The State of **Security 2023**

Global research: How leading organizations engage the entire business to build resilience

splunk>

Security 2023: Quick Reaction Force

Cyberattacks continue to grow in quantity and sophistication at the same time that organizations' systems become increasingly complex. Security teams, as always, feel the stress. But a surprising outcome of our 2023 State of Security research is that the number of respondents who say they just can't keep up has shrunk.

Don't plan a victory parade just yet; 53% of respondents worldwide tell us that keeping up with security requirements is harder than it was two years ago, and that's still a lot. But the number in 2022 was 66%. Our own security experts, able to spot the dark lining in every silver cloud, note that 2022 didn't have as many novel developments to throw security teams into disarray; no SolarWinds, no Log4J. "No iceberg for your organizational Titanic," to quote them directly.

Whether this data represents incremental improvement or a one-time windfall, organizations should press any advantage. Which won't be easy: Most security teams tell us they're too stuck in reactive mode to be effectively proactive.

Drilling down, we asked the slim majority who say their job has gotten harder to tell us what's making it harder. This subset's top challenges:

- The increasing sophistication of threats (according to 38%, ranking it No. 1 for the third straight year)
- Security stack complexity (according to 30%)
- IaaS and SaaS driving challenges in risk monitoring and management (29% and 28%, respectively)
- Workload demands trapping teams in "react mode" (28%)

That last bullet is further reflected in several trailing responses. Respondents tell us that they are overwhelmed by the number of attacks (24%) and false positives (25%). Another 25% each say they struggle to hire or retain enough skilled staffers.

There are global variations in terms of struggle. Organizations in the Asia-Pacific region are five to seven percentage points more likely than the global average to say that it's hard to monitor SaaS applications and to effectively analyze all security data. European respondents are less likely to voice that complaint, while North American orgs hewed to the worldwide average.

Methodology

Researchers surveyed 1,520 security and IT leaders who spend half or more of their time on security issues.

10 Countries

Equally split across North America, Western Europe, and Asia-Pacific: Australia, Canada, France, Germany, India, Japan, New Zealand, Singapore, United Kingdom, United States

15 Industries

Aerospace and defense, consumer packaged goods, education, energy, financial services (banking, securities, insurance), government (federal/national, state and local), healthcare, life sciences, manufacturing, media, retail/wholesale, technology, telecom, transportation/ logistics, utilities

We found that across industries and geography, security leaders and their peers throughout the organization are increasingly collaborating to improve resilience. Classic cybersecurity is concerned with proactive prevention of incidents, while resilience is reactive: It's about what you do once an incident occurs.

But preparing your organization to most efficiently recover from a crisis is very much a proactive undertaking. Risk assessment, incident response planning and key investments in technology and training, and more — these require strategic thinking beyond the strict confines of cybersecurity.

Our respondents tell us that security teams are finding more success at partnering across the organization, being seen as valuable partners — enablers rather than the Dept. of No-Can-Do. As we'll cover below, 79% of line-of-business stakeholders see the security team as valued partners, rewarding those teams with a seat at the collaborative table and better funding.

And the business leaders to set the budget for security are increasingly looking at metrics that measure resilience, starting with mean time to recover. In fact, MTTR tops the list.

We see tremendous challenges

Some of the most noteworthy stats you'll read in this year's report include:

- **64% of SOC teams struggle to pivot** from one security tool to the next, with little integration to make it easier.
- **88% of respondents report talent challenges**, whether key, high-level skills or just hiring enough bodies.
- Bad guys get in. And when they do, their average **dwell time is 2.24 months**, or about nine long weeks.

We also see efforts to address the countless challenges. High points include:

- **95% of organizations have increased their focus** on third-party risk assessment.
- **81% of orgs are converging** aspects of security and IT operations.
- **95% of security budgets will increase** over the next two years — 56% of them "significantly."

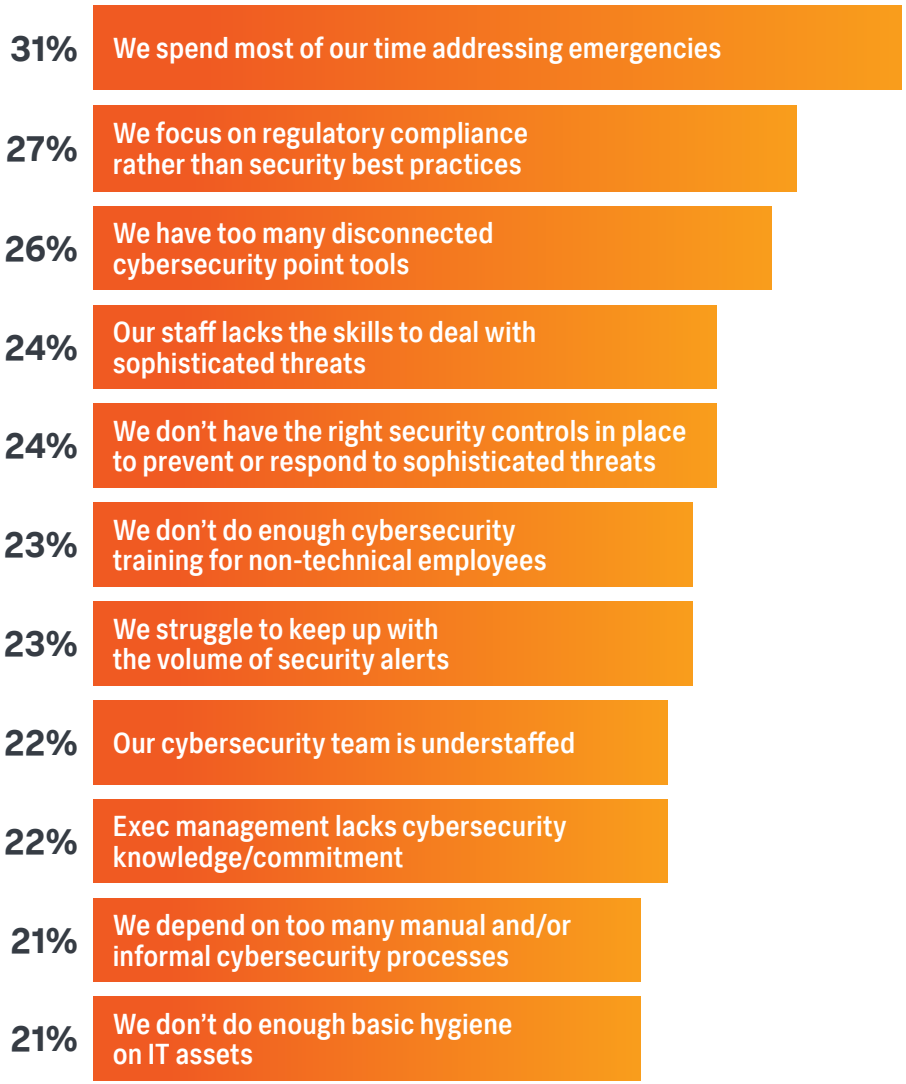
Across the board, whether they say that they're overwhelmed or not, respondents identified a diffuse range of challenges. While no one type of crisis dominated, the generalized problem of spending too much time tackling emergencies pulled into a comfortable first place.

There are a number of causes for this perpetual reactive mode and, frankly, not a lot of solutions. Organizations experience cyberattacks by the thousands, so a reactive stance is inevitable. While smart security teams do their best to get ahead of known attack vectors, there are always new techniques that send you scrambling again.

Additionally, compliance just doesn't get easier. The increasing sophistication of technology, of the ways in which data is used, and the methods of attack all mean that regulatory standards will (eventually) rise as well.

