2024

State of Security

The Race to Harness AI

splunk>

As a security professional and leader for over twenty years, I've witnessed the industry evolve many times over. But this time is different. Cybersecurity is rushing into a new frontier — one rife with opportunity and risk with the rise of generative AI. In Splunk's 2024 State of Security Report, we found that many CISOs and practitioners are blazing this trail without looking back. But they're also not sure what's ahead, given new compliance regulations and their impact on CISO accountability.

In today's cyber environment, we expect security professionals to explore how generative AI can empower their resilience journey — and with a staggering 93% of respondents claiming adoption, many already see it as a critical point of innovation. They're using generative AI to build better cyber defenses, execute more informed decisions, and fill critical skills gaps. At the same time, at least one-third of respondents have no generative AI policies. And their biggest reported fear? AI-powered attacks.

Meanwhile, more punitive incident reporting rules by the U.S. Securities and Exchange Commission (SEC) and the E.U.'s NIS2 are holding the CISO community to greater accountability. But we believe security professionals will also discover new opportunities to reshape their roles and teams. For CISOs, that means asserting priorities in the boardroom, and for security practitioners, it calls for tighter collaboration with ITOps, engineering, and cloud teams to expand visibility, minimize response times, and take resilience to new levels.

While security professionals continue to forge this new path, at Splunk we are excited about the potential of generative AI for defenders and encouraged by how quickly security priorities are becoming business priorities.

Jason Lee

Chief Information Security Officer, Splunk

Innovation in flux

The state of security in 2024 is a bit of a contradiction. Despite the obstacles in security professionals' paths — stringent compliance requirements, escalating geopolitical tensions, and a more sophisticated threat landscape — the industry is making progress.

Many organizations report that cybersecurity is becoming easier to manage compared to previous years. Organizations collaborate more and detect threats faster, and most have the authority and resources to solve the issues they face.

Complete victory remains elusive, however, as defenders attempt to outrun adversaries in the race to harness generative AI. Security teams are understandably concerned that generative AI will intensify the impact of the same attacks they've skillfully thwarted for years.

We think defenders are up to the task. The full impact of generative AI on cybersecurity may be unknown, but one thing we do know: The race is on.

Contents

Cybersecurity is trending easier over time

Being a defender means you rarely see the fruits of your labor. It's only natural to wonder: is any of this working? When it comes to keeping up with cybersecurity requirements, respondents were almost evenly split: 41% say it has become easier, while 46% find it more difficult.

However, the macro trends paint a hopeful picture. Since Splunk's State of Security 2022, managing cybersecurity is trending easier.

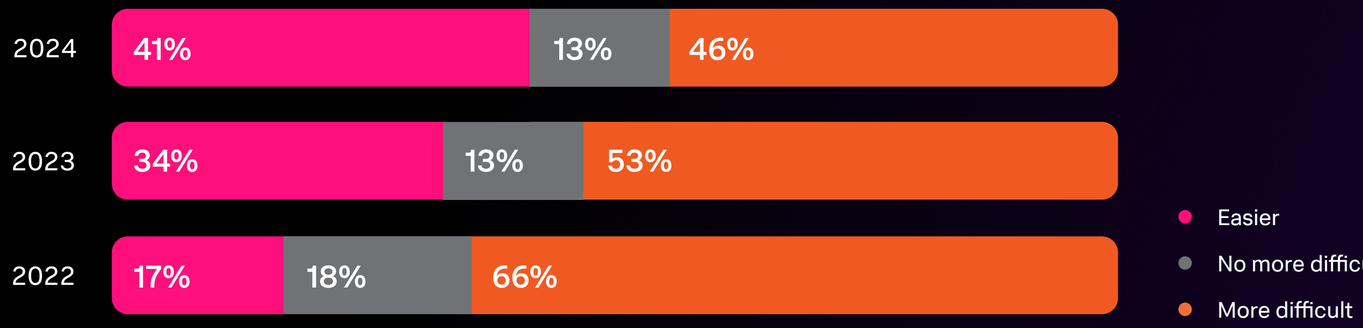
This perception may be surprising given increasing environmental complexity and attack sophistication. But it's likely easier for organizations with well-established security controls and processes to stay ahead of threat actors relying on tried-and-true attack strategies.

Collaboration may be one reason cybersecurity is getting easier: 87% of respondents say they are working more closely with other teams compared to a year ago. Three-quarters (75%) of respondents are joining forces more with IT operations this year.

In addition, 54% are collaborating more with software engineering — and when security starts early in the design and coding phases, addressing vulnerabilities becomes more manageable.

Organizations are also detecting threats faster. Fifty-five percent of respondents estimate their mean time to detect (MTTD) distruption-causing incidents as 14 days or less. This marks a significant improvement from last year, when only 28% of respondents estimated detection within the same timeframe. However, this is still too much time for attackers to access systems.

Keeping up with cybersecurity requirements over the past two years



But the battle isn’t over

Among those who say cybersecurity is getting more difficult, 38% cite threat landscape sophistication as the reason why. Geopolitical tensions and cyber warfare are on the rise. IoT, AI, and multicloud environments are increasing data volumes exponentially. And as a result, organizations still trying to implement basic cybersecurity controls will struggle to secure additional assets and endpoints. They’ll also have a harder time protecting against simple human errors, like misconfigurations, which rank as this year’s top threat vector.

Tighter compliance requirements also raise the stakes, particularly for security executives who are now personally on the hook for their organizations’ violations. Twenty-eight percent agree that regulatory compliance is making the job harder. And new government mandates will only ratchet up the pressure.

Similar to previous years, 27% of security teams struggle to address emergencies and dedicate adequate time to improve cybersecurity, indicating a lack of long-term strategy and investment. A barrage of security alerts also makes it difficult to keep up — 26% agree the volume is troublesome.

AI rises above the clouds

One of the most notable findings in this year’s survey is that AI hype is on par with reality. Nearly half (44%) of respondents cite AI as among their three main initiatives in 2024, surpassing cloud security.

While security teams recognize the many benefits of AI, so do threat actors that are unencumbered by laws and policies. When asked whether AI will tip the scales in favor of defenders or adversaries, respondents are almost evenly divided: 45% predict adversaries will benefit most, while 43% say defenders will come out on top.

The meteoric rise of generative AI sparks the imagination of what *could* be, but it also raises serious questions about what *will* be. What will it mean for the SOC? Will organizations introduce policies to encourage safe and effective usage? How will they enforce those policies without hampering innovation? The answers are starting to take shape.

Top security initiatives of 2024

Entering the AI gold rush

During the California Gold Rush, hundreds of thousands of prospectors with dreams of striking it rich migrated west. Similarly, today's generative AI boom involves chasing opportunity at breakneck speed into an unknown frontier, where the possibilities feel endless and the risks perilous. Everybody wants to strike the mother lode and enjoy first-mover advantage. It's possible — it just takes a little digging.

The promise and possibility of generative AI

Generative AI has gone mainstream, and organizations are actively implementing it to transform their businesses. From serving up personalized customer recommendations in e-commerce to mapping the human brain to imitating the brushstrokes of Rembrandt, generative AI boasts an assortment of use cases in nearly every industry.

These aren't mere speculations. Ninety-three percent of respondents report that line-of-business end users rely on public generative AI tools to help them do their jobs. This creates more work for security teams who protect the business from generative AI-related vulnerabilities such as data leakage.

Optimism about generative AI is powerful enough to sway even the most skeptical security professionals. Adoption is nearly as high among security teams as the overall business, with 91% of respondents using public generative AI. What's more, they're rooting for generative AI's success, with 46% declaring that generative AI will be "game-changing" for their security teams.

