Security Priorities Study

White paper outlining the 2022 research findings

FOUNDRY

Formerly IDG Communications

Automated digital attacks have been around for decades. (Remember the Confickerbotnet? Storm? EarthLink Spammer, even?) It stands to reason that defenders would need automation to keep up.

Spotting attack signatures isn't the only driver behind the rising trend of automating security tasks. This year's Security Priorities Study respondents —872 security leaders around the world —said automation is increasingly needed to address the challenge of finding, and keeping, skilled security staff. And it's also key to improving incident response too.

This automation comes in many forms. Security Orchestration, Automation and Response (SOAR) is respondents' top-ranked technology category on their radar or that they are actively researching (32%). Extended Detection and Response (XDR), for automated analysis of endpoint and cloud data in particular, ranks fifth on the same list (28%). Identity Threat Detection and Response (ITDR) garners a similar level of interest—that's more automation. "Everything I hear is much more focused on automation and orchestration—not just in SOAR but across everything," says Bob Bragdon, SVP and Managing Director of Foundry's CSO Worldwide, who hosts virtual and live CISO roundtables throughout the year.

In fact, various purveyors of low-code automation tools are already trying to leapfrog what their marketing literature describes as "legacy SOAR solutions." Gartner only coined the term SOAR in 2015, and the A initially stood for Analytics; time-to-legacy must be getting very short in the security product world these days.

But semantics and market jostling aside, automation is a vital theme for 2022. Bragdon notes that it doesn't just replace open job req.

How are IT executives addressing the security skills shortage?

- **45%** Asking current staff to take on more resposibilities
- **45%** Utilizing technologies that automate security practices
- **42%** Outsourcing security functions

"If you're short-staffed, you can't have someone looking at every alert. So how do you get past through the noise and chatter and down to the stuff you reallyneed to look at? And just give that to your Security Operations Center people?" he says. "The SOC team really likes that—it's something they can sink their teeth into, instead of just looking at firewall alerts."

Security incidents, skills gaps, and more: the 2022 Security Priorities Study explores the battle between these challenges and possible solutions, covering budget drivers, future technology plans, risk transfer via outsourcing and cyber insurance, and much more, as security leaders strive to protect and enhance organizational value, for this year and beyond.

Top sources of security incidents

1. Non-malicious user error (**34%**)
2. Security vulnerabilities at third-party individuals or organizations (**28%**)
3. Unpatched software vulnerabilities (**27%**)
4. Misconfiguration of services or systems either on-or off-premises (**26%**)
5. Software supply chain breaches (**17%**)

Incidents and challenges

The technical details of cyberattacks change continually. That said, many of the overall trends in the threat landscape and organizational challenges have continued from previous years. Eliminating user errors and system misconfiguration—easier said than done—would go a long way towards securing corporate data. Supply chain and third-party risks keep inching up.

90% of respondents say they believe their organization is falling short addressing cyber risks; this alarming stat is consistent with last year's results. To help CISOs eventually improve this top-line number, the survey starts by diving into their challenges in more detail.

Most security incidents still stem from mistakes

Non-malicious user error remains the most commonly citedcause of security incidents, but the percentage citing this factor dropped significantly, at 34% this year compared to 44% in 2021. Progress? Perhaps. With Zero Trust continuing to make headway—more on that shortly—it's possible that the impact or "blast radius" of user error is gradually being diminished.

When asked about the reasons for the reported shortfall in overall defensive effort, security leaders cited a wide variety of factors, with eight problems mentioned by at least 20%, but no problem rising above 27%.

Top challenges redirecting security leaders' time

1. Meeting governance & compliance regulations
2. Employee awareness and training issues
3. Unanticipated business risks
4. Preparing for or addressing risks from cyber threats
5. Budgetary constraints/demonstrating ROI

Top reasons include:

- Difficulty convincing all, or parts of our organization, of the severity of the risks we face
- Not investing enough resources (budget, people, technologies, etc.) to address the risks we face
- Struggle to find, acquire, and/or retain the technical or professional expertise we need
- Not proactive enough when it comes to security strategy
- Security is not always addressed during application development
- Inadequate security training for users (full and part-time employees, contractors, or outsourced users)

Others include complex IT and security environments with poor visibility, insufficient communication with lines of business, and new pandemic-related risks associated with remote work. Regarding proactive security strategy, or lack thereof, what tactical concerns distract security teams from thinking and acting in a more strategic manner? Meeting the demands of regulatory compliance is the top.