Top Cybersecurity Challenges

Respondents chose their top three internal challenges.



The state of the SOC

As the previous pages indicate, security teams are strained. Today's security operations center has a lot to cover, and not enough people to cover it.

- **64% of SOC teams complain about pivoting among too many disparate security tools and management consoles, with little (if any) integration, inhibiting comprehensive and timely investigations and response.**
- **49% say that they lack enough staff to manually triage, investigate and respond to an increasing volume of security events.**

The result: increased risk resulting from their workload. On average, respondents estimate that 41% of alerts that would be beneficial to investigate are ignored due to a lack of available SOC bandwidth. And of course, the alerts you don't investigate could include a true positive, allowing an attack to succeed. This undermines everything: the actual return on your investment in the expensive tools generating these alerts, the efficiency and morale of your analyst team, and the actual security and resilience of your organization.

As economies tip toward recession, staffing challenges are expected to get even more acute.

55% of respondents expect that hiring and retention would be harder in a recession.

32% think that hiring and retention would get easier.

Impact of the talent crisis

The perennial labor shortage remains a serious problem: 88% of respondents report challenges with cybersecurity staffing/skills, including 53% who say that they can't hire enough staff generally (matching last year's finding) and 59% (up from 58%) who can't find talent with the right particular skills.

Security leaders are turning to managed security service providers in high numbers (42% are increasing their use of MSSPs), allowing teams to both beef up off-hours coverage and offload tier-one issues around the clock. Despite this, the talent struggle has led to a number of issues over the last 12 months:

- **81% of respondents say that members of their staff have been forced to take on responsibilities that they aren't ready for — up from 76% last year.**
- **81% report that critical staff member(s) left the organization for another job due to burnout.**
- **78% of respondents say the resulting increase in their workload has led them to consider looking for a new role — up from 70% a year ago.**
- **77% say one or more projects/initiatives have failed — up from 68%.**

Talent is always in crisis in the cybersecurity space. But these numbers show not just a chronic condition, but an increasingly acute one. Shrugging it off as "It's always like this" would be a crucial mistake.

How SOCs Work

Mitigating talent challenges

Security leaders are taking steps to mitigate the challenges. As noted on the previous page, MSSPs are playing a bigger role: 86% of organizations have relied on service providers to help close skill gaps. In fact, 56% of respondents say the majority of security operations work at their organization is outsourced to a third-party service provider, most often to extend security operations to be more continuous and to gain access to service providers' more advanced tooling. Forty-two percent say they plan to increase those engagements.

Then there's looking for more help within one's org: 86% of organizations have started reskilling individuals outside of the security team to help fill gaps, with 38% planning to offload more security tasks to IT staff in the coming year.

Increased training is the No. 1 choice, besides more hiring, for respondents in every region. The top areas that security teams are under pressure to upskill include cloud operations and architecture (41%) and secure application development (42%).

Additionally, security teams are embracing automation and improving their tooling, and making data a focus (see chart), as a means of making shorthanded teams ever more effective.

Highest-Priority Tactics to Overcome Talent Challenges

(besides hiring)

The top choice for all regions was "more training" (45-47%), though in the Asia-Pacific region, "more investment in commercial security controls" tied for first place (at 47%).

Resilience is the main metric

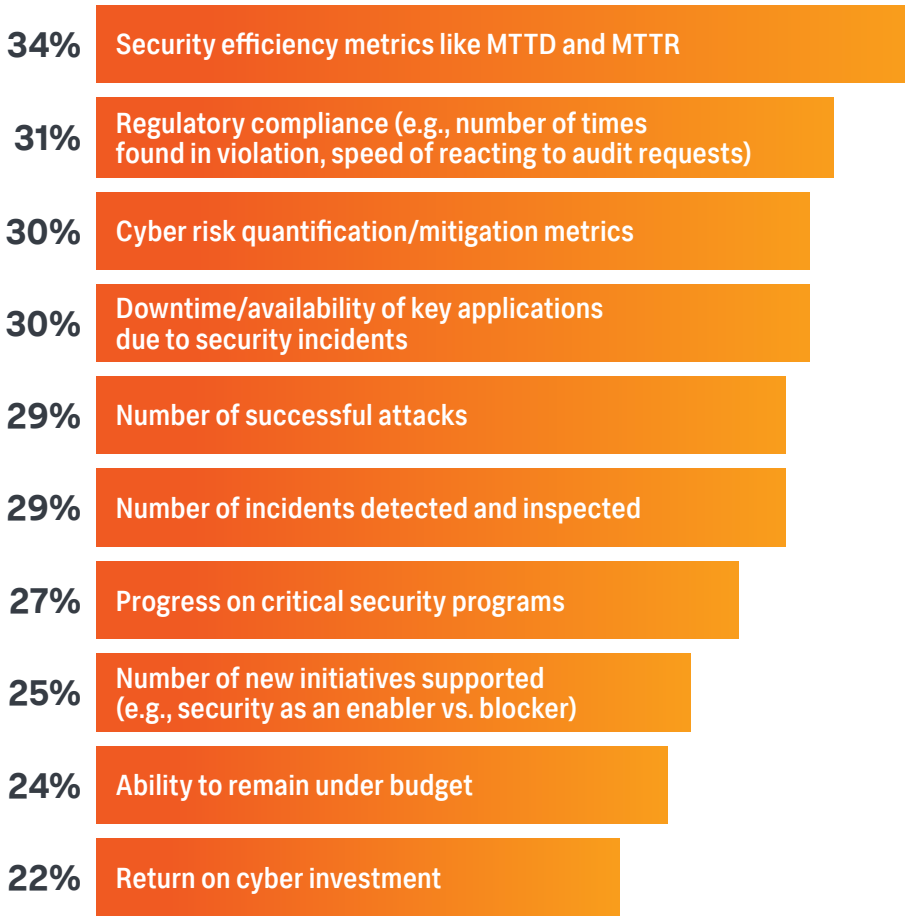
We asked respondents to indicate the top three performance metrics used by business leaders to judge security effectiveness, and saw a significant indication of a resilience mindset. In the chart at right, four of the top six responses (all but compliance and risk mitigation) play directly into resilience strategies, with mean time to detect and recover coming out on top (34%), and downtime (30%) ahead of counting attacks and incidents.

Whereas the quantity or sophistication of attacks you face is outside your control — you don't know who's coming at you next — you can definitely measure your MTTR. And if you accept that service disruptions are inevitable, then how quickly and effectively you deal with them really matters.

"MTTR is easier to measure and improve," notes Splunk Distinguished Security Strategist Ryan Kovar, who leads our SURGe threat advisory team. "You can't necessarily hone your MTTD, because the threats are unknown. SolarWinds was a novel attack, and your time to detect on that was two years. But you can drill for MTTR. And that's where you create resilience."

How Business Leaders Measure Security Success

Top metrics used by business leaders to understand cybersecurity



Security teams have long understood their value to the business and that good security, and strong resilience, is not about saying no to every new initiative. But it has taken time for businesses to understand this mentality and embrace security as an active partner, enabling business success. Our survey this time shows that for most teams, the business side gets it.

Respondents tell us that 79% of line-of-business stakeholders see the security team as either a trusted source of information (49%) or a key enabler of the organization's mission (30%). It's a slim minority that still sees security as a necessary inconvenience (12%) or complete roadblock (8%).