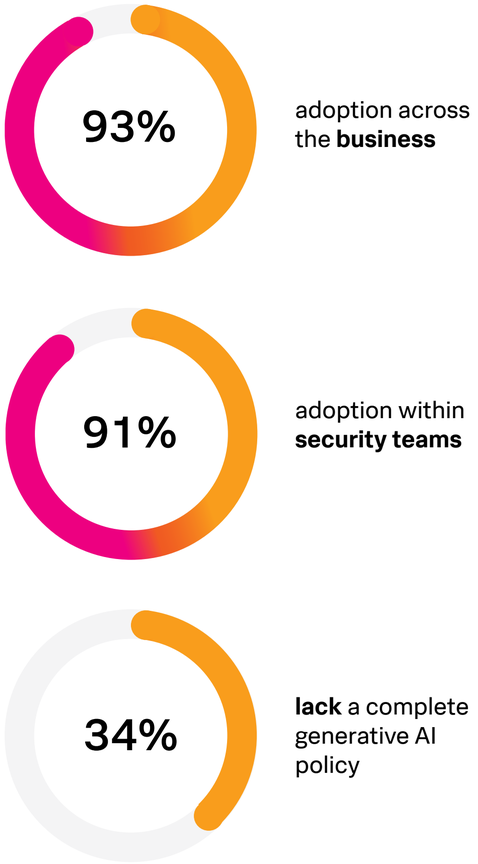
The race to harness generative AI is so intense that 50% of respondents say their organization is in the midst of developing a formal plan for using generative AI for cybersecurity, but the plan isn't complete or agreed upon.

Security and innovation can go hand in hand if done correctly. At the same time, we wonder if pressure from the business or board — or just good ol' fear of missing out — is driving generative AI adoption among security teams.

Just two years ago, it would've been almost preposterous to ask organizations how many end users are using public generative AI tools — but today, generative AI in the business is table stakes.

— Kirsty Paine, Field CTO and Strategic Advisor for EMEA, Splunk

Generative AI adoption outpaces policy



Generative AI policy is uncharted territory

"Move fast and break things" might sound counterintuitive to most security practitioners, but it could be the right philosophy as organizations seek innovation at speed. And while security teams rarely turn down a chance to write a policy, 34% of organizations do not have a generative AI policy in place, despite its high adoption rate.

"Companies that clamp down too tightly on the use of generative AI risk not only falling behind their competitors, but also leaving themselves open to the threat actors who won't hesitate to use these tools," says Shannon Davis, principal security strategist at Splunk SURGe.

If we learned anything from cloud or IoT adoption, a lack of process and planning could come back to haunt security teams. The push from the business to haphazardly follow these trends resulted in undesirable consequences, such as non-compliant clouds paid on personal credit cards, or unsecured IoT devices rife with software vulnerabilities. Security teams must balance the speed of innovation with thoughtful and sustainable processes.

Robust policies depend on understanding the implications of a technology, yet 65% of respondents admit they lack education around generative AI. Teaching the rest of the organization about generative AI shouldn't be the sole burden of the cybersecurity team, however.

"Organizations should form a cross-functional governance board to oversee the development and adoption of AI with a comprehensive framework for responsible AI," says Hao Yang, VP of AI at Splunk.

The influence of generative AI is wide-reaching, so navigating it calls for a range of perspectives and specializations. Splunk's AI committee, for example, spans multiple business units, including product and technology, legal, privacy, security, human resources, go-to-market, and marketing.

Of course, thoughtful security policies don't necessarily translate to complete prevention, but they can go a long way to minimize data leakage and other new vulnerabilities.

The long arm of the law comes for generative AI

Like internal governance, the frontier of generative AI remains relatively untamed and unregulated by any enforceable laws — for now. However, AI compliance is starting to take shape.

For example, The European Union's AI Act aims to introduce a common regulatory framework based on risk categories. In 2023, the European Parliament amended its initial proposal to include generative AI, which must comply with certain transparency requirements. These requirements include registering the foundation model in a database and developing and retaining technical documentation.

In the United States, the Biden Administration's AI Bill of Rights suggests that users should be notified when they are communicating with an automated system, and allows to opt out and interact with a real person instead. These guidelines could foreshadow future government action.

This impending tsunami of government regulation may be why 45% of respondents name better alignment with compliance requirements as a top area for improvement, right behind data leakage. Getting ahead of this trend requires a renewed focus on internal compliance controls.

Organizations should form a cross-functional governance board to oversee the development and adoption of AI with a comprehensive framework for responsible AI.

— Hao Yang, Vice President of AI, Splunk

Generative AI: Friend or foe?

Who has the generative AI advantage? Respondents are split.

43%

Defenders will benefit most

12%

They will cancel each other out

45%

Adversaries will benefit most

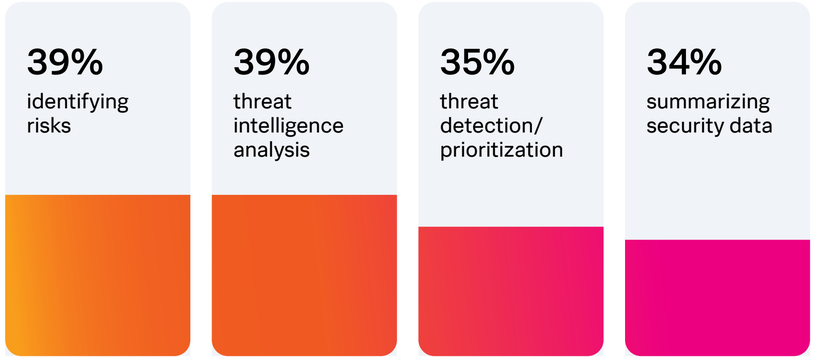
Generative AI as the security sidekick

Perceptions of generative AI are evolving fast. Just eight months ago, only 17% of respondents in our CISO report said generative AI would advantage defenders. Now, almost half (43%) feel the same way.

More and more vendors are incorporating generative AI into their products, demonstrating its use in security workflows, and defenders are starting to see the possibilities. While the potential for novel generative AI-fueled attacks and AI poisoning remains a possibility, they have yet to become commonplace.

Defenders seem optimistic and agree that generative AI is a good match for several cybersecurity use cases, naming threat intelligence analysis and risk identification as the top two applications.

Top generative AI cybersecurity use cases



What generative AI use cases may look like in practice

Identifying risks
Generative AI can enhance risk-based alerting by quickly aggregating diverse datasets to provide security analysts with alerts that are context-rich. Large language models (LLMs) help to deliver this information at a speed and efficiency far beyond human capability.

Threat intelligence analysis
LLMs can determine the indicators of compromise and MITRE ATT&CK techniques described in a threat intelligence report. This would save intelligence teams from a lot of drudgery and enable them to perform deeper analysis faster.

Threat detection and prioritization
Prioritizing and triaging alerts are tasks particularly susceptible to analyst misclassification, fatigue and human errors. Generative AI can parallel process multiple threats while improving accuracy.

Summarizing security data
Generative AI can summarize quickly, thoroughly and accurately to help security teams save time and keep up with news and information, like Biden's Executive Order on Improving the Nation's Cybersecurity.

Solving the cybersecurity skills shortage

Skilled professionals sit at the heart of any SOC, and many organizations are still coping with talent shortages. Generative AI could offer some breathing room to address this very real need.