Budgets, Tech, and Process Priorities

SMB budgets booming

Respondents reported an average security budget of $65M, with enterprises (1,000+ employees) coming in at $122M, and smaller companies at $16M.

SMB budgets look paltry, compared to their larger brethren, but the SMB trajectory over the past three years of this survey is striking: 2020 – $5.5M, 2021 – $11M, 2022 – $16M.

Smaller organizations appear to be investing rapidly to strengthen their security postures.

$65M

Average annual security budget

- **$16M** SMB average annual security budget
- **$122M** Enterprise average annual security budget

Top security priorities for the coming year

How will security leaders allocate their time and all that money in the next year? Improved incident response ranks as the most commonly named priority, which suggests many security leaders have come to terms with the idea that 'breach happens'.

This is where many CISOs will focus improvement efforts. In terms of what drives overall spending, though, respondents continue to rank compliance (cited by 53%) as the top factor—despite wide recognition that regulatory compliance doesn't equal security. Compliance is followed by best practices (49%), then evolving risks resulting from changing business dynamics such as remote work (41%) and from digital transformation efforts such as moving to the cloud (39%).

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

When asked what current security activity was "in production", respondents' said: endpoint security protections for laptops, desktops, servers (51%), endpoint detection and response (48%), patch management (48%), and security awareness training (46%).

When looking at what's currently in production compared to 2021, data related processes and solutions such as data classification rose four percentage points from last year to 33%, data access governance rose two percentage points to 32%; and data analytics rose five points to 32%.

As mentioned earlier, security leaders are planning to spend in the next 12 months. Part of that will be on upgrades to their existing technology. This year, 22% of respondents cited they plan to upgrade/refine their authentication technology (i.e., multifactor, role-based) as well as access controls (i.e., network, data). For data backup and recovery tech, 21% cited plans to upgrade. This is to mitigate the risk from ransomware attacks that are still highly prevalent for all security leaders and businesses today.

Incident response remains a key priority. This year's top security priorities:

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

There were also worries that hybrid work could affect diversity and inclusion efforts, cited by 16% of respondents.

Respondents report piloting and researching a wide range of newer solutions

Security decision makers are thinking about what else to add their tech stack. Respondents to this year's survey cited they are "piloting" Zero Trust technology (16%), behavior monitoring & analysis (14%), and Extended Detection and Response, also known as XDR (13%). Like any new purchase in the tech world, research is done to make sure the solution fits their security needs for 2022 and beyond.

Where Zero Trust stands

33%
In production/ upgrading/refining

16%
Piloting

32%
On my radar/actively researching

19%
Not interested

Top security technologies being actively researched

- Security Orchestration, Automation and Response (SOAR) (**34%**)
- Zero Trust technologies (**32%**)
- Secure Access Service Edge (SASE) (**32%**)
- Deception technologies (**30%**)
- Ransomware broker (**30%**)

Security leaders also shared where they will be increasing their spending this year and next. Cloud-based cybersecurity services lead the pack at 36% of respondents and cloud infrastructure management, application development security, and access controls all at 35%.

Zero Trust still accelerating

Industry prophets were saying "the perimeter is dead" well before the year 2000; Zero Trust has emerged as the name for the model that's (finally) reaching critical mass in replacing the old perimeter-centric approach. Zero Trust architectures and technologies are steadily working their way into corporate security.

One-third of organizations say they have Zero Trust already in place, and more are on the path. The percent of businesses who expect to have Zero Trust architectures in place "in less than a year" rose to 21% this year, compared to 13% in 2021.

Could these numbers reflect a certain abuse of the term Zero Trust? It's possible. Bragdon says he does still encounter people equating Zero Trust with just one component or technology—most often multifactor authentication. However, with NIST's Zero Trust guidance now more than a year old, and other robust vendor frameworks rolling out, the general trend is toward real change, he says.

People and Organization

To meet the full suite of challenges, security needs support from the top. It's good news, then, that the Board of Directors increasingly wants to talk about security. On the other hand, respondents indicate that the challenge of finding qualified staff is holding back their security plans.