The security team's role as a strategic partner and enabler facilitates the broader collaboration and a holistic focus on resilience, as we'll see. And at the leadership level, respect and a seat at the table produce tangible results. Respondents told us that access to business leadership improves the security team's ability to collaborate with other parts of the business (46%) and results in increased security team funding (42%).

79% of business stakeholders see the security team as a partner, not an obstacle.

Incidents, Alerts and Threat Vectors

Despite new strategies and better cross-organization partnerships, security teams face significant challenges. The bad guys aren't slowing down, either. Globally, our research found more incidents, longer dwell times and business-impacting damage.

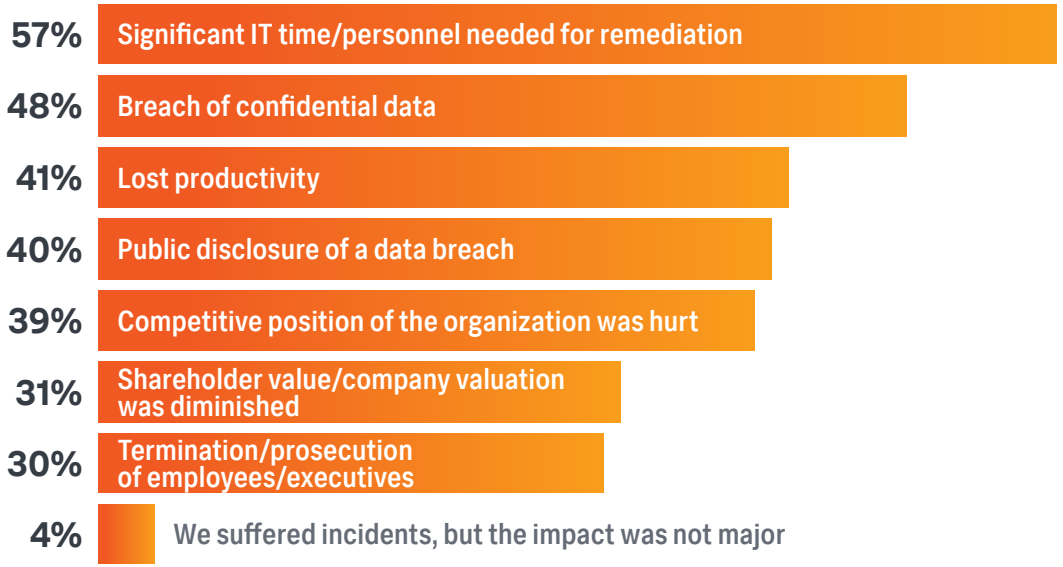
The existential impact

Security incidents are an existential threat. In addition to the considerable time and resources expended to clean up the mess, significant numbers of respondents say incidents had damaged their company's competitive position, hurt the stock price, or created a public embarrassment. Only 4% of respondents say they had suffered incidents but experienced no significant consequences.

In terms of attack types, note that by "supply chain attacks" (which hit 46% of respondents, globally) we mean actual attacks that succeeded using that vector. If we'd measured it to mean "you discovered unexploited vulnerabilities in third-party software and remediated them in time," the number would be higher. By a lot.

Whatever the avenue, once the bad guys get in, they've got time to get comfortable. On average, respondents tell us that it's 2.24 months, or about nine weeks, from the moment a bad actor penetrates their systems until appropriate parties are aware of it. That's a lot of time to steal or break things.

Effects of Incidents Over the Past Two Years



Incidents Experienced in the Past Two Years

Lack of resilience is a dire threat

Security teams understand that they need to improve resilience. Most respondents (62%, up from 54% last year) report that cybersecurity incidents take down business-critical applications at least once a month. The mean number of those outages is about 22 per year (up from 19).

Security teams say they're working to continue to improve those resilience metrics. On average, they say they aim to reduce MTTD by 40% and MTTR by 53%. We did see improvement this year over last year's research: The average mean time to recover (MTTR) for business-critical workloads suffering from unplanned downtime tied to a cybersecurity incident is 15.5 hours (down from 21.4 hours). Still, downtime costs consume 2.7% of annual revenue.

Controlling those costs isn't the only issue. Asked why they're focusing on resilience:

- **83% of respondents agree that their risk of significant business disruption is elevated.**
- **79% think a loss of productivity will put them at risk of being out-innovated.**
- **78% of respondents agree that downtime's effect on digital experience may cost them customers.**

The issue resonates at the highest level. Nearly everyone (91%) says their CISO is actively collaborating more with line-of-business leaders (finance, marketing, operations, etc.) on cyber resilience strategies and investments. But those CISOs have their work cut out for them:

- **Just 31% say they have a formal approach to cyber resilience that has been instituted organization-wide across critical systems.**
- **Only 38% have a resilience strategy in place in pockets of the organization.**
- **31% say they have yet to implement any resilience strategies.**

While **91% of CISOs** are collaborating across the business on resilience, fewer than a third have an organization-wide approach to resilience in place.

Vector by vector

When we asked respondents to review a stressfully long list to pick their three most concerning potential vulnerabilities, the responses are fairly evenly distributed, with no dominant leaders. Two high-profile attack types that deserve a deeper dive are the software supply chain and ransomware, while the ubiquity of public cloud as part of organizations' attack surface merits its own consideration.

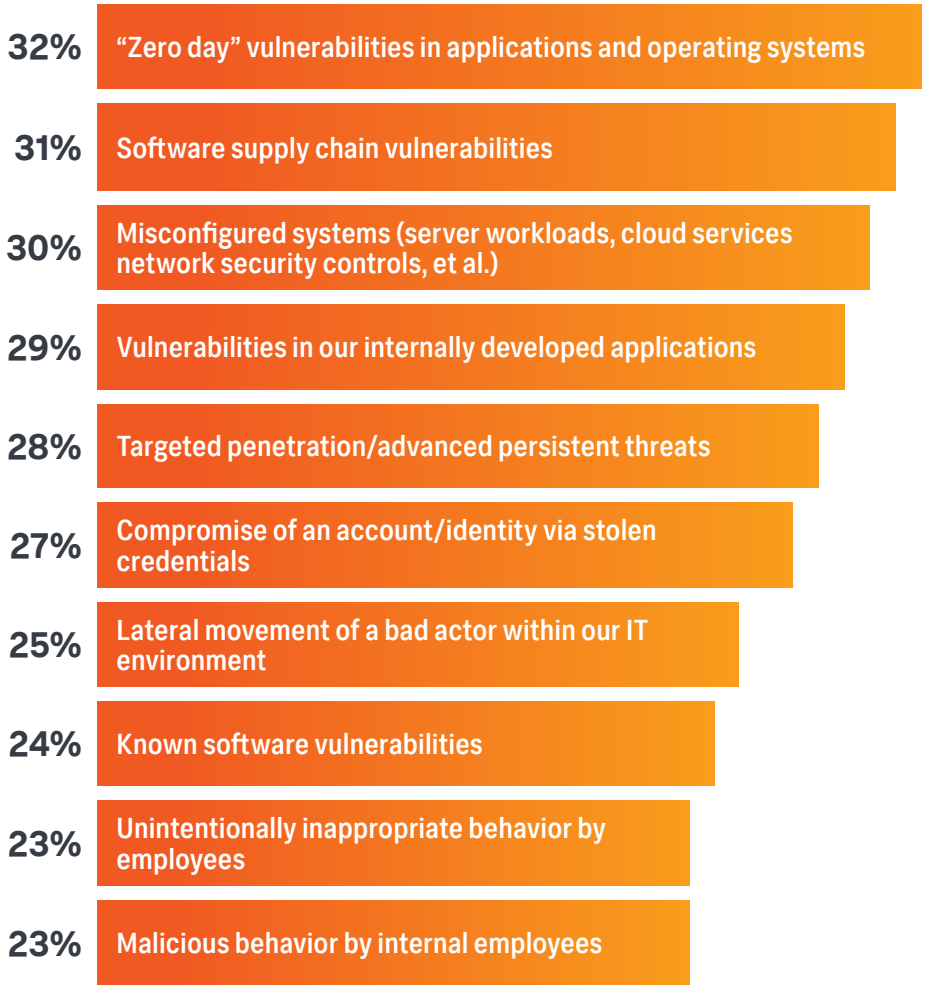
Supply chain. Software supply chain attacks are top-of-mind in the post-SolarWinds (and Log4j, and Kaseya, and ...) era. Fully 95% of organizations have increased their focus on third-party risk assessment activity, up from an already noteworthy 90% a year ago.

