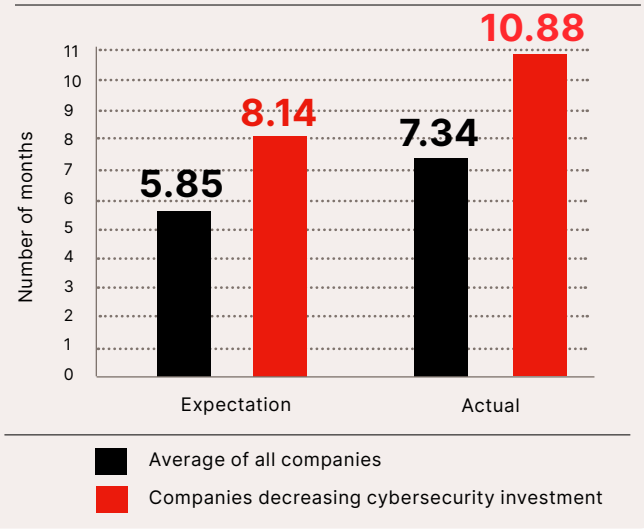
Businesses favor in-house recovery teams, with 61% calling upon their IT teams and 39% working with external cybersecurity firms to help get them back on track. They relied less on invoking insurance to cover costs, with fewer than one in three respondents doing so. Market data suggests that it will become harder to get cyber insurance, as the average cost of a data breach soars to $4.88m - its highest ever[5].

Organizations also take a dim view of third-party partners who contribute to these cyber incidents. In the wake of last summer's global IT outage, 29% would consider changing cybersecurity vendors following high-profile security incidents or software quality problems. Almost half (48%) are rethinking how they use their existing cybersecurity tools.

The focus on prevention demonstrates an increased awareness that prevention is better than cure; cybersecurity should be a proactive measure. However, a coordinated and well-funded response is still crucial to deal with attacks that break through these defenses.

Figure 1

Recovery time after cybersecurity incidents



4 Weston, David. "Helping our customers through the CrowdStrike outage". Microsoft, 20 July 2024, https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

5 "Cost of a data breach 2024 | IBM." 4 Nov. 2024, www.ibm.com/reports/data-breach.

How confident are organizations in their security infrastructure, and how confident should they be?

Almost no companies are untouched by cyber incidents. On average, they have suffered almost 40 known cyber incidents in the last year, and fewer than one in ten have experienced none. US organizations have seen the most - on average one incident per week. Larger organizations have fared even worse, with 64 incidents a year on average, reflecting their high attack surface.

Plenty of threats stem from simple mistakes. Misconfigured IT assets have caused problems for 25% of respondents. Other problems include software bugs (33%). However, the patches and other IT changes to stop them often don't come quickly enough, causing security problems for 18% of companies. Secure DevOps (SecDevOps) can help by preventing bugs and accelerating IT changes to fix any vulnerabilities that make it through.

Tension between manual processes and automation stands out. Manual processes are a factor in 24% of incidents. Many companies still depend on employees manually following security processes and policies rather than designing security directly into technology solutions. That caused problems for 16% of respondents.

Cyber incidents wreak havoc

Cyber incidents caused revenue loss for almost a quarter (23%) of respondents, who lost 3% on average from a cyber incident in 2024. Downtime is another big consequence, as demonstrated by recent outages, followed by lost data.

Regulatory fines and legal action are also risks associated with cyber incidents. Compliance violations have been an issue for 17% of respondents, and 19% have seen customer accounts compromised, potentially violating privacy laws.

Reputational damage is a big factor, affecting 22% of companies, while 18% and 19% respectively report a loss of customer trust and falling customer satisfaction. This affects client retention; 14% of respondents have seen more customer churn after an incident.

Facing down another year of threats

Concern over cyber threats is ongoing. The specter of more automated attackers keeps 42% of respondents up at night. Many worry that their own cybersecurity technologies are not keeping up, with 29% bemoaning a lack of defense automation and a quarter fretting about slow change management. Automating cybersecurity is the second highest security priority for respondents in the next 12 months, at 21%.

Worry about cyber defense affects the quest for more innovation elsewhere. Digital transformation brings opportunities for growth, but 40% worry that the extra software and digital infrastructure will make them more vulnerable to attackers, especially given that 32% don't feel experienced enough to secure modern complex software architectures.

Around half (52%) believe that they are unprepared to deal with sophisticated threats, while 46% feel they lack robust internal cybersecurity technologies.

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 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.

