Executive summary

Security Priorities Study 2023

The security leader’s ongoing battle for cyber resilience

FOUNDRY
an IDG, Inc. company

In the battle between cybersecurity adversaries and defenders, the adversaries at least for now, have the upper hand on many global organizations. The relentless cycle of new phishing scams, malware attacks and cybersecurity threats make it hard to stay a step ahead. Even worse, adversaries are accelerating and widening their range of sophisticated attacks at scale through automation, cybercrime-as-a-service models, impersonations and adaptation.

In fact, 88% of security leaders surveyed in the 2023 Security Priorities Report believe their organization is falling short addressing cyber risks. Yes, that sounds bad, but on the bright side that number is down from 90% in 2022. The reasons for their gloom—security leaders struggle to convince all or parts of the organization about the severity of the risk (28%). Some organizations aren't investing enough budget resources for people and technology (26%) and others can't find and retain the skilled talent that they need (26%).

But amid these challenges are possible solutions. Budgets are increasing or holding steady, security teams are testing AI security tools to increase their speed and agility, and to make up for skills shortages. They're beefing up cyber insurance policies, and they're investing in new technologies to increase incident response, protect sensitive data and fortify corporate resilience.

The 2023 Security Priorities report surveyed 790 IT security executives, managers and professionals from around the globe to gain a better understanding of the current security projects that

88%

of security leaders believe their organization is falling short addressing cyber risks.

Non-malicious user error (i.e., falling victim to phishing) is the no. 1 cause of data security incidents at organizations.

organizations are focused on today and in the year ahead. The survey also looked at the issues that will demand the most time and strategic thinking for IT and security teams. The survey defines a security incident as an event that indicates an organization's data or systems have been compromised. This includes a wide variety of security violations, including ransomware attacks, data breaches and third-party or supply chain breaches.

Causes and outcomes of security incidents

It's important to recognize that despite all the security technologies available, people are most often responsible for security incidents. For the third year in a row, the most commonly cited cause of security incidents is non-malicious user error, this year at 31%, but that number has inched slightly lower over the years—down from 33% last year and 44% in 2021. This could be thanks to increased security awareness training or because security models like Zero Trust are having an impact. Other main causes of security incidents were unpatched software vulnerabilities (27%), third-party security (25%) and misconfiguration of services or systems on or off-premises.

Top security priorities

Security leaders have a long list of priorities for the coming year, starting with being appropriately prepared to respond to security incidents, at 41%. They also want to improve the protection of confidential and sensitive data (36%). Corporate resiliency is another top concern, with 34% of organizations planning to upgrade IT and data security, and 33% improving security of cloud data and systems. And while fewer employees are falling for phishing attacks and other human-error exploits, 32% of organizations still plan to increase or improve security awareness training of end users.

This year's top 5 security priorities:

1. Be appropriately prepared to respond to a security incident
2. Improve the protection of confidential and sensitive data
3. Upgrade IT and data security to boost corporate resiliency
4. Improve security of cloud data and systems
5. Improve/increase security awareness among end-users through training

Challenges forcing security leaders to redirect their focus:

1. Meeting governance and compliance regulations
2. Budgetary constraints/ demonstrating ROI
3. Employee awareness and training issues

But those priorities often face headwinds. Security leaders are consistently forced to redirect their time, and lately the most common distraction has been meeting governance and compliance regulations (26%). Almost half (46%) of security leaders say new SEC rules, which require disclosure within four days when a cybersecurity incident may be material to investors, is impacting how they handle cybersecurity initiatives at their company. More than a third of enterprises (38%) have processes in place to determine materiality, along with 22% of small and midsize companies. Another 30% overall are still developing policies, and 29% have no policies in place.

Security priorities have also gone off-course due to budget constraints (24%), employee awareness or training issues (23%) and IT audits (22%), according to survey respondents.

98%

of security budgets will either increase or stay the same over the next 12 months.

Factors determining security spending

- Digital transformation initiatives (51%)
- Compliance and regulatory mandates (45%)
- Industry best practices (43%)

Security investment plans

Overall security budgets will increase or hold steady for nearly all organizations surveyed (98%) for the coming year. In terms of what's driving overall spending, it's the evolving risks resulting from changing business dynamics, such as digital transformation efforts (51%), followed by compliance and regulatory mandates (45%) and industry best practices (43%). More specifically, IT and security leaders will focus this spend on improvements in the areas of authentication, data analytics, cloud data protection, cloud-based cybersecurity services and cyber risk insurance (32% each), along with a dozen other items.