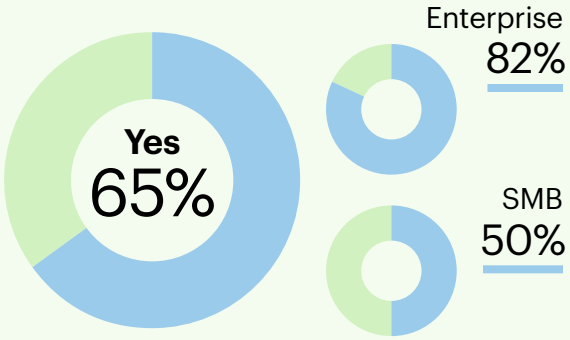
Talking to the top

The vast majority of security leaders, 82%, report regular or frequent engagement with the Board. About one-quarter of respondents (27%) talk to Board Directors multiple times each month, with SMBs (33%) outpacing enterprises (23%) in this area. This is likely because security executives at SMBs are more likely to report to the Board of Directors (26% vs. 15% enterprises).

In terms of reporting relationships, most organizations' dotted and solid lines remained the same in this year's survey. The biggest movement is a drop in CRO reporting relationships, down from 25% last year to just 8% in 2022. Otherwise, reporting relationships for security leaders appear to have arrived at a status quo.

Some loose historical context: In a 2003 "State of the CSO" survey, 26% of respondents reported directly to the CIO/CTO and 12% CEO/President. These numbers aren'tprecisely comparable because the 2021 and 2022 surveys include both direct and indirect reporting relationships. Broadly, though they illustrate that security's status today is worlds beyond where it stood two decades back.

Does your company have a CISO, CSO or top security executive?



Security reporting into the top

	2022	2021
CEO	44%	44%
Corporate CIO	26%	26%
Board of Directors	20%	21%
CFO	10%	7%
Chief Risk Officer	8%	25%

Q: To whom does your security function report, directly or indirectly?

Skills, or lack there of, and what to do about it

A persistent pain point that contributes to outsourcing: respondents note difficulty finding staff." Everyone building out an internal security function is reinventing the wheel, and there aren't enough people for everyone to do that," says Bragdon.

So what are security teams doing about it? As noted up top, automation is a top solution, cited by 45% of respondents overall—highest in North America (48%) and lowest in EMEA (at 37%, which is still that region's third most common answer).

"Put more on everyone's plate", perhaps not a sustainable long-term tactic, also scored 45%, and surprisingly this is even more prevalent at larger companies than at smaller ones: It's the top answer for those with more than 1,000 employees (45%).

There is an argument to be made, and in security community discussions it often is made, that for example, 84% of respondents identified as male, suggesting that women continue to represent an underutilized pool of talent available to help build out the team. Also, "recruit from other parts of the company" ranked a distant fifth, cited by 27% of security leaders. Internal employees already know something about the business, which can counterbalance the need to train them on security skills.

Risk transfer: Outsourcing, cyber insurance grow

Some companies just don't want the hassle. Outsourcing security is a slow-motion wave, still only about one-third of respondents, but advancing a few points in each year's survey.

This year, the meanpercentage of security functions handled in-house dropped to 67%, while the medianscore fell by five points, to 70%. The difference suggests that the companies who do choose outsourcing are moving more aggressively in that direction.

"Each year we see a continued move to the cloud. It's incremental but inexorable," says Bragdon. One CISO recently told Bragdon he wants every person on his internal staff to be a manager: "'I don't want anything run in-house. I want all of it under contract with service providers,with KPIs they have to live up to. And then we manage their performance and their contract.'"

A different form of risk transfer, cyber insurance, has even more traction, with about half of respondents reporting that they now hold a policy or policies. On a scale of 1 (least satisfied) to 10 (most satisfied), respondents' average rating of the insurance process is 7.9—a number that would indicate high satisfaction with this coverage overall."As much as people like to complain about insurance, when you ask the specifics, they're not terribly put out by it," Bragdon says.

The main complaints are what one might expect for any kind of insurance purchase: 49% agree or strongly agree that their policy is too expensive, and 35% agree or strongly agree that the insurance policy process demands too much effort.