In 2023, three quarters of our survey base planned to invest more in cybersecurity. A year on, half of all companies feel that they have under-invested in key areas of cybersecurity and worry that this has left them vulnerable to attack. 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 under-invested 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 dollars; 36% said they had invested far too much, with no clear plans on where to allocate resources.

Those making cuts are the last ones that should

On the upside, at 87% even more organizations than last year plan to increase their investment in cybersecurity. However, given that 76% of companies planned to invest more in cybersecurity last year and that half still feel under-invested this year, intentions might not reflect reality.

Only 4% plan to reduce their cybersecurity investment, which as Fastly's Director, Technical Strategy, Jay Coley points out might not mean reducing functionality. "They may also be moving to cheaper solutions, consolidating contracts for cost efficiencies or even looking at open source options," he points out.

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 investment

Companies can achieve a lot by investing in the preventative 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.

Mapping the shift in accountability

If a cyber incident occurs, who is held accountable? Increasingly, regulators are pointing to the chief information security officer (CISO). In October 2023, the SEC prosecuted not just SolarWinds but its CISO Timothy G. Brown with fraud and internal control failures (most charges were dismissed)[6]. The SEC and other regulatory bodies have adjusted their language to make the CISO's liability clearer?

An empty response to CISO liability

Respondents are aware of the accountability shift, with 93% making related policy changes. However, in many cases these are not meaningful. The most common measure cited - finally giving the CISO a seat at the table when discussing strategic decisions (41%) - is hardly revolutionary.

Some measures are defensive or box-ticking exercises. The 38% promising 'increased scrutiny of security disclosure documentation from supervisory agencies' are simply committing to read the rules. The same proportion promise more legal support for their cybersecurity staff to protect them should those agencies come calling. Barely one in five (21%) stress that CISOs are bound by law with regards to cybersecurity.

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

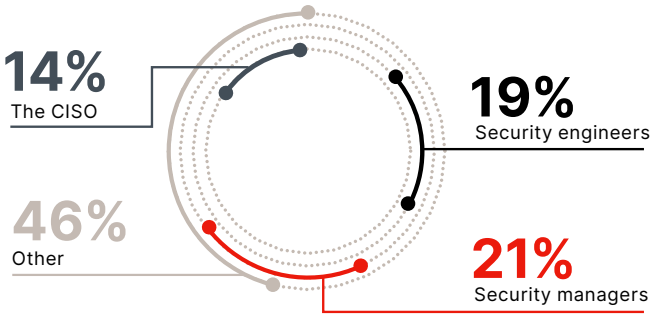
Who does the buck stop with?

Part of the problem lies with a lack of clarity over who is responsible for cybersecurity incidents. There is no clear leader responsible, with various roles at different levels feeling somewhat accountable. The CISO actually comes third, at 14%, behind security engineers (19%) and security managers (21%). (*Figure 2)*

There are some encouraging signs. The rise in accountability across teams like application developers (10%), platform engineers (8%) and site reliability engineers (7%) suggests that responsibility for cybersecurity incidents is no longer siloed within security-specific roles.

In an ideal world, these figures would mean that everyone is responsible. In practice, it means no one is. Only 36% of respondents clearly identify roles and responsibilities for cybersecurity. This leaves nearly two-thirds with no clear ultimate responsibility, and 46% feel there is a lack of clarity around who is responsible for cybersecurity incidents. Ultimately, someone has to step up.

Figure 2
Who is responsible for cybersecurity incidents



Employees in the Cross Hairs

For security to truly be a pan-organizational responsibility, all employees must be aware of it and empowered to follow policy. Social engineering attacks - the most feared threat among respondents in the coming year at **37%**- squarely target employees. The rise in hybrid work has also had a security impact, with **70%** of companies fearing attacks on remote workers.

Many (**77%**) believe that they communicate the importance of cybersecurity compliance to all employees. This seems to be working, as **70%** say non-IT workers understand their impact on cybersecurity, and 69% say that all employees follow cybersecurity rules. However, there are some caveats; **55%** cite a lack of internal education around cybersecurity best practices.

Knowing the rules is one step, but another is having the resources to follow them. While **72%** of companies say they provide those resources, meaning that over a quarter do not. Reporting procedures are not always clear. While **73%** of respondents claim a clear and universally accessible process for reporting incidents, fewer (**63%**) feel that non-IT staff are confident about identifying and responding to potential threats.