Tech: What's already in place, and what's next

Organizations have added more security tools, technologies and services than they have retired over the past 12 months. Three-

> **69%**
>
> of security decision-makers agree that understanding which security tools and solutions fit best within their company is becoming more complex.

quarters of organizations added three or more new security tools in the past year (75%) compared to 56% that have retired three or more tools in the same period.

When asked what current security activity was "in use," respondents said: authentication (79%), endpoint protection (76%), access controls (75%), data backup and recovery services (74%), and security education/awareness training (74%).

Organizations will spend a portion of security budgets on improving those existing technologies. For example, 20% of organizations are upgrading or refining authentication tools, as well as access controls (20%).

Hot security tools being researched

Understanding which security tools and solutions fit best within a company is becoming more complex, according to 69% or security leaders, and companies are researching dozens of potential security technologies to find the right fit.

As mentioned earlier, security leaders are looking to improve authentication, and that's probably why zero trust leads the list of technologies being actively researched at 32%, with another 49% already using it. Those numbers haven't budged from 2022, which may indicate that organizations in research mode are still weighing their options.

Rounding out the top five hot security tools being researched are secure access service edge (SASE), deception technologies, extended detection and response (XDR) and biometrics.

67% of organizations are leveraging AI in their security technologies.

72% have already seen benefits, with the no. 1 being faster identification of unknown threats.

The rise of AI

Some 67% of organizations are leveraging artificial intelligence in their security technologies to keep up with ever-evolving threats and to help offset staff shortages. That number is higher for enterprises (79%) and lower for SMBs (55%). AI is being used

> **34%**
>
> of security ITDMs say they need to carry more than one cyber insurance policy to get the level of coverage they need.

in threat detection (44%), malware detection (36%), automated alerts and triage (32%) and real-time risk prediction (26%). Almost three-quarters of security leaders (72%) say they have already seen the benefits of AI-enabled security tech used in their own organization. It helps them more quickly identify unknown threats, accelerates response time, eliminates time-consuming tasks and reduces employee workload. AI can also sift through large amounts of data faster than previous solutions.

Investment in cyber insurance

As mentioned earlier, one of this year's top spending drivers is investment in cyber insurance policies. More than half of organizations already have cyber insurance policies, but only 18% have had to file a claim. Another 22% are actively researching policies. Some organizations see these policies as a necessary evil, with roughly half of respondents insisting that cyber risk insurance is a key part of their strategy to offload risk (52%) and roughly half also saying that cyber insurance is too expensive (53%). They also say that renewal is becoming more difficult (44%). Some feel that insurers' requirements are too difficult to meet and not worth the effort (40%). Others need to carry more than one cyber insurance policy to get the level of coverage they need (34%).

People and organizations

Cybersecurity leadership at the top of the organization remained steady from a year ago, with 65% of organizations having a CISO, CSO or top security executive. Although enterprises reported slightly higher numbers (83%) and SMBs slightly lower numbers of top cyber executives (47%) than last year.

85% of security leaders have regular or frequent engagement with their board of directors.

As the security stakes increase both domestically and abroad, boards of directors are taking a more active role in security issues. The vast majority of security leaders, 85%, report regular or frequent engagement with their board of directors. Nearly half (48%) meet with the board one or more times a month. One reason this communication has become more frequent may be that 25% of security leaders now report directly to the board, up from 20% a year ago.

> **57%**
> say that the no. 1 challenge associated with implementing a security operations center is a skills and knowledge shortage.

More security leaders have also centralized operations to unify and coordinate all security technologies and improve the organization's threat detection, response and prevention. Some 91% of organizations have a security operations center, either in-house or outsourced, or plan to add one. But nearly all of those organizations, 90%, still face ongoing staff and skills shortages in their operations centers, as well as insufficient budgets for an SOC (35%).

To fill the talent gaps, more than half of IT leaders say they're upskilling current staff and transitioning them into new roles (56%), while others outsource some security functions (42%) or turn to AI to automate security practices (38%).

Conclusion

An alarming 88% of security leaders believe their organization is falling short in addressing cyber risk, specifically when it comes to convincing their organization of the severity of risks they face.

To improve the situation, more top security execs are having regular engagement with the board of directors, and about half say their board has experience with cybersecurity-related issues.

IT leaders are addressing security risks by investing in new solutions and increasing spend on their existing security stack.