Eighty-six percent of organizations believe generative AI will help them hire more entry-level cybersecurity talent, and 58% say it would help onboard entry-level talent faster. Ninety percent of respondents say that entry-level staff can lean on generative AI to help develop their skills in the SOC once they're hired — which could include fundamental tasks such as writing a Python script or spinning up test environments.

Generative AI will also be a force multiplier for seasoned security professionals. Sixty-five percent believe it will make them more productive, enabling experienced practitioners to more easily synthesize news and information, and accelerate research and detection engineering.

And while the fear of AI replacing jobs isn't entirely unfounded — about half (49%) say generative AI will eliminate some existing security roles — it's more likely to help organizations train new talent and prevent employee burnout. It could also simply reshuffle the deck of cybersecurity talent as it introduces new roles like prompt engineering.

How generative AI can close skill gaps

86% believe that it can help organizations hire more entry-level talent

65% believe that it will allow seasoned security pros to be more productive

Generative AI as the attacker's ally

Security teams are also rightfully concerned that generative AI is yet another tool in the arsenals of adversaries. Forty-five percent of respondents believe generative AI will be a net win for cyber attackers, and 77% say it expands the attack surface to a concerning degree.

Same attacks, different day

What unique threats will generative AI unleash upon the world? Odds are that instead of an immediate windfall of new attacks, generative AI will amplify threats already confronting security teams.

Thirty-two percent of respondents are most concerned about attackers using generative AI to optimize existing attacks, such as crafting more realistic phishing emails or refining malicious scripts. Less skilled, opportunistic hackers will exploit generative AI to drive a significant uplift in social engineering attacks. And 28% of respondents worry that generative AI will also help adversaries increase the volume of existing attacks.

The enemy within

Not all AI threats originate from outside sources; 77% of respondents agree that more data leakage will accompany increased use of generative AI. However, only 49% are actively prioritizing data leakage prevention — possibly because there aren't many solutions yet that control the flow of data in and out of generative AI tools.

Lack of education around generative AI only amplifies these concerns. When 65% of security executives admit they don't fully understand generative AI, it's fair to assume confusion is even higher among non-security roles. Without the proper education, end users are bound to make mistakes like putting sensitive company data into an LLM, which will place security teams in the crosshairs.

Top uses of generative AI by threat actors

It's like the question, 'Would you rather fight a horse-sized duck or 100 duck-sized horses? It's probably more manageable to focus on a single threat, but generative AI will create the less-appealing scenario, acting as a force multiplier for existing attacks.

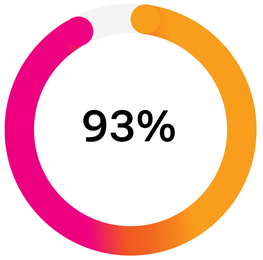
— Kirsty Paine, Field CTO and Strategic Advisor for EMEA, Splunk

Mapping the future of generative AI

Where will generative AI go from here? No one has a crystal ball, but security teams have been embracing traditional forms of AI like machine learning (ML) for some time, and 93% say these experiences will influence their future approach to generative AI.

Many organizations have gotten a taste of the increased productivity that ML tools provide, with 92% receiving substantial advantages already. The technology is not perfect, though, and needs special care: 73% say tools with traditional AI and ML capabilities can generate false positives, and 91% say they require tuning. Similarly, generative AI calls for oversight to spot and prevent hallucinations that can undermine its value.

Those pioneers who have already built a solid foundation with traditional AI and machine learning will likely find themselves on the fast track of their generative AI journeys.



say experiences with ML will influence their future approach to generative AI

The building blocks of leading organizations

In the race to stay ahead of threats, some organizations follow a center of excellence model to build mature cybersecurity practices. In 2024, 47% of respondents identify their security programs as “extremely advanced.” We’re classifying this group as leaders and will be comparing their unique characteristics and survey responses with those of the cohort who labeled their programs as “developing.”

For starters, leaders are confident in their ability to keep up with the threat landscape. Forty-nine percent of leaders say managing cybersecurity requirements is getting easier, while only 29% of respondents with developing programs say the same. Leaders also outperform those with developing programs in several other aspects, painting a picture of what may be considered gold standard practices.

Resource and empower appropriately

Leading organizations aren't born; they are made. Their winning approach reflects a deep connection to the board and business stakeholders, cross-departmental collaboration and steady investments. Leading security teams have the budget to be proactive — 67% are significantly increasing cybersecurity spending in the next one to two years, versus 28% of respondents with developing programs.

A close connection to the business pays off for leading organizations, too. An impressive 95% say they have the resources and authority to address challenges, which mirrors the finding in our CISO Report that 47% of CISOs now report to the CEO.

Collaborate and recognize resilience

Being connected to the business isn't just about having the CEO's ear, it requires partnering across the business. Leading organizations collaborate more with these tech departments:

Collaboration with	Leading organizations	Developing organizations
Software engineering	56%	46%
Engineering operations	51%	31%
IT operations	76%	67%

Collaboration also extends to compliance. Forty-nine percent of leading organizations strongly agree that everyone on the security team makes compliance a part of their jobs, compared to just 27% of organizations with developing security programs.

Leading organizations recognize that there's a lot on the line when it comes to digital resilience. They more strongly agree that greater digital resilience leads to more innovation (41%), less business disruption (39%), and avoiding compliance penalties (39%) — likely because they're more closely connected to business outcomes.

Without executive buy-in, achieving cybersecurity maturity is a losing battle.

— Jason Lee, CISO, Splunk

Innovate more with generative AI

Leading organizations are also more likely to innovate with AI, with 48% declaring it as a top initiative, compared to 30% of their less mature peers. Generative AI adoption among their security teams is higher and more widespread, too — 75% of leaders say that most security team members were using generative AI, and only 23% of developing organizations say the same.

Generative AI usage among leading organizations appears to be less experimental and more methodical in contrast to developing organizations:

- **82% of leaders have established generative AI security policies, while only 46% of developing organizations have done so.**
- **55% of leaders have a formal plan to use generative AI for cybersecurity use cases, while only 15% of developing organizations make this claim.**

Detect and respond to incidents faster

Cyber maturity doesn't translate to fewer cyberattacks. However, leading organizations detect and respond faster than their peers, which softens the blow of an attack and its consequences.

For incidents that caused disruption, leading organizations cite a mean time to detect (MTTD) of 21 days, while developing organizations, on average, spend over a month (34 days) detecting a threat within their networks. Leading organizations also spend far less time in recovery mode. Their average mean time to recover (MTTR) business-critical workloads is just over 44 hours, while developing organizations' average recovery time is 5.7 days.

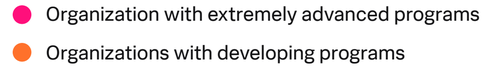
"The ability to reduce detection and response time speaks directly to the maturity of a security program. That's why MTTR and MTTD are such crucial metrics for boards and executives. They want to see measurable success in the long term," says Mick Baccio, global security advisor at Splunk's SURGe security research team.

The ability to reduce detection and response time speaks directly to the maturity of a security program. That's why MTTR and MTTD are such crucial metrics for boards and executives. They want to see measurable success in the long term.

— Mick Baccio, Global Security Advisor, Splunk

The building blocks of a leading organization

Organizations that describe their cybersecurity programs as extremely advanced consistently outperform their peers in four critical dimensions.