6 Becky Bracken, Senior Editor. "Sizable Chunk of SEC Charges Against SolarWinds Tossed Out of Court." Dark Reading, 18 July 2024, www.darkreading.com/application-security/solarwinds-charges-tossed-out-of-court-in-legal-victory-against-sec.

Rethinking the cybersecurity talent gap

Skills are a big stumbling block in cybersecurity, with 30% of respondents citing a lack of skills to counter modern security threats as a challenge. Almost half (47%) haven't invested enough in cybersecurity talent through new hires and wage increases. Training and talent acquisition is the top priority in the coming year, at 28%.

Companies might be looking for talent in the wrong places. Half (51%) aren't finding the skills they need in the talent pool. In fact, only 13% see no significant issues with the current talent on offer for cybersecurity recruiters.

It takes substantial time and effort to mold a raw recruit into a productive member of the security team. Fresh cybersecurity graduates must learn more technical skills, such as how to work with a company's specific toolset and workflow, along with organization-specific cultural nuances.

These challenges will only increase as companies scale. Working in larger, constantly evolving environments is a challenge for employees, with 17% of respondents citing the talent pool's inexperience with large-scale technologies and enterprises as a problem.

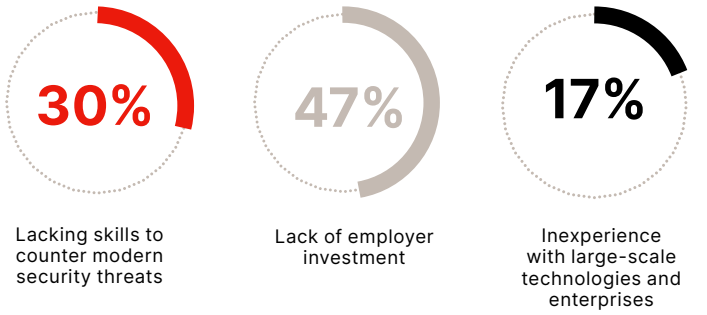
Alternatives to external recruitment

With these challenges in mind, perhaps companies should be focusing inward for skills development? There are several options:

- **Upskilling.** Training existing staff for new responsibilities means they're already aligned with your culture and at least partly fluent in your specific systems and processes.
- **Mentoring.** On-the-job training from more experienced staff is an invaluable way of cementing a junior employee's skills and shaping them for success.
- **Cross-functional collaboration.** Better communication between security and other teams such as IT, compliance, support, and product development can create well-rounded employees with a strong sense of how security fits into other functions. There are even opportunities for secondments here. The ideal outcome is an expansion of skill and responsibility to non-security teams. A product development team with a better understanding of security could foster secure-by-design principles in its development practice, for example.

Sourcing talent from within - especially from across different functions - carries several advantages. It helps to promote the idea that everyone is responsible for security. It also supports the drive for digital transformation. With 40% of companies worrying that digital transformation initiatives will increase their vulnerability to attack, an integrated security culture can help to drive security throughout the transformation process.

Figure 3
Shortcomings in the current talent pool



Choosing the right tools for a shifting threat landscape

With cybersecurity threats constantly evolving, the tools we use to protect ourselves must do the same.

Social engineering is the most worrisome threat vector for many companies, at 37%. This encompasses other common threats like phishing, which is a crucial step in attacks such as business email compromise and ransomware (the latter is the second most feared threat, at 34%).

Many threats overlap, creating an even more complex landscape. Account takeover (which 20% of respondents cited as a threat) is often a direct outcome of phishing. Data exfiltration (a worry for 28% of people) is a common outcome of ransomware compromise.

Third-party compromise, which 20% of respondents cited, has become a particular worry for companies in the wake of incidents such as the 2020 SolarWinds hack and the 2021 Kaseya ransomware attack. More recently, we've seen Amex credit cards exposed in a third-party breach , and the UnitedHealth breach brought large parts of the healthcare ecosystem to a standstill. *(Figure 4)*

Investing for protection

Organizations are investing broadly to protect themselves, with some thoughtful product and service purchases to help fend off these threats. We're pleased to see modern authentication features among the top two investments, at 35%. The use of tools such as identity and access management, along with multi-factor authentication, will help to mitigate the social engineering attacks that form the basis of so many other threats.

The rising threat of API exploitation has given many companies pause, prompting 29% to invest in API gateway security. The same percentage have also invested in web application firewalls. This was more than the 21% who cited web application exploitation as a concern, although WAF products are also a common form of layered defense against other attacks, including low-volume DDoS. On average, organizations spend $1.58m annually on web application and API security solutions.