Some 98% of security leaders say they expect their security budgets to increase or remain the same over the next 12 months. They'll spend on beefing up defenses, protecting data and creating better security awareness, with the added assurance of cyber insurance policies and artificial intelligence in their security technology.

About the survey

The 2023 Security Priorities Report analyzed data from a Foundry online questionnaire given to 790 security professionals. All respondents are involved in IT and/or corporate IT and physical security decision-making, with 77% having an executive, IT or security title. Respondents represent companies primarily in North America (49%), with some in the Asia-Pacific region (33%) and in Europe (18%). These companies come from a variety of industries, including technology, manufacturing, financial services, professional services, healthcare, government, education and retail. The average company has 11,110 employees.

Key global differences

For many survey questions, security leaders report similar results across all three regions surveyed. However, a few key points of difference stick out.

North America

Challenges redirecting their time from strategic security initiatives

- Meeting governance and compliance regulations **(28%)**
- Budgetary constraints/ demonstrating ROI **(27%)**
- Employee awareness and training issues **(25%)**

What are NA security leaders increasing spend on?

98% expect their budget to increase or stay the same over the next year.

They're increasing spend on:

- Cyber risk insurance **(35%)**
- Data analytics **(31%)**
- Cloud data protection **(30%)**
- Endpoint protection **(30%)**

Security decision-makers in NA are researching tools to add to their security stack

The following are on their radars:

- SASE (Secure Access Service Edge) **(34%)**
- SOAR (Security Orchestration, Automation, and Response) **(34%)**
- XDR (Extended Detection and Response) **(33%)**
- Zero Trust technologies **(32%)**

AI's impact in security

63%

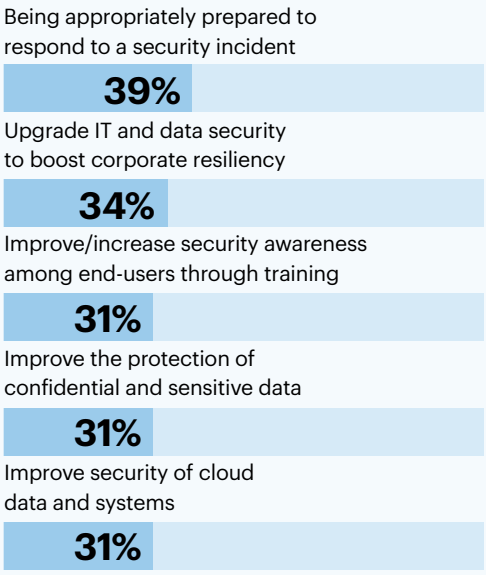
of NA security ITDMs are leveraging AI in their security technologies.

67% are already seeing benefits, including:

- Faster identification of unknown threats **(33%)**
- Accelerated detection and response times **(30%)**
- AI can sift through large amounts of data faster than previous solutions **(30%)**

EMEA

The top security priorities



Challenges redirecting their time from strategic security initiatives

- Meeting governance and compliance regulations **(30%)**
- Preparing for or addressing risks from cyber threats originating outside our organization **(26%)**
- Employee awareness and training issues **(23%)**

What are EMEA security leaders increasing spend on?

96% expect their budget to increase or stay the same over the next year. They're increasing spend on:

- Authentication **(41%)**
- Cloud data protection **(39%)**
- Application development security **(39%)**
- Cloud-based cybersecurity services **(38%)**

Security decision-makers in EMEA are researching tools to add to their security stack

The following are on their radars:

- Zero Trust technologies **(28%)**
- CASBs (Cloud Access Security Brokers) **(27%)**
- SASE (Secure Access Service Edge) **(26%)**
- Deception technology **(26%)**

AI's impact in security

73%

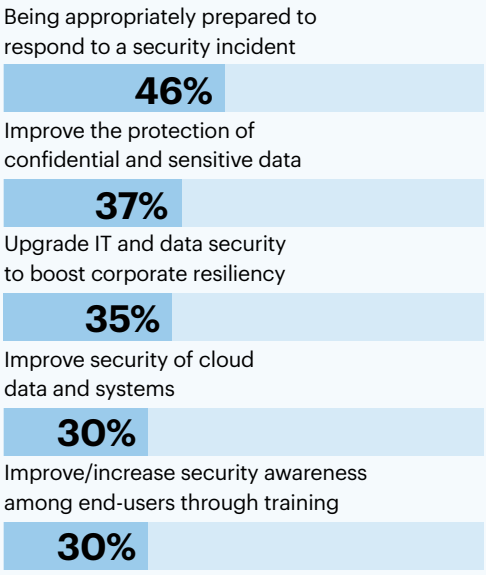
of EMEA security ITDMs are leveraging AI in their security technologies.