Looking into the tactics involved reveals a very diffuse approach to supply chain security. From a list of 17 responses to supply chain threats, the top three answers tied with a 26% adoption rate:

- **Assessing security controls to understand prevention/detection capabilities specific to supply chain attacks**
- **Hardening authentication systems**
- **Increasing security budgets**

The fragmentation of responses — the lack of any widely adopted tactic — suggests a disjointed approach to a problem that only recently entered the spotlight.

Most Concerning Threat Vulnerabilities



Ransomware. Ransomware is like Covid-19. You may still know people who haven't had it yet, but there are fewer of them all the time. Since the 2022 State of Security research, the number of organizations reporting that they had not yet been hit with a ransomware attack dropped from 21% to just 13%. Similarly, while 35% of organizations in 2022 reported having had data/systems held hostage, this year's number rose to 43%.

When orgs get hit, they're likelier than ever to pay up. Last year, 66% of organizations said that they (or their insurer) just paid off the attackers. This year, that number is 75%. And ransoms continue to rise: Last year, only 32% of respondents said their largest ransom had been $250,000 or more. This year, it's 50%. On average, respondents say that the largest ransom they'd paid attackers was $430,978, up 24% (from $346,897) since last year.

(This surprised us, because other research in the past year has suggested ransoms are going down. Rechecking our numbers, we find that the most senior respondents, who should really know, are even more likely (79%) to say that they've paid more and more often.)

As with supply chain risks, there's a wide spread in adoption of tactics to combat ransomware. There's slightly more commonality in the approaches, though, with two tactics being adopted/accelerated by 33% of respondents: investment in SIEM solutions and focus on email security. Four other tactics had a 31% adoption rate: SOAR, advanced analytics, multifactor authentication, and endpoint configuration hardening tools.

On the other hand, the lower percentage investing in air-gapped backup/restore capabilities (21% of respondents) suggests that organizations are prioritizing detection and response over recovery.

Data is the answer: 91% of respondents agree that better capture and analysis of detection data is one of the most effective tools to prevent successful ransomware attacks.

Cloud security. The cloud is where the action is, with 50% of respondents saying that the majority of their SOC team's time is spent addressing issues in the public cloud, while just 13% spend most of their time on on-premises issues.

This tracks, because much of our IT environments is in the cloud. Fifty-three percent of respondents say that the majority of their business-critical applications and workloads run in the cloud. Interestingly, this is down from 66% a year ago, but still significant. And in the public cloud, the threat is generally not an attack that outwits your cloud provider's defenses. It's more likely to be a misconfiguration on your end. The bad guys aren't looking to break down any doors; they're trusting you to leave one open for them.

Respondents gave us their top three cloud security challenges:

1. **Maintaining security consistency across their data center and public cloud environments (No. 1 for the third year in a row, but with the percentage declining from 45% last year to 33% for 2023)**
2. **Keeping identity and access management (IAM) systems accurate and up to date (32%, and up from third place a year ago)**
3. **Use of multiple cybersecurity controls increases cost and complexity (28%, and slipping from No. 2 a year ago)**

We then asked them what they're doing about it. Again, there was a wide range of tactics with no runaway leader, but the most common approaches are:

1. **Identifying workload configurations that are out of compliance and/or don't adhere to industry best practices (No. 1 for the third year in a row, though the percentage declined from 39% in 2022 to 30% this year)**
2. **The configuration of security groups (e.g., externally facing server workloads) (25%, and up from fourth place a year ago)**
3. **Improving audit trail understanding among privileged and service accounts (24%, holding steady at No. 3)**

Cloud and hybrid architectures are new, complex and ever-changing. They'll continue to be an area of intense challenge.

Must know cloud: When we asked about the various areas in which security teams are under pressure to upskill, cloud operations and architecture led — cited by 41% of respondents.

Goals and Strategies

The pursuit of cyber resilience and overall business resilience is driving security strategies, from increased funding and collaboration to priorities around cloud, analytics, automation and more.

Converging on resilience

To meet new and persistent challenges, organizations are focusing on resilience and agility. For the next 12 months, 51% of respondents plan solutions or investments that combine cyber resilience efforts with traditional business continuity/disaster recovery preparation. Further, 48% will make investments to speed the recovery of user services, and 47% are planning investments that speed security teams' response.

Resilience is a team sport, and most respondents understand that converging security operations with other functions (e.g., collaborating more closely, creating hybrid roles that overlay functions, etc.) holds promise:

- **81% of organizations are converging aspects of security and IT operations.**
- **69% are converging aspects of security operations and digital experience.**
- **69% are converging aspects of security operations and application development.**
- **61% are converging aspects of security operations and observability.**

Why? Respondents most often believe convergence will help with overall visibility of risks in their environment (58%) and that they will see improved cooperation in threat identification/response processes (55%).

Top Security Initiatives

Asked to name their three top priorities, respondents most often cited these.

Budgets rise, priorities shift

Security teams are spending more and collaborating more broadly. Fully 95% of respondents expect their security spending to increase over the next two years, and 56% say spending will increase significantly (up from 51% a year before).

Where funding will go to tools and technology, there's an even split in terms of approach: 50% say they'll focus on platform-based tools with out-of-the-box integration. The other half will emphasize a best-of-breed approach, integrating individual solutions as needed through APIs.

Strategic focuses have shifted since last year, as evident in the top four priorities:

- **Developing and building an integrated software architecture for security analytics and operations tools (38% versus 21% a year ago, moving to the top spot from a tie for third)**
- **Purchasing security operations tools designed to help an organization automate and orchestrate security operations processes (35% versus 22% a year ago)**
- **Consolidating tools and personnel into an enterprise SOC (35%, up from 15% in 2022 to break into the top 10 responses)**
- **Developing more formal documented security operations processes (33%, up from 17% and 10th place)**

Taken as a whole, these four leading strategies point to a desire to create a more effective, faster-moving and more professionalized SOC.

95% of security budgets will increase over the next two years — 56% of them "significantly."

Analytics and automation

Deployment of technologies designed for security analytics and operations automation and orchestration hold remarkably steady this year. Sixty-seven percent report deploying such technologies — 37% extensively. This is essentially unchanged from last year's research, which found 67% adoption, with 36% doing so extensively.