Among companies that do have a policy, 17% overall said they have filed a cyber insurance claim, but this varies considerably by size and region. Among enterprises (1,000+ employees), 26% have filed a claim, compared to just 9% of smaller companies. In EMEA, it's 32%, versus 12% of North American companies.

Which industries have filed the most cyberinsurance claims?

33% Financial services
20% Government
22% Healthcare
14% Education
12% Manufacturing
14% Retail
20% High tech

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

Of the security incidents NA organizations experienced last year, 36% were caused by non-malicious user error, 29% security vulnerabilities from 3rd party individuals or organizations, unpatched software vulnerabilities (24%). 86% in NA are aware of what caused their security incidents.

#1 security priority in North America -being appropriately prepared to respond to a security incident

When it comes to top security priorities this year, 50% of North America respondents said theirs is "being appropriately prepared to respond to a security incident" such as ransomware, data breach, etc.

The average annual security budget in NA for 2022 is $68 million. NA security leaders are planning to increase their investments in:

- Cloud-based cybersecurity services (**37%**)
- Access controls (**36%**)
- Authentication (**35%**)
- Cloud infrastructure management technology (**34%**)
- Data backup & recovery (**34%**)

EMEA

In EMEA 88% of respondents are aware of what caused their security incidents this past year. In fact, 33% of EMEA respondents cited the incidents were caused by software supply chain breaches, and 33% said they were due to misconfiguration of services or systems (on or off prem.)

88%

of EMEA security leaders are aware of what caused their security incidents in the past 12 months

EMEA's top security priorities this year:

- upgrading IT and data security to boost corporate resiliency (**43%**)
- improving/increasing security awareness training among end users (**40%**)
- being appropriately prepared to respond to a security incident (**40%**)

EMEA has the lowest average annual budget among the 3 regions at $40.8M -- compared to the global average of $65 million. But EMEA security leaders are still looking to increase their spending in certain areas. Cloud being one of them. They plan to increase their investments in:

- Cloud-based cybersecurity services (**42%**)
- Cloud infrastructure management technology (**42%**)
- Cloud data protection (**40%**)

APAC

90% are aware in APAC and their top incident last year was also non malicious user error (fell victim top phishing or non-malicious violations of security policies), unpatched software vulnerabilities 34%, misconfiguration (30%.)

$90.9 million

APAC average annual security budget

90%

of APAC security leaders are aware of what caused their security incidents in the past 12 months

53% of APAC organizations see being appropriately prepared to respond to a security incident their #1 top priority. Jumping down to second at 40% is upgrading IT and data security to boost corporate resiliency and improve the protection of confidential and sensitive data at 37% for #3.

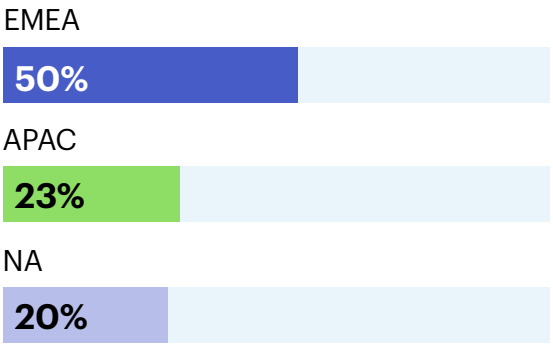
APAC has the highest budget among all three regions this year of $90.9 million. In this region, security decision-makers are looking to increase their investments mainly in cloud infrastructure management technology (33%), cloud data protection (30%), and cloud-based cybersecurity services (30%).

Overall key differences among 3 regions:

EMEA Boards of Directors are highly engaged

Yearly engagement with the Board of Directors

Engages multiple times per month

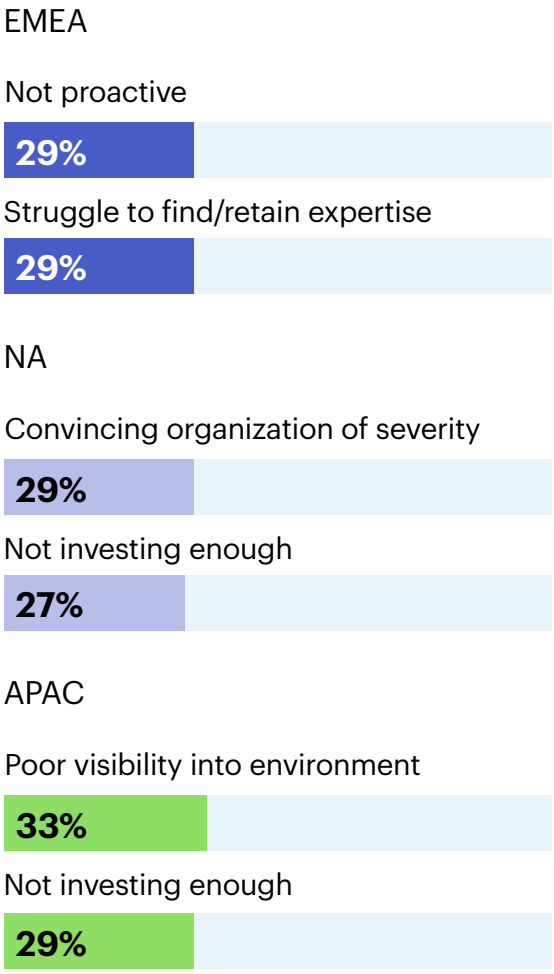


The top overall challenge across all regions, "not investing enough," is heavily influenced by the two regions APAC (where it is cited by 29% of respondents) and NA (27%).

EMEA is quite different, with only 19% named this factor—ranking it only eighth in this region.

Conversely, APAC has a different top shortfall, "visibility into IT environment," which at 33% is higher than any other specific shortfall in any region. Visibility is a middling concern for EMEA (at 22%) and very low for NA (16%).

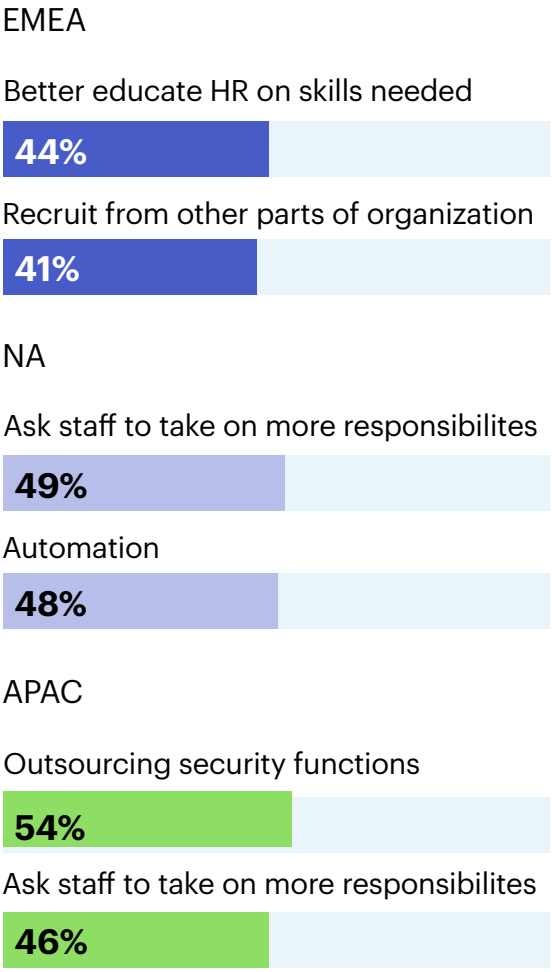
Areas "falling short": Top two answers.



The top approaches to staffing problems hardly overlap across the three regions.

Each region is trying very different approaches to the finding and keeping staff. While NA organizations are somewhat likely to try increasing compensation and benefits (42%), that's much less common in APAC (26%). And EMEA's preference for internal recruiting (41%) barely registers in APAC (13%).

Tactics for addressing the skills gap: top two answers



About the survey

The 2022 Security Priority Study was conducted via online questionnaire from June through August 2022. 872 total respondents with IT and/or corporate security leadership responsibilities were collected from NA (55%), EMEA (18%) and APAC (27%) regions. Top represented industries include technology (25%), manufacturing (13%), government/nonprofit (10%), and financial services (8%). The average company size was 10,991 employees.

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 & Analytics
- Cloud Computing
- Digital Business
- Security 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.