We were surprised to find DDoS investments down in ninth place, at 25%, and bot mitigation near the bottom at 15%. Bots are a common tool in credential stuffing attacks, which are a frequent factor in account takeover.

Respondents also invested in services to mitigate cybersecurity incidents. One approach is risk transfer; cyber insurance tied with modern authentication as the top investment, at 35%. Another is to outsource cybersecurity prevention and incident response to a managed security services company, which 29% of respondents do.

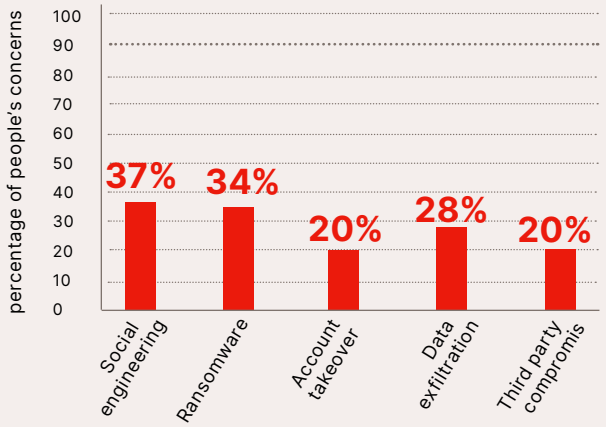
Those that outsource security often use multiple providers, with 27% of all respondents reporting this approach, while 32% have their security response under a single external service provider. 17% prefer to consolidate their security response under an internal team, while 18% use a mixture of both approaches.

Toolsets are still fragmented

Overlapping tool sets is a problem for respondents. On average, organizations rely on 7.85 network and application security solutions, with those in the Nordic region using the most at a whopping 9.4. Well over a third (37.7%) of these tools overlap, although that's a slight improvement on last year's 41%.

Figure 4

Primary reason for wanting to consolidate tools



Why it's time to consolidate, centralize, and bake in security from the beginning

If there's one takeaway from our 2024 survey it's this: businesses face tensions between rising cyber threats and constraints on cybersecurity investment. With 75% agreeing that cybersecurity is essential but 50% feeling vulnerable because of an inadequate investment in protection, it's no wonder that many of them hope to invest more in protection. However, history has shown that they don't always follow through. That's at least in part because it's difficult to justify those costs to senior leadership. Executives feel they can better use that money elsewhere.

The reliance on fragmented and overlapping tool sets exacerbates this problem, because these cybersecurity franken-stacks are both expensive and complex to integrate. 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 cyber 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 (see box: Thinking Vertically).

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 18% 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: 34% of our respondents feel that cybersecurity is a waste of time and budget that would better be spent elsewhere. Those feeling that way are far more likely to be decreasing their cybersecurity investment (55%).

Lack of cybersecurity visibility among senior executives is a problem here, warns 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.

Thinking Vertically

Cybersecurity threats are rampant, but they're not evenly distributed. Each vertical sector faces its own profile of weighted risk. This year we looked at six sectors, up from last year's four.

Finance Two in five cybersecurity professionals (41%) working in financial services and accounting predict social engineering attacks - phishing, smishing etc. - to be the biggest threat driver. Financial decision makers are 08% more likely to consider it a major threat compared to the average across other industries.

Public sector Government organizations are particularly at risk of DDoS threats, with 15% experiencing service disruptions from these attacks as geopolitical tensions rise. However, this doesn't mean that attackers aren't after government data too, with almost half (47%) reporting a downtime or outage, and over one third (35%) data loss, as the main impact of security incidents.

continued on next page

Thinking Vertically *continued*

Healthcare While criminals attack finance companies to move money, the goal in healthcare is patient data, which fetches plenty of money on the dark web. That's why 39% of healthcare and life sciences organizations have suffered data loss from security incidents - 7% higher than the average across all sectors. It's no surprise therefore that data exfiltration is one of the biggest threat drivers for healthcare companies over the next 12 months.