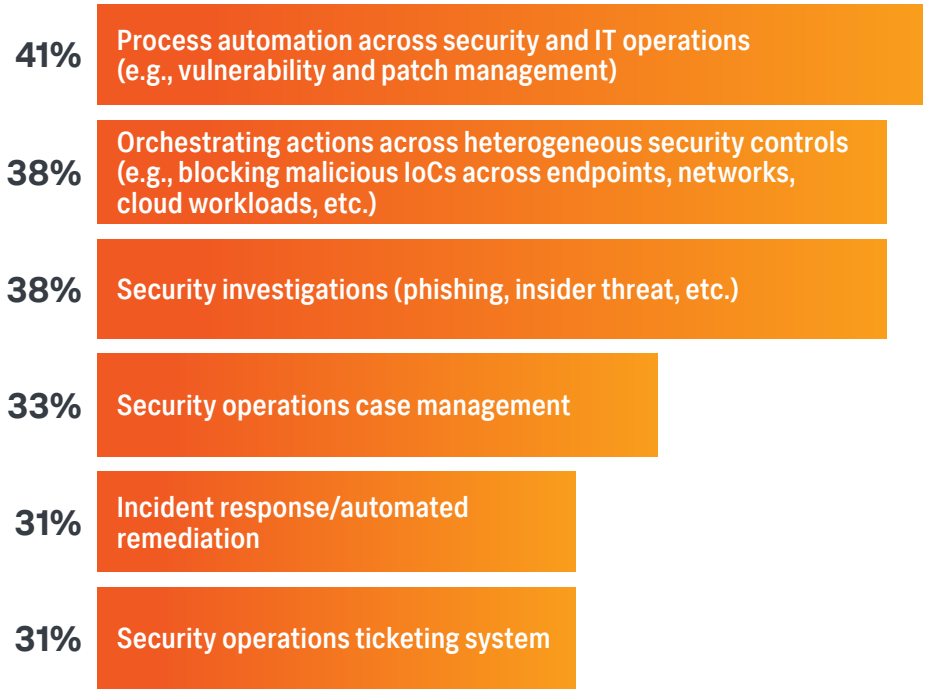
Respondents say they're using analytics across the entire attack lifecycle, to improve threat detection (37%), to help identify cyber risks (36%), to accelerate investigations (33%) and automate remediation (35%).

Top uses also include: to automate security processes based on real-time data (33%), and to help determine which investigations to prioritize (also 33%).

From a task perspective, the top targets for automation are:

- **29% prioritize integrating security tools with IT operations systems.**
- **27% prioritize integrating external threat intelligence with internal security data.**
- **27% prioritize automating basic remediation tasks (such as updating endpoint security controls) with their automation and orchestration initiatives.**

Top Priorities for Process Automation



It's not all forward progress. Efforts to enrich security analytics with other analytics — IT operations, business and risk management — appears to be plateauing. A year ago, 43% of organizations reported a significant level of integration across these sources; today the figure has fallen to 39%. (Another 35%, globally, report marginal integration.) There's a distinct difference among global regions, with 45% North American respondents reporting significant integration, versus Europe and Asia-Pacific trailing at 35% and 36%, respectively.

The best explanation for the regression would seem to be the complexity of data and the difficulty in integrating disparate tools.

"There's a lot of complexity that goes into developing good analytics," SURGe leader Ryan Kovar notes. "The pandemic drove a lot of change and an explosion of new data sources. Just as orgs might have been getting a handle on that kind of analytics integration, they've got all this new data and are having to refactor everything."

That said, vendors (including yours truly) are always looking to create more out-of-the-box ways to reduce complexity, helping organizations overcome any setback. To get back on track requires starting the processes from the beginning: defining integration goals; standardizing data, using pre-built detections that often come with security analytic solutions and, where possible, tools; and continuing to collaborate and build trust across teams and siloes.

Integration of Security Analytics With Other Analytics Data

e.g., ITOps, business, management and other analytics

From next-to-zero to resilience hero

We noted that security teams are increasingly seen as valued partners rather than boxes to check or obstacles to overcome. The result (or cause) is deeper collaboration at all levels.

For an example at the grassroots level, DevSecOps is pretty much everywhere. Only 3% of respondents say their organization does not leverage DevSecOps practices, down from a 25% holdout rate the previous year.

At the leadership level, we noted that 91% of CISOs are collaborating with other leaders on resilience. Sixty-eight percent of CISOs meet with their boards either weekly (29%) or monthly (39%). Only 8% meet less than quarterly. And the top results of these meetings, according to respondents, have been:

- **Improved ability to collaborate across business units (46%)**
- **Improved perception of security by other parts of the organization (44%)**
- **Better prioritization of security spending (43%)**
- **Increased security funding (42%)**
- **Instilling of cybersecurity initiatives across broader culture (42%)**

Across the board, collaborative practices are helping security teams hold the line against increasingly sophisticated attackers.

63% reported each of the following benefits of DevSecOps: operational efficiencies; better cloud security; more secure, reliable software; a better, more proactive security posture.

59% reported fewer security incidents as a result of DevSecOps practices.

Notably, respondents in Europe were more likely to report positive results, beating the global average every time, usually by 4-9 percentage points.

Recommendations

Security teams need to work with the entire organization to succeed. Here are eight ways that the teams who make the best partners are building more resilient organizations.

True organizational resilience lies not only with the security team's crucial efforts to improve threat detection and incident response, but through holistic collaboration. In the organizations we've worked with, resilience has been strongest with a collaborative approach in which everything — from software development and infrastructure monitoring to business continuity planning — brings security leaders to the table with IT and business executives to protect the organization.

The theme of trusted partnership ran through our findings in this year's survey, and when we look at how those most trusted organizations pursue their mission, certain recommendations emerge. The first four tie directly into the value of cross-organizational partnership.

1. Use data and analytics to optimize threat detection and response.

Security teams seen as enablers more often leverage analytics to identify cyber risks (38% versus 26%), improve threat detection (40% versus 25%), accelerate investigations (35% versus 27%) and automate remediation (38% versus 22%). As these teams' efforts to build data-driven efficiencies across detection, investigation and response improve security operations results, they'll likewise continue to elevate the security team's status with the business.

2. Plan for resilience.

The "business enablers" are much more apt to report that their organization has a formal approach to cyber resilience, instituted organization-wide (32% versus 19% of those teams seen as roadblocks). This is essential. Being an enabler is not just about collegiality. It correlates with actually improving your enterprise-wide posture on resilience.

3. Invest in resilience.

Security teams that are seen as enablers have definitive resilience investment plans for solutions that:

- Increase visibility throughout the entire technology environment (48% versus 38% of the "roadblocks")
- Accelerate response and remediation of incidents (53% versus 39%)
- Speed the recovery of customer and user services (50% versus 40%)
- Combine cyber resilience efforts with traditional business continuity/disaster recovery preparation (54% versus 39%)

4. Embrace functional convergence.

Teams seen as enablers are 2.5x as likely (32% versus 13% of the roadblock cohort) to note that their security operations team is collaborating with "all" adjacent functional areas included in the survey — ITOps, app dev, observability and digital experience.

From the security perspective, resilience emerges from a complete approach to the threat lifecycle. Data and analytics tools help you detect anomalies, while solid playbooks, effectively automated, help you respond faster. Then a unified approach to security operations allows teams to overcome the problem of having to swivel from one disjointed tool to another. (We're always up to help with that, BTW.)

These next recommendations are also actions more often undertaken by the enabler teams, though there is not necessarily a direct correlation between these actions and effective collaboration. We note them as additional best practices of organizations that have used cross-team partnership to improve security posture, instill broader resilience and increase their budgets.

5. Focus on the foundational.

When security teams are seen as enabling partners, they get the basics right. The obstacle/roadblock teams are more likely to say that a lack of basic hygiene on IT assets remains a key challenge to preventing security incidents (28% versus 19% of those seen as enablers). This is interesting, because you'd think that the roadblock security org would be more rigid about enforcing basic protocols. It seems that the more collaborative teams actually have better mastery of the basics, as well.