Resource and empower appropriately

Will significantly increase cybersecurity spending in the next one to two years:

67%

28%

Say they have the resources and authority to address challenges:

95%

79%

Collaborate and recognize resilience

Increased collaboration with engineering operations within the last year:

51%

31%

Increased collaboration with IT operations within the last year:

76%

67%

Innovate more with generative AI

Have a generative AI security policy:

82%

46%

Say that most security team members are using generative AI:

75%

23%

Detect and respond to incidents faster

MTTD of disruption-causing incidents:

21 days

34 days

MTTR for business-critical workloads:

1.8 days

5.7 days

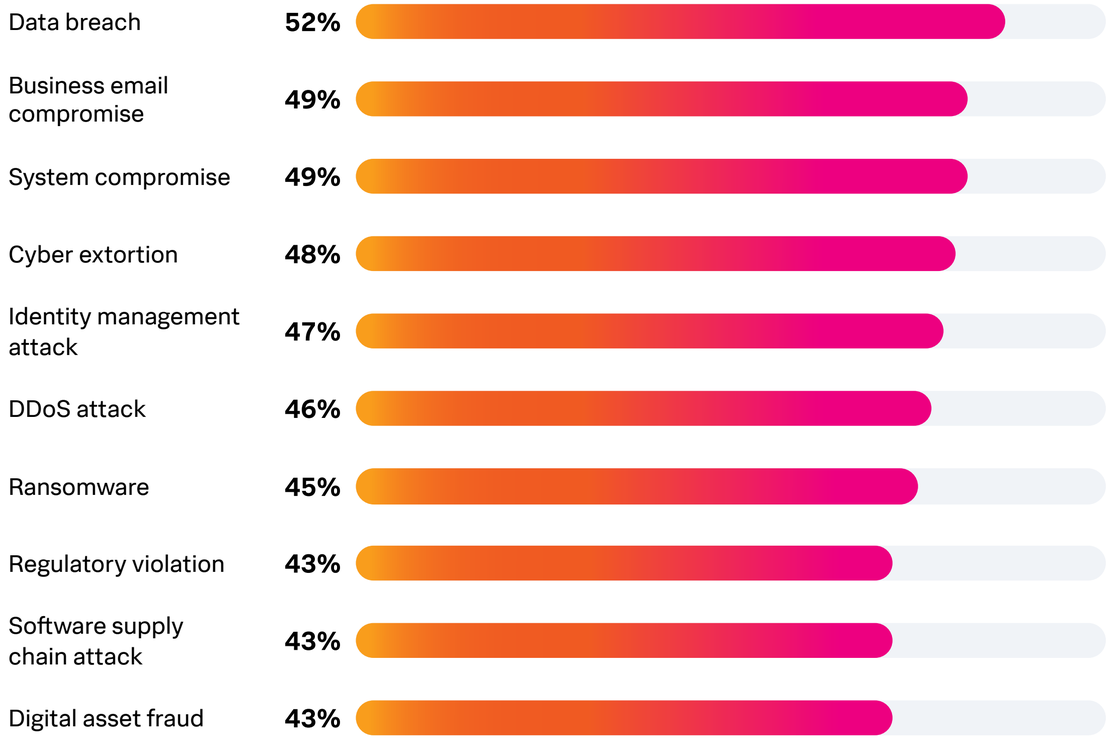
Sizing up the threat landscape

While security teams fight the good fight, threat actors will still find ways to slip past even the best defenses. The State of Security 2024 demonstrates that attackers aren't slowing down, with data breaches and ransomware increasing 13% and 14% respectively since 2021.

In 2024, we've seen attackers use diverse tactics — for example, business email compromise capitalizing on human deception, to DDoS attacks relying on brute force. Despite these varied approaches, these threats share an objective: cause disruption.

Cybersecurity incidents still have far-reaching reputational, legal, and financial consequences, but organizations appear to be better at absorbing the blow — even while enduring more attacks overall. For example, only 44% of respondents say that remediating incidents required significant time and personnel this year, down 13% from last year. Also, fewer respondents lost productivity and suffered confidential data breaches this year, indicating that digital resilience initiatives are working.

Most frequent incidents experienced in the past two years



Cyber anxieties don’t always match realities

While million-dollar ransom payments, CISO indictments and zero-days make great headlines, they are uncommon. When cybersecurity professionals are asked about threats they find most concerning versus those they are *actually* experiencing, their fears are sometimes misplaced.

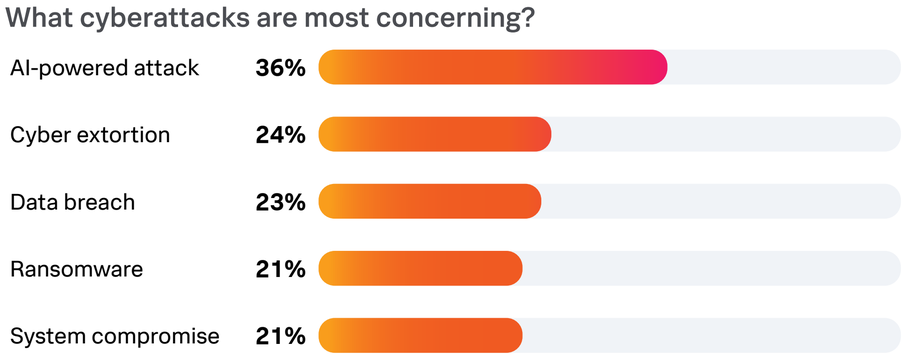
For example, though respondents say AI-powered attacks are their number one concern, they experience data breaches, business email compromise, system compromise, and identity-based attacks far more often.

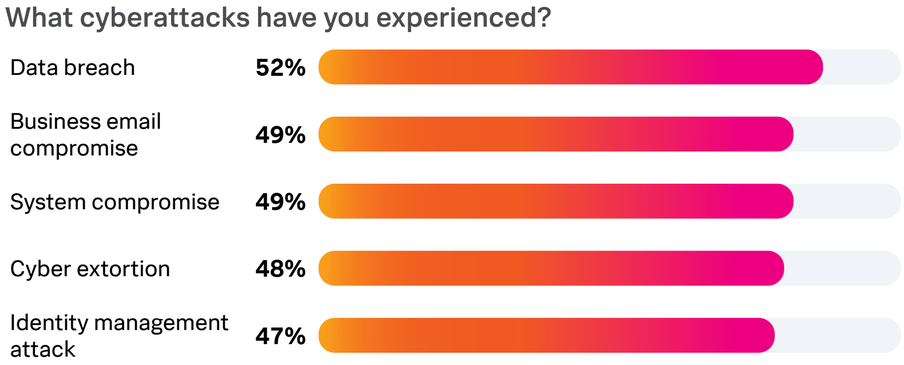
The opposite is also true — the perceived threats pale in comparison to the actual attacks. Only 18% of respondents rank business email compromise (BEC) as their most concerning threat, even though it was number two on the list of most common incidents in 2024.

However, some fears line up to reality. Data breaches, for instance, are both a top concern and the attack experienced most often, with 52% reporting at least one data breach incident in the past two years.

Fear lies in the unknown. Organizations have processes and procedures to defend against well-known attacks like data breaches, but they don’t know what — if anything — will stop AI-powered attacks yet.

— Marcus LaFerrera, Director of SURGe, Splunk





Human beings are the common denominator

How are bad actors getting in? Despite the rise in automation and generative AI, humans are still the weak link. Respondents name misconfigured systems as both the most common threat vector (38%) and the most concerning threat vector (35%).

This alignment between concern and experience suggests security teams know misconfiguration is a problem (kudos to monitoring!) but cannot manage it effectively. More complex systems and scarce security talent may exacerbate the issue and make eliminating misconfigurations altogether seem like a game of whac-a-mole.