83% are already seeing benefits, including:

- Faster identification of unknown threats **(44%)**
- Accelerated detection and response times **(40%)**
- Reduced employee workload **(30%)**

APAC

The top security priorities



Challenges redirecting their time from strategic security initiatives

- IT audit **(24%)**
- Unanticipated business risks **(23%)**
- Meeting governance and compliance regulations **(21%)**
- Budgetary constraints/ demonstrating ROI **(21%)**

What are APAC security leaders increasing spend on?

98% expect their budget to increase or stay the same over the next year. They're increasing spend on:

- Cloud-based cybersecurity services **(34%)**
- Data backup and recovery, including cyber recovery services **(34%)**
- Authentication **(33%)**
- Application development security **(33%)**
- Data analytics **(32%)**
- Cloud infrastructure management technology **(32%)**

Security decision-makers in EMEA are researching tools to add to their security stack

The following are on their radars:

- Zero Trust technologies **(34%)**
- XDR (Extended Detection and Response) **(32%)**
- Deception technology **(30%)**

AI's impact in security

68%

of APAC security ITDMs are leveraging AI in their security technologies.

75% are already seeing benefits, including:

- Faster identification of unknown threats **(39%)**
- Accelerated detection and response times **(30%)**
- Eliminates time consuming tasks **(28%)**
- Reduced employee workload **(28%)**

Examining the marketplace

Research is an invaluable way for marketers to better understand customers and prospects, with the goal of building quality connections. At Foundry this is one way we are focused on building bridges between tech buyers and sellers. Our first-party relationships with the most important tech buyers and influencers around the world, allows us to apply value across our customers marketing stack. Our research portfolio explores our audiences' perspectives and challenges around specific technologies—from analytics and cloud, to IoT and security—and examines the changing roles within the IT purchase process, arming tech marketers with the information they need to identify opportunities.

To see what research is available, visit FoundryCo.com/tools-for-marketers. For a presentation of full results from any of these studies, contact your Foundry sales executive or go to FoundryCo.com/contact-us**.**

Buying process

Each year we take a deep dive into the enterprise IT purchase process to learn more about who is involved and who influences decision-making, what sources purchasers rely on to keep up to date with technology—and throughout the purchase process—and how they want to engage with the vendors they are working with. Visit FoundryCo.com/customerjourney for more information.

Buying process studies

- Role and Influence of the Technology Decision-Maker
- Customer Engagement

Technology insights

Each year we explore the technologies that are top of mind among our audiences to understand the business challenges, drivers, and adoption within the enterprise. These research studies are designed to help IT marketers understand what their customers are focused on and where the market is moving.

Role and priority studies

- CIO Tech Poll: Tech Priorities
- State of the CIO

Technology-specific studies

- Data and Analytics
- Cloud Computing
- Digital Business
- Security Priorities
- AI Priorities

Stay in touch with us

Email: Sign up for Foundry's newsletters and receive media and marketing trends as well as our proprietary research, product and event information direct to your inbox. **Go to** FoundryCo.com/newsletter.

Twitter: To get results from Foundry research when it's released, or any other news, follow us on Twitter: @FoundryIDG

LinkedIn: For research, services and events announcements, visit us on LinkedIn: https://www.linkedin.com/company/foundryidg/

Find it all on FoundryCo.com

About Foundry

Foundry's vision is to make the world a better place by enabling the right use of technology, because we believe that the right use of technology can be a powerful force for good.

Foundry (an IDG, Inc. company) is a trusted and dependable editorial voice, creating quality content to generate knowledge, engagement and deep relationships with our community of the most influential technology and security decision-makers. Our premium media brands including CIO®, Computerworld®, CSO®, InfoWorld®, Macworld®, Network World®, PCWorld® and Tech Hive®, engage a quality audience of the most powerful technology buyers with essential guidance on the evolving technology landscape.

Our trusted brands inform our global data intelligence platform to identify and activate purchasing intent, powering our clients' success. Our marketing services create custom content with marketing impact across video, mobile, social and digital. We simplify complex campaigns that fulfill marketers' global ambitions seamlessly, with consistency that delivers quality results and wins awards. Additional information about Foundry is available at FoundryCo.com.