6. Cloud security is key.

Enablers are more likely than the roadblock group (31% versus 20%) to place importance on identifying misconfigured cloud workloads, misalignment with best practice frameworks like CIS, etc. We believe that more rigorous cloud workload hardening puts these security teams in a better position to say "yes" to the organization's cloud transformation projects, which is part of why they are held in higher esteem. SURGe's Ryan Kovar notes, "It's always better to be a team that can say yes than a team that says no."

7. Invest against ransomware risk.

Enablers are much more likely to report increasing investment, for the expressed purpose of helping mitigate ransomware risk. Not only is protecting against ransomware important in itself, but enablers' proactive steps to protect against this high-profile threat should also score points with the business leaders and build a more effective relationship. Specific ways enablers do that:

- Advanced analytics for anomaly detection (35% versus 18%)
- SOAR solutions (35% versus 21%)
- Endpoint detection and response (34% versus 17%)
- Privileged account monitoring (30% versus 20%)

8. Take a proactive stance against supply chain threats.

As with ransomware, the teams that are enablers are visibly more proactive about supply chain risk. Again, the benefits are both improved security and resilience and further establishing the credibility and partnership that makes security a more effective force in the organization. Specifically, these actions are favored by enablers against the specter of supply chain attacks:

- More frequent meetings between the CISO and executives and/or the board of directors (26% versus 15%)
- Conducting incident response activities like threat hunting and/or forensic investigations (25% versus 13%)
- Assessing whether current security controls would prevent/detect SCAs (30% versus 15%)
- Increasing log inspection (26% versus 16%)

We all know that no action, set of actions, protocol or arcane supernatural ritual will make our organizations attack-proof. But the strategies and tactics of those organizations that have had the most success becoming strategic partners to their broader organizations are great ways to begin to minimize risk while building greater resilience to withstand any storm.

Year-over-year (over year) highlights

Notable changes over time in global averages

2022 was a rough year for keeping up with security requirements. While 49% in 2021 said it was slightly or much more difficult to keep up, the number jumped to 66% in 2022, before settling to 53% this year:

Keeping up with cybersecurity requirements over the past two years is:

	2021	2022	2023
Much more difficult:	13%	28%	23%
Somewhat more:	36%	38%	30%
No more difficult:	20%	18%	13%
Somewhat easier:	22%	10%	22%
Much easier today:	9%	7%	12%

The biggest change over time among those respondents who found it harder to keep up with security requirements regarded "the more sophisticated threat landscape." In 2021, 48% indicated that problem, dropping to 38% in both 2022 and 2023. (Our 2021 research was conducted not quite a year into the global Covid-19 pandemic.)

We asked respondents what type of attacks they'd suffered in the previous two years. In every case there was a large jump from 2021 to 2022, and a slight increase or steady number between 2022 and 2023. Examples:

- **Data breach:** 39% in 2021, 49% in 2022, 52% in 2023
- **Ransomware:** 31% in 2021, 45% in 2022, 49% in 2023
- **Business email compromise:** 42% in 2021, 51% in 2022, 51% in 2023
- **Insider attack:** 27% in 2021, 39% in 2022, 40% in 2023

Downtime is up. Comparing 2022 numbers to 2023, security-related disruptions occurred:

- **Weekly or more often:** 21% in 2022, rising to 24% in 2023
- **Once every few weeks:** 19% in 2022, rising to 22% in 2023
- **Monthly:** 14% in 2022, rising to 16% in 2023
- **Every few months:** 16% in 2022, dropping to 15% in 2023
- **Every few quarters:** 11% in 2022, dropping to 10% in 2023
- **Once a year or less:** 19% in 2022, plunging to 12% in 2023

Mean time to recover has improved since 2022.

- **Within minutes:** 10% in 2022, 17% in 2023
- **A few hours:** 31% in 2022, 29% in 2023
- **Several hours:** 32% in 2022, 34% in 2023
- **Days:** 16% in 2022, 15% in 2023
- **A week or more:** 10% in 2022, 6% in 2023

Over time, strategic priorities have shifted. The following four strategies are much more important in 2023:

- **Actively develop and build an integrated software architecture for security analytics and operations tools:** 38%, up from 21% in 2022 and 18% in 2021
- **Consolidate tools and personnel into an enterprise SOC:** 35%, up from 15% in 2022 and 14% in 2021
- **Purchase tools to automate and orchestrate security operations processes:** 35%, up from 22% in both of the previous two years
- **Develop more formal documented security operations processes:** 33%, up from 17% in 2022 and 15% in 2021

Country highlights

Snapshots of the global state of security

Australia and New Zealand

Ransomware is not exactly top-of-mind in Australia and New Zealand (ANZ): Just 19% call it a top focus area for next year, versus 29% of respondents in the rest of the Asia-Pacific region. Possibly related: organizations in ANZ seem to rely more on cyber insurance for ransomware than their peers, so maybe system lockouts are just a cost of doing business. We also saw more focus in ANZ on zero trust, less on ransomware — more reliance on insurance.

Among organizations that have been the victim of successful ransomware attacks, 38% in ANZ say they have most often had their insurance company pay (versus 21% of their peers in the rest of the world). Maybe the insurance rates are better there, since ransoms in ANZ tend to be lower in ANZ versus the rest of the world. So far.

Other notable findings:

- CISOs tend to meet less often with their LOB peers: Just 14% say their CISO provides weekly briefings on security posture — less than half the frequency (30%) reported by respondents in the rest of the world.
- Though ANZ orgs are slightly more likely to call DevSecOps a fairly significant focus area, they report less success with it. Only 49% say DevSecOps has resulted in a reduction in incidents (versus 60% in the rest of the world), and only 48% say it has helped with compliance (versus 63%).

Canada

Respondents in Canada are generally more anxious about rising threats and security requirements; 76% say keeping up with security requirements has gotten harder over the last two years, versus 51% in the rest of the world.

The pessimism may be earned. Canadian organizations more often report security incidents in the recent past, including system compromises by bad actors (62% versus 51% in the rest of world) and breaches (65% versus 51% in the rest of world). Canadian respondents also report greater struggles with critical workload uptime and availability: 33% say they've seen weekly or more frequent outages among business-critical applications as a result of security incidents versus 19% of their U.S. peers.

On the bright side, Canadian orgs perform above the mean for both MTTD and MTTR.

- MTTD: 39% of Canadians say their mean time to detect is two weeks or less, versus 26% in the United States.
- MTTR: Canadians are also more likely than U.S. respondents to say their recovery time can be measured in minutes (24% versus 14%).

So, while Canadian orgs struggle with more incidents and more frequent downtime, they display relatively high agility in handling issues.

Canadians are also more likely than U.S. respondents to say that DevSecOps practices are increasing collaboration between security and development teams (73% versus 63%) and improving compliance (71% versus 59%).

Canadians also voice more faith in AI's ability to fortify the SOC: 61% say AI technologies outperform human analysts at identifying fraudulent actions, versus 40% in the United States.

France

French respondents really feel like they're on top of things. Just 14% say staying ahead has gotten much harder, versus 29% of peers elsewhere in Europe, and 24% across the rest of the world. Two potential reasons:

1. French respondents less often say that finding skilled labor is a challenge (10%, versus 23% in the rest of Europe and 26% in the rest of the world).
2. Only 12% of French respondents say they're inundated with false positives and/or alerts lacking context — not quite half the rate of European peers (25%) or the rest of the world (26%).