Top threat vectors

38%
Misconfigured systems

31%
Vulnerabilities in internally developed apps

30%
Zero-day vulnerabilities

29%
Known software vulnerabilities

28%
Lateral movement

Financially-motivated attacks persist

When it comes to data breaches, ransomware, and extortion — the trio of financially motivated attacks — the bogeyman is real. The number of respondents who had their data and systems held hostage rose from 35% in 2022 to 42% in 2024. And cyber extortion, a ransomware tactic that involves stealing and threatening to release company data publicly, was more common than ransomware itself. Forty-eight percent of respondents say they experienced cyber extortion, compared to 45% who were ransomware victims.

The popularity of cyber extortion may be attributed to the success of 2021's Colonial Pipeline incident, and more recently, the MOVEit attacks in which the Russian-based ransomware group Clop anticipated earnings of $75-100 million from extortion.

As organizations realize the importance of testing backups, cybercriminals may be moving away from encryption and toward data exfiltration and extortion — techniques that involve less work, yield higher payouts, and don't rely on failed backups.

Geopolitics inflame cyber woes

2024 has been afflicted by global unrest. These rising geopolitical tensions have cyber implications that affect even seemingly apolitical organizations. A 2023 hacktivist attack on a Pennsylvania-based water treatment plant underscores that no one is completely safe from nation-state adversaries and terrorist groups.

Eighty-six percent of respondents say the current geopolitical climate is contributing to their organization being targeted more. Technology companies in particular agree strongly with this sentiment (42%) compared to 29% of respondents overall. High-profile breaches with geopolitical ties like SolarWinds remind technology companies, particularly IT services providers, that they can be a bridge for politically motivated actors to reach a range of targets.

Interestingly, only 17% of public sector respondents strongly agree that rising geopolitical tensions make them more of a target, perhaps because government organizations have been — and likely always will be — a target for geopolitical attacks.

"Hacktivism isn't always sophisticated," says Audra Streetman, security strategist at Splunk SURGe. "Politically motivated attackers often use older vulnerabilities, default passwords, and other low-hanging fruit to target organizations, so a commitment to cyber hygiene is more important than ever."

Growing geopolitical tensions will continue to increase risks, even to organizations that are seemingly apolitical. A byproduct of our global supply chain is the inherited risk with every digital link.

— Mick Baccio, Global Security Advisor, Splunk

The mounting pressure of compliance

For security professionals, regulatory compliance is up there with death and taxes: they can count on it. In fact, 62% say they've already been impacted by changing compliance mandates that require disclosure of material breaches.

Security professionals are keenly aware that the regulatory environment will trigger changes to their work in intended and perhaps unintended ways. For example, 87% agree that one year from now they will handle compliance very differently. And while compliance and cybersecurity aren't contradictory by any means, the unintended consequences could include sacrificing one program for another. Eighty-six percent say they'll shift budgets to prioritize compliance regulations over security best practices.

The responses echo our October 2023 CISO Report, in which 84% of CISO respondents were concerned about personal liability for cybersecurity incidents. In the same study, 84% of CISOs said their boards or governing bodies equated strong security with regulatory compliance and not with traditional security success metrics.

It's not hard to see why. New rules in the U.S. require organizations regulated by the Securities and Exchange Commission (SEC) to disclose and describe all "material" cybersecurity incidents, and to share information on their risk management programs annually. Failing to comply could result in steep financial penalties, legal prosecution, and even jail time for executives. In the European Union, the NIS2 Directive requires organizations to establish appropriate teams to respond to incidents and information systems to exchange information. Leaders can be held personally liable for infringements.

Security professionals are caught between a metaphorical rock and a hard place. Underestimate the damage, and they can face fraud allegations and possible jail time. Overestimate, and their assumptions can cause stock prices to nosedive and breed general distrust with the board.

This poses somewhat of a moral quandary: Do you underreport a breach and hope it flies under the radar? Or overreport an incident to cover all your bases — and yourself — in the process, knowing your company share price might take a hit?

Regulation is now an undeniable mainstay of security strategy. Simulation exercises such as tabletops can help companies uncover gaps, while also proving to regulators they are invested in continuous improvement — before they become the next headline.

The consequences of new regulations to report material breaches

63%

expect that organizations will overreport breaches as material to avoid penalties.

61%

predict that valuations of publicly traded organizations will decline as a result of reporting material breaches.

26%

believe both things will happen.

Security, legal, and compliance teams join forces

Once upon a time, compliance was largely a transactional function. Compliance teams operated in silos, often without communicating with or even fully understanding the role of the security teams, and vice versa.

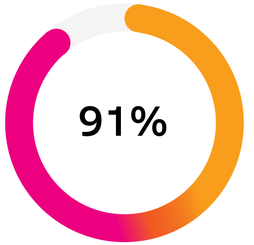
The dearth of regulations puts those days in the rearview as non-compliance carries more serious consequences. In October 2023, the SEC charged SolarWinds' former CISO with fraud and internal control failures that led to the devastating 2020 cyberattack, alleging that he misled shareholders about the company's cybersecurity practices. Communication between the board, legal, compliance, and security teams is non-negotiable, so learning to play nice together is a must.

Organizations and their boards will have to think long and hard about who is most liable when — not if — a breach occurs. That likely means the CISO. But it also could include the CTO, CIO, or even the cyber expert on the board, who could be targeted for a derivative suit or suffer additional scrutiny.

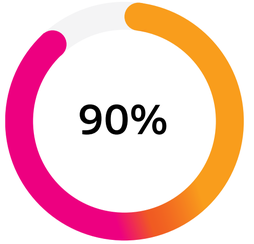
These developments are not lost on security professionals, with the majority of respondents ramping up security practices and facilitating alignment among legal and compliance teams.

Getting everyone on the same page will pay dividends. Aligning priorities, roles, and responsibilities makes your security posture more effective, while empowering legal and compliance teams to become more self-sufficient.

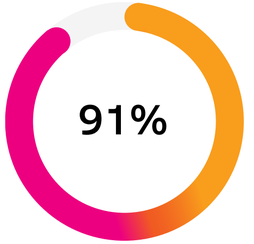
How security and compliance teams are working together



are ramping up **security** training for legal and compliance teams



are ramping up **legal and compliance** training for security teams



say everyone on their security team makes compliance a part of their jobs

Compliance gets personal

The SolarWinds' indictment was a watershed moment — the first time the SEC ever charged a CISO in relation to a cybersecurity incident. This unprecedented action marked a turning point in how the world views cybersecurity, and it will have lasting implications for security leaders and their teams. Cyber risk is now unequivocally synonymous with business risk.

The SEC is holding executives and other stakeholders accountable, and they're not holding back. Along with a spate of new, fully-enforced global mandates, security teams must also report incidents more quickly. The E.U.'s NIS2 allows 24 to 72 hours, while the SEC provides slightly more breathing room with up to four business days. Still, the window is shrinking — a development that will likely be a call to arms for the most seasoned professionals.

More accountability for incidents may lead to better security practices, but it may also have a chilling effect on the profession. How many would be willing to go to jail for making a mistake on the job?

The fear is probably overblown, but these outliers represent a real deterrent. At a time when cyber teams grapple with talent shortages, the fear of compliance penalties is one more reason to consider a different career.

Compliance pressure creates career doubt

76% agree that the risk of personal liability is making cybersecurity a less attractive field.

70% say they've considered leaving the industry altogether due to job stress.

Forging ahead

In 2024, cybersecurity is guided by a medley of global dynamics, including new compliance requirements and geopolitical tensions, but there are also reasons to be hopeful. Being bold and bullish on AI will bode well for defenders — especially if organizations can mitigate the risks and maintain control over how their employees use AI tools.