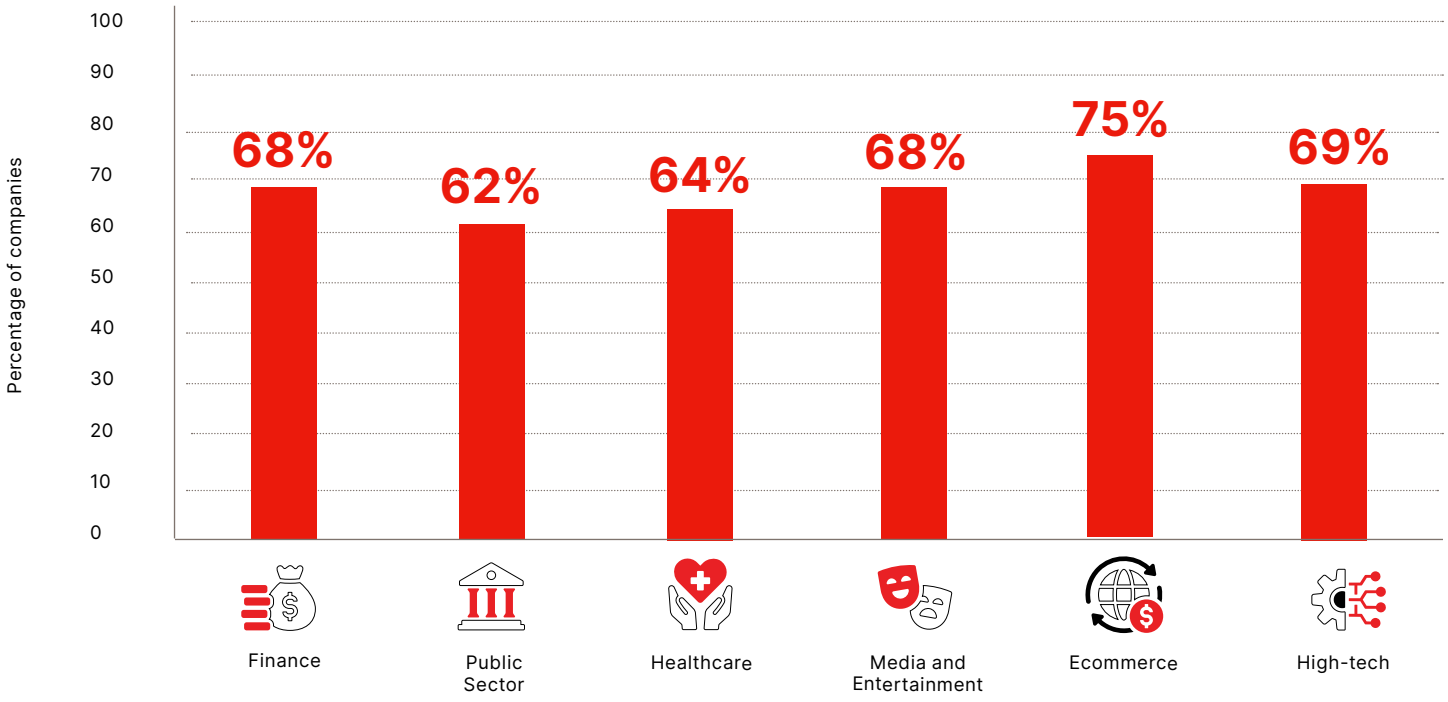
Media and entertainment The crown jewel in this sector is content. In fact, cybersecurity professionals working in the media and entertainment industries are 36% more likely to be concerned about unauthorized scraping of proprietary content being a major threat driver over the next 12 months than other industries.

Ecommerce Retailers face attacks on multiple fronts, from theft of credit card details through to shipping fraud and customer account takeover, with over one in five (22%) retailers predicting that account takeovers would be the biggest cybersecurity threat, reinforcing the need for secure authentication.

High-tech Intellectual property is the holy grail for black-hat hackers targeting high-tech firms, but user accounts are also easy to monetize, which is why 22% of companies in this sector predict account takeover threats as the biggest cybersecurity threat over the next 12 months. Those working in tech are less concerned about ransomware and extortion being a main threat driver over the next 12 months.

While each sector faces its own risk, half of all surveyed (52%) agree on one thing: as the threat landscape becomes more sophisticated, they are ill-prepared to deal with future attacks.

Percentage of companies that had a security incident in the last 12 months



About the research

This research surveyed 1,800 key IT decision makers with an influence in cybersecurity, in large organizations spanning multiple industries across North, Central and South America, Europe, Asia-Pacific, and Japan.

The interviews were conducted online by Sapio Research in September 2024 using an email invitation and an online survey. Results of any sample are subject to sampling variation.

The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. In this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 2.6 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

About Sapio

Best new agency finalist, Sapio is adept at opinion polling (we have access to 80 million people internationally), focus groups, face-to-face interviews, telephone interviews, online research, desk research and statistical modelling to mention just a few techniques. We love B2B research and consultancy. Our business is based on partnership principles inspired by social enterprise.

About Fastly, Inc.

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.