As in other countries where concerns run lower (see Germany, on the following page), incidents are also fewer:

- 29% of French orgs report breaches in the past two years, versus 61% across the rest of Europe.
- 23% report compliance violations, versus 54% elsewhere in Europe.
- 26% report insider attacks, versus 53%.
- 27% report account takeover attacks, versus 52%.

The French see fewer security-related business-critical outages, too: 6% suffer them weekly, versus 40% in the rest of Europe; and 22% say that outages come yearly at most, versus 6%.

French respondents report comparable progress on resiliency, but there is nuance: 61% say their resiliency investments for the next year will focus on accelerating incident response and remediation (versus 40% in the rest of Europe) while their European peers are more focused on the ability to recover a "known good" copy of data (42% elsewhere in Europe, versus 31% in France).

Also noteworthy: French respondents struggle more with tool complexity.

- On general security challenges, 29% struggle to manage too many disconnected security point tools, versus 19% in the rest of the region.
- On cloud-specific challenges, 37% say the use of multiple cybersecurity controls increases cost and complexity (versus 24% in the rest of the region).

Both data points indicate that French teams should pursue simplification and rationalization of point tools — without sacrificing security efficacy, of course.

Germany

Only 38% of German respondents say that keeping up with threats and security requirements has gotten harder in the last two years — compared to a weary 61% of respondents in other European countries, and 54% across the rest of the world.

Maybe German confidence comes from their progress in terms of resilience: 27% report having a formal, organization-wide approach to cyber resilience, compared to just 18% of other respondents in the region (putting Germans in line with, not ahead of, global norms).

It might also be that German orgs have seen fewer incidents. Just 40% report having been breached in the last two years, versus 57% across other surveyed European markets and 53% across the rest of the world. German respondents also cite fewer compliance violations (25% versus 52% in other European nations surveyed), insider attacks (32% versus 50%), and business email compromise (36% versus 63%).

On the downside, German response to those incidents that do happen is more sluggish. Post-incident analyses show that in Germany, bad actors have access to systems for nearly three months before the organization is aware, versus less than two months among other European respondents. MTTR is slower by a similar margin.

More differences: German respondents more often say that finding skilled security staff has gotten harder for them (33% versus 18% among others in Europe). Adding to this, German respondents report more hesitance around AI. Only 30% say AI is capable of outperforming analysts at anomaly detection (versus 53% of other respondents in the rest of the region). They also have made less progress around security operations automation and orchestration: Only 29% report extensive progress here versus 40% of their peers in the region. Skills scarcity, combined with less investment in AI and automation, may put German organizations on a path where security teams will eventually struggle more to keep up.

India

Data from India presents a daunting picture. On the one hand, Indian teams are very well-resourced: 66% of respondents report more than 25 FTE resources in their SOC versus 36%, on average, in the rest of the world. On the other hand, they're really scrambling to keep up:

- 42% of Indian orgs report being overwhelmed by the number of attacks (versus 23% in the rest of the world).
- 44% report being inundated with false positives (versus 24%).

Part of the problem seems to be the complexity of their tool ecosystems: 48% say their security stack is too complex, compared to 28% in the rest of the world.

The result, unsurprisingly, is that respondents in India more often report having been breached in the last two years (59% versus 45% of respondents elsewhere in the broad Asia-Pacific region) and incidents are causing negative business outcomes at higher rates, including reduced company valuation (42% versus 25% in the rest of the region).

The good news is that CISOs are rising to the challenge: 33% report briefing line-of-business leaders on the organization's security posture weekly (versus 16% across the rest of Asia-

Pacific). The efforts are paying off, with 57% of respondents saying this has directly led to greater prioritization of security investments (versus 42% in the rest of the region).

Another bright spot is that organizations in India appear to be converging aspects of their security operations with complimentary functions more often than their peers: 42% say they are converging security operations with all areas included in the survey (observability, digital experience, ITOps and application development) versus 25% in the rest of the region. Attribute it to enthusiasm for the potential benefits: 74% aim to improve visibility into risks (versus 53% in the rest of the region); 64% aim to identify issues sooner (versus 51%), and 70% converge aspects of security and other functions to improve cross-functional collaboration (versus 53%).

Japan

The Japanese are more focused on ransomware: 35% of respondents list it as a top-three initiative for the next year, versus 23% across the rest of the Asia-Pacific region. And it looks like that focus is paying off: 40% of Japanese orgs report suffering a ransomware attack in the past two years, versus 50% across the rest of the world.

In other areas, Japan's focus lags:

- Fewer Japanese organizations have a formal approach to cyber resilience that has been implemented organization-wide across critical systems (23% versus 34% in the rest of the region).
- Fewer Japanese orgs plan investments in resiliency technology to increase visibility (37% versus 46% in the rest of the region) or to better understand the downstream impacts of incidents (40% versus 50%).

Organizations in Japan also appear to be more complacent when it comes to software supply chain attacks. Only 15% report that recent incidents have led to more meetings between the CISO and other business leaders (15% versus 29% of respondents in the rest of the region) or to updates of their vendor risk management policies (16% versus 26%).

Singapore

Singaporean respondents' concerns are often very different from the rest of the world's worries.

Start with supply chain: Singaporean orgs are less likely to report software supply chain security as a top area of focus for the coming year (23% versus 33% in the rest of the world). In fact, only 38% of Singaporean organizations say they've significantly increased that focus following recent software supply chain attacks (versus 70% of respondents in the rest of the world). And they've less often taken actions specifically aimed at mitigating software supply chain risk, such as:

- Hiring third-party service providers to conduct a risk assessment (15% versus 26% in the rest of the world)
- Adopting more thorough software supply chain security policies (15% versus 23%)
- Conducting penetration testing or red team exercises (15% versus 25%)

Second example: ransomware. Singaporean respondents are less likely to say that their organization has implemented, or

increased investment in, key controls to help with ransomware, including:

- Endpoint detection and response (17% versus 30% in the rest of the world)
- Solutions to implement ransomware detection rules (17% versus 26%)
- Advanced analytics for anomaly detection (22% versus 32%)

Finally, respondents in Singapore are increasing investment in security at a lower rate than their peers: Just 27% say that their organization will increase spending significantly over the next 12-24 months (versus 59% across the rest of the world).

While Singapore's security teams don't report a higher incidence of ransomware or supply chain attacks to date, their lower focus and lower funding elevates future risk.

United Kingdom

The security picture in the UK is bleak. UK respondents report having suffered from a recent breach at twice the rate of their peers in Western Europe (68% versus 34%) and have run afoul of regulations more often (64% versus 24%). Moreover, UK respondents are more likely to say that these incidents have had real consequences, such as hurting their company's valuation (37% versus 25%).

No surprise, then, that UK respondents more often report high levels of anxiety about keeping up with security requirements and threats (35% say it has gotten much harder over the last two years versus 12% of respondents in the rest of Western Europe).

Two key drivers: 26% of respondents say they are overwhelmed by false positives and alerts that lack context (versus 15% across the rest of Western Europe) and 30% say their cybersecurity posture is based on regulatory requirements rather than security best practices (versus 20% across the region).

Resilience also lags: 25% of UK respondents say their security teams have not yet developed a formal resilience strategy — five times the rate of organizations in the rest of the world. And just 16% have a formal approach to cyber resilience that has been instituted organization-wide (versus 35% of organizations in the rest of the world).

UK respondents know they have work to do:

- They're targeting larger reductions in both MTTD (48% versus 41% across other European markets) and MTTR (67% versus 48%).
- They understand the value of resilience, strongly agreeing that not increasing resilience will put them at risk of losing customers (59% versus 35% across other European markets) and being out-innovated due to disruptions and lost productivity (57% versus 28%).
- They have also significantly increased their focus on third-party risk assessment activity as a result of recent software supply chain attacks more often than their peers (79% versus 64%).