Another reason for optimism moving forward is that businesses are investing more in cybersecurity. Nearly every organization surveyed (96%) says they will increase their spending on cybersecurity in the next one to two years.

A bit of parting advice

With so much change and evolving technology, it can be difficult for organizations to determine where to focus their efforts. Splunk experts shared their advice with this year's data in mind.

Embrace generative AI throughout the business.

Widespread adoption is already occurring across the business (93%) and within security teams (91%). Organizations that resist generative AI may get left behind. Attempting to ban it altogether will close the door to innovation while simultaneously opening one for shadow AI.

Craft thoughtful generative AI policies without sacrificing innovation.

Rushing to adopt generative AI without considering the risks and implications is a mistake. Create a policy around generative AI and develop a plan for business and security use cases to pull ahead of the 34% of organizations without a codified policy. Determine which generative AI risks are most concerning — for 49% of respondents, it's data leakage — and build policies that address them specifically.

Emphasize collaboration among teams and consolidation among tools.

Digitally resilient organizations are breaking down silos in software engineering, engineering operations, and most importantly, IT. Seventy-six percent of leading organizations increased collaboration with IT operations this year to improve digital resilience. Another way to reduce friction is tool consolidation, which can prevent dashboard overload and help teams focus on meaningful threats. Forty-three percent of respondents report that they pivot between too many disparate security tools and management consoles.

Get in lockstep with legal and compliance teams.

This year ushers in a new era of compliance for security leaders, who should work closely with legal and compliance teams for maximum alignment. Ninety-one percent say security teams already make compliance part of their jobs. Organizations can lean on simulation exercises such as tabletops to help uncover security and compliance gaps, while also proving to regulators they are invested in continuous improvement.

Highest cybersecurity priorities over the next two years

1. Provide security operations training for cybersecurity and IT operations staff

2. Purchase security operations tools designed to help automate/ orchestrate SecOps processes

3. Actively develop and build an integrated software architecture for security analytics and operations tools

4. Research, test and/or deploy cloud-based security analytics/ operations technologies in addition to existing tools

5. Increase the use of outsourced resources for security operations (e.g. third-party managed security service providers)

Learn how to effectively advocate for resources.

Cybersecurity maturity comes from the top down — 95% of leading organizations say they have the resources and authority to solve problems. CISOs in particular should be able to discuss and translate security risk from a business perspective to earn a seat at the table with executives. Communicate to the board in ways that highlight the business value of cybersecurity investments. This includes reporting the impact of cybersecurity incidents to the business, or articulating compliance requirements with severe legal or financial consequences.

Think outside the box to close talent gaps.

Data shows that leading organizations lean on less traditional hiring and training methods. Fifty-three percent of leaders are using AI and machine learning to fill hiring gaps, compared to only 28% of developing organizations. These creative hiring and training strategies — like programs that allow people in non-security roles to shadow in the SOC — can help close the skills gap and infuse much-needed diversity into a security team.

Don't forget the basics.

While cybersecurity threats are becoming more sophisticated, adversaries still rely on tried-and-true techniques, and misconfigured systems remain a top vector in 2024. Implementing basic controls is where organizations can get the greatest return on investment, making it easier to keep up with requirements in the long term. Although 76% say completing an IT asset inventory takes too much time, it's time well spent. An up-to-date view of your assets and their dependencies can prevent dangerous blindspots.

Tune into global dynamics that affect the cybersecurity landscape.

Cybersecurity doesn't exist in a vacuum. Politics, global conflict, and tightening compliance mandates have direct and indirect impacts on the threat landscape. Eighty-six percent of respondents say that the current geopolitical climate makes them a bigger attack target, and 62% say they've been impacted by changing compliance mandates. When organizations are aware of these changing dynamics, they can more readily navigate the associated obstacles.

Learn how to catalyze your digital resilience with Splunk

Perspectives by Splunk — by leaders, for leaders

Looking for more executive insights on cybersecurity trends in 2024 and beyond? Learn how leaders are tackling today's most pressing security challenges including AI, emerging threats, and the changing compliance landscape.

Learn more

Build digital resilience

Today's security teams are under constant pressure from cyber threats, ever-changing regulations, and rising geopolitical tensions. See how your organization cannot just recover but thrive amidst disruptions.

Get started

Industry highlights

We identified key insights across six select industries worldwide.

Manufacturing

Manufacturers are more focused on cloud security than other industries, with 40% citing it as a top initiative. Zero-day vulnerabilities are also top-of-mind for manufacturers, with 39% naming them as a top concern — possibly due to the inherent difficulty of patching critical infrastructure.

Respondents in the manufacturing sector are also struggling to keep up with the changing threat landscape:

- **51% of manufacturing security professionals report that security requirements have become harder over the last 12 months.**
- **Manufacturing respondents are more likely to say that increases in threat sophistication are bogging them down (50% versus 38% across all industries).**

These setbacks could indicate a lack of investment from the business, as manufacturers are much less likely (36%) to expect a significant rise in cybersecurity spending, versus 48% across industries.

However, manufacturing respondents appear to have an edge over other industries when it comes to hiring security talent:

- **27% say that stress on the job made them or others consider leaving cybersecurity multiple times, well below the 36% across industries.**
- **27% say a critical project was delayed multiple times due to the skills gap, compared to 37% across industries.**

Since manufacturing organizations struggle to secure additional cybersecurity budget, security executives should demonstrate the financial impact of incidents and focus on key risks to gain C-suite and board level buy-in.

Financial services

Compared to other industries, financial services respondents are more optimistic about their ability to keep up with cybersecurity requirements. Fifty percent say it was easier to keep up this year, versus 41% across industries.

More collaboration across IT and engineering may be driving that optimism. Security teams at financial institutions say they're apt to work more closely with engineering operations on digital resilience initiatives (64%, versus 46% across industries).

Financial services respondents are also more hopeful about generative AI's role in alleviating the talent gap. They agree that generative AI would help:

- **Organizations source and onboard talent faster (63% versus 58% across industries)**
- **Enable seasoned security professionals to be more productive (71% versus 65% across industries)**

However, they also recognize the risk of generative AI. Seventy-six percent of financial services respondents say they don't have enough education to fully understand the implications of generative AI, versus 65% across industries. Accordingly, 39% list AI-powered attacks as a top concern.

Unsurprisingly, security professionals at financial services firms say that compliance has become such a large job that it necessitates a separate team (43% versus 39% across other industries). Cyber extortion is also more common at financial institutions (54% versus 48% across industries).

Methodology

Researchers surveyed 1,650 security executives in December 2023 and January 2024. Respondents were in Australia, France, Germany, India, Japan, New Zealand, Singapore, United Kingdom, and United States. They also represented 16 industries: Aerospace and defense, business services, consumer packaged goods, education, financial services, government (federal/national, state and local), healthcare, life sciences, manufacturing, technology, media, oil/gas, retail/wholesale, telecom, transportation/logistics, and utilities.

Communications and media

Communications and media respondents are most likely (57%) to identify their cybersecurity programs as “extremely advanced” (versus 47% across industries). Yet, this industry is also the most likely to say they didn’t have the resources or authority to address challenges (16%, compared to 8% across industries).

Communications and media stood out as the industry struggling most with the following:

- **82% say it’s difficult to keep up with security hygiene and posture management due to frequent changes and growth in the attack surface, compared to 71% across industries.**
- **62% say their SOC pivots between too many disparate security tools and management consoles, compared to 43% across industries.**
- **47% say themselves or others have considered leaving cybersecurity multiple times due to the inability to hire or retain staff with the right skills, compared to 36% across industries.**
- **74% say they are impacted by changing compliance mandates, compared to 62% across industries.**

These difficulties may have led to communications and media organizations encountering several types of incidents with increased frequency, including insider attacks (55% versus 42% across industries), digital asset fraud (59% versus 43% across industries), software supply chain attacks (57% versus 43% across industries), and targeted attacks (54% versus 44% across industries) than industry counterparts. Misconfigured systems are more problematic for the communications and media sector, with 44% of industry respondents citing it as a root cause in the past two years.

Communications and media organizations should focus on achieving executive buy-in to boost the maturity of their cybersecurity programs even further. When cybersecurity teams have the resources and authority to solve problems, they’ll likely see better outcomes around threat prevention.

Technology

Respondents from technology companies indicated that they struggle with complex environments. As a result:

- **Tech companies are more likely to cite security stack complexity as a reason why they find it difficult to keep up with cybersecurity requirements (36% of tech companies, versus 26% across industries).**
- **Tech companies are more apt to say they have too many fragmented security tools and a lack of human resources to accomplish manual work (37% of tech companies, versus 26% across industries).**
- **Known software vulnerabilities (34%) and vulnerabilities in internal applications (34%) are more frequently the root cause of incidents in the technology sector.**

The changing regulatory environment is another barrier — 41% of respondents from tech companies say this contributes to their difficulties with keeping up, compared to 28% across industries.

Geopolitical conflict also affects technology companies more acutely. They strongly agree (42%) that international conflicts were contributing to their organization being targeted more by adversaries, compared to 29% across industries.

On a positive note, technology companies are much more likely (63%) to report a significant rise in anticipated security spending, compared to 48% across industries.

For tech organizations struggling with complexity, the name of the game should be simplification. Tool consolidation could be an important initiative for this sector, which appears to suffer from shiny object syndrome.

Healthcare

Healthcare organizations have the most problematic MTTDs out of any industry, with 31% stating they measure MTTD in months versus only 19% of organizations across all industries. They also deal with ransomware attacks more than other industries, with 56% reporting a ransomware attack in the past two years, compared to 45% in aggregate. The healthcare sector is also more likely than other industries to cite overly permissive accounts (33%) as the most frequent root cause of incidents.

Healthcare respondents report greater hiring-related issues than other industries:

- **44% say team members have been asked to lead projects without requisite experience, compared to 39% across industries.**
- **44% say a critical projects or initiatives have been delayed because of hiring problems, compared to 37% across industries.**

Most healthcare respondents say they have been impacted by changing compliance mandates (67%). They are also more likely to strongly agree — 44%, the highest of any industry — that these changes are causing more senior-level individuals to be on call 24/7, compared to 35% across industries.

Respondents in healthcare are the least optimistic about generative AI. Fifty-two percent say they expect adversaries to benefit from it more, compared to 45% across industries. They're also less interested in using AI to combat that competitive edge they expect adversaries to gain — only 37% of healthcare organizations list AI as a priority, compared to 44% across industries.

Considering the healthcare sector's hurdles with threat detection, ransomware prevention, and hiring, going back to the basics of cybersecurity hygiene could be a successful path forward that enables these organizations to do more with less.

Public Sector

Data from the public sector highlights a quest for knowledge. Public sector respondents place more focus on security awareness training (24%, compared to 17% across industries). Accordingly, they list their top challenge as a lack of cybersecurity knowledge and commitment from executives (28%, compared to 20% across industries).

While last year's public sector respondents were hesitant about traditional AI's ability to lighten the security team's load, this year the public sector show optimism for generative AI:

- **Respondents from the public sector are most likely to see opportunities for generative AI to have a "game-changing" impact to the business (55% versus 47% across industries) and anticipate the most benefit to the security team (55% versus 46% across industries).**
- **Security teams in the public sector are leading for adopting acceptable use policies for AI (77% versus 66% across industries).**
- **Public sector respondents are also more likely to envision security use cases for generative AI, including threat detection (46%, versus 35% across industries), penetration testing (42% versus 29% across industries), and security team training (44% versus 34% across industries).**

Public sector organizations also appear to have greater SecOps automation aspirations than their peers, including automating SSL certificate management (43% versus 31% across industries), the orchestration of actions across security controls (53% versus 38%), and alert enrichment (47% versus 32%).

For cybersecurity basics, the public sector more frequently cites misconfigurations as the top vector for threats, with 42% saying they are most often the root cause. Public sector respondents are also most likely to be concerned about lateral movement, with 39% listing it as their primary concern.

Lack of knowledge and excitement for AI can be a dangerous combination, so public sector organizations should take a measured approach to AI adoption and educate themselves on the risks before jumping on the generative AI bandwagon.

Country highlights

Snapshots from across eight countries across the globe.

Australia

Data from Australian organizations paints a harrowing picture of the country's cybersecurity landscape. Organizations in Australia are more likely to strongly agree that geopolitical stress exacerbates cyberattacks (44%, compared to 29% globally). Fifty-six percent of Australian respondents experienced nation-state attacks compared to 39% globally.

In fact, Australian respondents experience a higher-than-average rate of every attack type we asked about, including but not limited to data breaches (63%, versus 52% globally); regulatory compliance violations (53% versus 43% globally); insider attacks (55% versus 42% globally) and business email compromise (59% versus 49% globally).

Perhaps the higher frequency of cyberattacks can be attributed to Australian respondents' visibility-related issues. Seventy-two percent say they pivot too much between disparate security tools (compared to 43% globally), and 35% cite issues with visibility across the attack surface (compared to 20% globally). It's no surprise then that Australia also cites problematic detection, with 50% saying typical MTTD takes months compared to 19% globally.

Respondents in Australia also deal with staffing-related challenges more than other countries:

- **52% say team members were asked to lead projects multiple times without requisite experience, compared to 39% globally.**
- **50% say stress on the job has made themselves or others consider leaving cybersecurity multiple times, compared to 36% globally.**
- **52% say critical security projects or initiatives have been delayed multiple times, compared to 37% globally.**

Australia is a leader in both generative AI adoption and policy creation, with 69% reporting that employees use public generative AI tools to do their jobs compared to 54% globally, and 73% reporting they had established security policies for generative AI use, compared to 66% globally.

France

Respondents in France are more apt to say that they've struggled to keep up with cybersecurity requirements within the past year (56%, compared to 46% globally). Unsurprisingly, they also appear to have lower cybersecurity maturity, with only 37% describing their programs as "extremely advanced" compared to 47% globally.

When asked why cybersecurity requirements are harder to keep up with, 33% of respondents in France report the number of tools and vendors within their security stacks have become too excessive, compared to 26% globally. A complicated tech stack often results in misconfigurations, and 40% of French respondents cite this as a concern.

France trails behind other countries for extensively adopting cybersecurity tools with AI and machine learning capabilities (27%, compared to 37% globally). And while organizations in France are more apt to say they are focused on AI — 56% in France, versus 44% globally — they are also less likely to have established security policies for generative AI usage at 52%, compared to 66% globally.