United States

U.S. respondents are generally less anxious about keeping up with security requirements and the rising threat landscape than their peers: 44% say that it has gotten harder over the last two years, versus 76% of non-U.S. North America, and 56% in the rest of the world. Several factors contribute to U.S. organizations' lower-stress vibes. Two important ones:

1. Staffing seems less of a pain point. Only 20% of U.S. respondents cite an understaffed security team as a key challenge, versus 30% among other respondents in North America, and 23% in the rest of the world). U.S. respondents report fortifying their internal teams with managed services at a higher rate: 54% say the majority of their SOC workload is handled by partners versus 41% of their peers in the region (and 56% in the rest of the world).
2. U.S. orgs have placed a greater emphasis on resiliency as a security tenet. Forty-five percent report that their organization has a formal approach to cyber resilience that has been instituted organization-wide across critical systems, compared to just 25% of respondents in the rest of the world.

These differentiators are helping U.S. organizations fare better when it comes to security incidents. Regionally, U.S. respondents are less likely to report experiencing, in the past two years, a data breach (51% versus 65% in the rest of North America), business email compromise (42% versus 58%), DDoS attacks (39% versus 53%), and system compromises (46% versus 62%). This led to fewer instances of downtime for business-critical workloads (mean frequency per year: 19 versus 25).

Strategically, U.S. respondents are more apt to say their organization will emphasize DevSecOps (37% versus 28% in the rest of the world) and security automation (41% versus 35%) over the next year, but they may face higher levels of exposure to ransomware, with just 19% saying this is a top security initiative (versus 30% in the rest of the world).

Industry highlights

Standout data points for four select industries worldwide.

Communications and Media

Data from the communications and media industry points to two notable trends:

1. Security tool complexity appears to be a bigger issue. When asked about their SOC operations, communications and media respondents are more apt to say that their analysts spend too much time pivoting between too many disparate security tools and management consoles, with little, if any, integration, which inhibits a comprehensive and timely response (47% versus 37% among respondents in other industries).

   The data reveals possible contributing factors:

   - Communications respondents more often say that their existing security tools don't support cloud environments (27% versus 19% across other industries), meaning they may have felt the need to adopt separate solutions for cloud environments.
   - Communications respondents are also less likely to say they're converging aspects of IT operations with security (75% versus 82%).
   - Higher levels of fragmentation (across both teams and environments) may be contributing to complexity, though communications respondents are more likely to say that, going forward, their organizations will emphasize platform approaches to security (57% versus 49%).

2. CISOs in this industry are less engaged with senior business leaders. Just 17% of respondents in this sector report that their CISO has weekly discussions with executives about overall security posture and key metrics (versus 30% of respondents in all other industries).

   One of the key outcomes of these types of discussions, and their frequency, is increased funding for the security team. Given that CISOs at communications companies have less frequent touchpoints with their business leaders, it is not surprising to note that respondents at these organizations are less likely to report their organizations will be significantly increasing security spending over the next 24 months (45% versus 57% among other industries).

Financial Services

Respondents in the financial services sector stand out from peers in other industries in three ways:

1. They've had more success mitigating risks associated with ransomware. Thirty-two percent of respondents say they've had data and systems held hostage, versus 45% in other industries. Financial firms also are more likely to have made/increased investments in four areas with expressed intent of helping with ransomware detection, prevention and response:
   - Email security hardening (41% versus 31% across the board)
   - Creation/implementation of specific ransomware detection rules (32% versus 24%)
   - Advanced analytics solution for anomaly detection (36% versus 30%)
   - Security information and event management (SIEM) solution (39% versus 32%)

2. They've had more success preventing supply chain attacks. Forty percent of financial firms report that they've experienced a supply chain attack, versus 48% across other industries. Notably, financial firms are more likely to have:
   - Reassessed/changed policies toward vendor risk management (27% versus 21% across other industries)
   - Performed an assessment of current security controls to determine whether they would prevent/detect supply chain attacks (31% versus 25%)
   - Increased questionnaires/audits of their software supply chain vendors (30% versus 22%)

3. They've had less success instituting DevSecOps initiatives. Respondents in the finance space are significantly less likely to say that their DevSecOps initiatives had delivered benefits for them in areas such as:
   - Repeatability across software development projects (56%, trailing other industries, which averaged 63%)
   - Cybersecurity proactivity (57% versus 65% across other industries)
   - Collaboration between their cybersecurity, development and operations teams (67% versus 59%)
   - Ability to respond to audits (55% versus 62%)
   - Security of sensitive cloud-resident data (65% versus 55%)

Given these more muted results, it's not surprising that financial services respondents are more likely to report DevSecOps as a focus area for the next year (40% versus 28%).

Manufacturing

Respondents in the manufacturing sector indicate acute problems with staff and skills scarcities. For example, 56% of them say that they don't have enough people to handle the increasing volume of security events (versus 47% across other industries). Similarly, manufacturers more often say that they struggle both to hire enough staff, with the right skill sets, to handle the workload (31% versus 22%).

Not surprisingly, then, respondents at manufacturing companies are more apt to say that, in the past 12 months, staffing issues contributed to multiple instances of:

- Considering finding a new job due to their current workload (51% versus 39% across other industries)
- Team members being asked to lead projects without the requisite experience (60% versus 40% elsewhere)
- A project failing (52% versus 36%)

Furthermore, manufacturers are less likely to report that their SOCs run 24 hours a day, 365 days a year: 17% versus 27% across other industries. Manufacturers more often operate their SOC only during business hours: 30% versus 13% across other industries.

Manufacturers appear to be trying to close their skill gaps with automation and AI. They are more apt to say that they're using machine learning technologies extensively for security analytics (43% versus 32%) and have deployed security and operations automation and orchestration technologies extensively (44% versus 35%). However, their greater likelihood to report having suffered weekly outages of business-critical systems due to security incidents (44% versus 19%) suggests that these approaches have not completely offset their staffing challenges.

Public Sector

A common theme from our public sector respondents is that they're struggling to keep pace with the risk landscape. More than two-thirds (68%) explicitly say that keeping up with cybersecurity requirements (i.e., deploying/tuning controls, monitoring network behavior, following threat intelligence, etc.) is more difficult today than it was two years ago (compared to 52% of respondents from other industries).

Alert volumes in particular appear to be a pain point, with 34% of public sector respondents saying keeping up with security alerts is among their top security challenges (versus 23% of respondents in other industries).

Two causes are at play: tool complexity and staffing shortages. Public sector respondents are more likely than their private sector counterparts to report that their organization suffers from both issues (37% versus 26% across other industries).

Additionally, public sector respondents are consistently more negative about AI's ability to lighten the security team's load. They are less likely to report that AI can outperform human analysts today in areas such as:

- Threat hunting (24% versus 46% across other fields)
- Triaging and prioritizing events (43% versus 28%)
- Identifying anomalous user behavior (30% versus 47%)

As a sector, these organizations would be well served to investigate how intelligent automation can help their team better keep pace — which may help close the recovery time gap observed in the industry (a mean time to recover of 22.3 hours, versus 15.1 hours for other industries).

Make your organization more resilient with the unified security and observability platform. Go from holistic visibility to effective action, fast and at scale. See how Splunk can help you keep your organization securely up and running, no matter what digital disruptions come your way.

Learn More

23-119356-Splunk-State of Security-EB-108

splunk>