On the bright side, French respondents say they've experienced fewer incidents than the global average across the following attack types in the past two years:

- **44% experienced a data breach**
- **37% violated regulatory compliance**
- **37% experienced a DDoS attack**
- **40% were victims of a ransomware attack**

Germany

Data from German respondents indicates a more acute awareness of generative AI's risks compared to their peers:

- **41% of German respondents strongly agree that generative AI expands their attack surface to a concerning degree, compared to 31% globally.**
- **38% of German respondents strongly agree that generative AI makes their existing attack surface more vulnerable, compared to 29% globally.**

Organizations in Germany appear to have a hard time with staffing in particular. Thirty-three percent cite an inability to hire enough skilled security staff as the reason why cybersecurity requirements were harder to keep up with in the past year, compared to 25% globally.

In the SOC, 53% of German respondents say there is too much pivoting between disparate security tools (compared to 43% globally). Perhaps many of these disparate tools are cloud-based, because Germany cites attacks on cloud infrastructure as one of the most concerning types of incidents (23%).

These hiring and tooling constraints may have contributed to slightly longer MTTDs than their peers; 40% of German respondents measure their MTTD in weeks, compared to 35% globally.

Despite these setbacks, Germany stands out from other countries in its ability to salvage data and systems during a ransomware attack. Fifty-eight percent have been successful with this over the past two years — the highest percentage of any country we surveyed — compared to 44% globally.

Respondents in Germany are also more likely to agree (94%) that today's geopolitical climate is contributing to being targeted more by adversaries, compared to 86% globally.

India

Compared to other countries, India has the highest percentage of organizations (66%) that rate their security programs as "extremely advanced," compared to 47% globally. They also have higher rates of increased collaboration across internal teams — 58% with software engineering, 52% with engineering operations, and 78% with IT.

Respondents in India are also particularly focused on cloud security, with 48% citing it as a top initiative compared to 35% globally. Unsurprisingly, India is the most likely to cite attacks on cloud-based infrastructure as a top concern (25%) compared to other countries. Most top of mind for India, however, is cyber extortion, with 37% saying it was a top concern compared to 24% globally.

Compliance mandates requiring the disclosure of material breaches appear to heavily impact India, with 81% of Indian respondents reporting they've been impacted by these changes, compared to 62% globally. Accordingly, 54% of Indian respondents strongly believe that everyone on the security team should make compliance a part of their jobs, compared to 42% globally.

Respondents in India are the most optimistic about how generative AI will tip the scales — 51% expect defenders to gain a bigger advantage, versus 43% globally. They also recognize potential use cases of generative AI more often, including:

- **Threat detection and prioritization (52% versus 35% globally)**
- **Training use cases (50% versus 34% globally)**
- **Threat intelligence analysis (55% versus 39% globally)**
- **Creating detection rules (44% versus 30% globally)**
- **Summarizing security data (54% versus 34% globally)**

Similarly, respondents in India appear to be ahead of the curve in establishing generative AI policies. Eighty-two percent have established generative AI security policies for end users, compared to 66% globally.

Japan

Compared to their peers, Japanese respondents are more likely to say that cybersecurity requirements are getting harder to keep up with (54% versus 46% globally). Only 27% of Japanese respondents say security is getting easier, compared to 41% globally. Out of those respondents, only 5% say that it is getting much easier, compared to the global 17% average.

Why are Japanese organizations having trouble keeping up? They cite the following pitfalls more than their peers:

- **36% say their security stacks have become too convoluted, compared to 26% globally.**
- **29% are unable to effectively analyze all security-relevant data, compared to 21% globally.**
- **27% have limited visibility into their attack surface, compared to 20% globally.**

Another possibility could be a lack of budget. Japan is less likely (38%) to report a significant rise in anticipated cybersecurity spending.

Japanese respondents are less optimistic about the benefits of generative AI to SOC practitioners, with only 37% strongly agreeing that it would help develop their skills compared to 43% globally.

Out of the countries surveyed, Japan is most focused on ransomware protection, with 21% calling it a top initiative. That enhanced focus could possibly be paying off in the form of faster MTTD — 43% of respondents in Japan report an MTTD measured in days, compared to the 33% global average.

Singapore

Data from Singaporean respondents indicates that their organizations' cybersecurity programs are less mature than other countries.

- **Singapore has the highest percentage of respondents who identified their cybersecurity programs as "developing" (14%, compared to 7% globally).**
- **They are less likely to say they have the authority and resources to address cybersecurity challenges (only 77%, compared to 91% in aggregate).**
- **They are the least likely (28%) to report a significant rise in anticipated cybersecurity spending.**
- **26% of Singaporean respondents do not know their average MTTR, and 25% did not conduct post-incident analyses to calculate MTTD.**

As such, Singapore respondents are less likely to recognize the business impact of digital resilience. Only 23% strongly agree that digital resilience could improve customer retention, compared to 33% globally. Twenty-five percent strongly agree that digital resilience could prevent significant disruptions to operations, compared to 35% globally.

Organizations from Singapore appear to focus less on collaboration among compliance, security, and legal teams. Only 29% strongly agree with ramping up their compliance team's security training, compared to 42% globally. Only 29% strongly agree with the concept of incorporating compliance into the security team's workflow, compared to 42% globally.

Our data indicates a correlation between program maturity and AI prioritization, so it's not surprising that only 36% of Singapore respondents are focused on AI initiatives, compared to 44% globally. They are also less likely (48%) to have established generative AI policies. Compared to other countries, Singapore is also the least worried about AI-powered attacks, with only 23% citing it as a top concern.

United Kingdom

Data from the United Kingdom paints a generally positive picture compared to their global counterparts.

UK organizations are increasing collaboration to achieve resilience more often:

- **66% say their security and software development teams are collaborating more (versus 54% globally).**
- **56% say their security and engineering operations teams are collaborating more (versus 46% globally).**

UK respondents are also ahead of other countries in terms of their automation capabilities. In particular, they have high rates of automation in regards to general process automation (40%) and vulnerability management (35%).

Skills shortages do not affect UK organizations as much as other countries. Thirty percent of UK respondents say that team members have been asked to lead projects multiple times without requisite experience, compared to 39% globally. Only 23% say critical security projects have failed multiple times due to skills shortages, compared to 33% globally.

These successes may be why UK organizations experience lower-than-average rates of the following attack types compared to their peers:

- **Regulatory violations (35% versus 43% globally)**
- **Insider attacks (37% versus 42% globally)**
- **Business email compromise (38% versus 49% globally)**
- **DDoS attack (38% versus 46% globally)**
- **Account takeover attack (34% versus 42% globally)**
- **Ransomware attack (37% versus 45% globally)**
- **Software supply chain attack (35% versus 43% globally)**

United States

Data from U.S. respondents rarely deviates from the global averages. However, one area where U.S. respondents are ahead of the mean is the generative AI usage policy — 72% have established one, compared to 66% globally. Conversely, U.S. respondents are the least concerned group to cite AI misuse as a root cause at only 18%.

U.S. respondents also struggle with longer MTTDs. Forty percent measure their MTTDs in weeks compared to 35% globally, and 22% say a typical MTTD is months compared to 19% globally. But this appears to be a work in progress, as 30% mention they improved MTTD with process automation, compared to 25% globally.

For future priorities, U.S. respondents are slightly more inclined to address the cybersecurity talent shortage. Twenty-one percent say they want to hire more security operations personnel (compared to 18% globally) and 25% plan to provide security operations training (compared to 23% globally).

About Splunk

Splunk helps make organizations more digitally resilient. Leading organizations use our unified security and observability platform to keep their digital systems secure and reliable. Organizations trust Splunk to prevent infrastructure, application and security incidents from becoming major issues, recover faster from shocks to digital systems and adapt quickly to new opportunities.

Keep the conversation going with Splunk.

splunk>

24-492903-Splunk-State-of-Security-111