CYBEREDGE GROUP℠

10th ANNIVERSARY

Special Edition

2024 Cyberthreat Defense Report

North America | Europe | Asia Pacific | Latin America | Middle East | Africa

Image created using ChatGPT

<< Research Sponsors >>

PLATINUM

CLOUDFLARE

CYBERARK The Identity Security Company

Google Cloud Security

imperva a Thales company

ISC2

proofpoint. Protect people. Defend data.

GOLD

BLUECAT

Delinea

opentext™

SailPoint

THREATX

tufin

SILVER

axiad

LEGIT SECURITY

netwrix

Phosphorus

PICUS

Reveal security

Table of Contents

Introduction

CyberEdge's annual Cyberthreat Defense Report (CDR) plays a unique role in the IT security industry. Other surveys do a great job of collecting statistics on cyberattacks and data breaches and exploring the techniques of cybercriminals and other bad actors. Our mission is to provide deep insight into the minds of IT security professionals.

A decade after its first edition, the CDR has become a staple among IT security leaders and practitioners by helping them gauge their internal practices and security investments according to those of their counterparts across multiple countries and industries. If you want to know what your peers in IT security are thinking and doing, this is the place to look.

CyberEdge would like to thank our Silver, Gold, and Platinum research sponsors, whose continued support is essential to the success of this report.

Top Five Insights for 2024

Our CDR reports yield dozens of actionable insights. Here are the top five takeaways from this year's installment:

1. **Confidence is building.** Several long-running trends have reversed in the last year or two. Survey data contains multiple indications that security professionals are becoming more confident about their ability to reduce the impact of cyberattacks. The percentage of organizations compromised by cyberattacks fell substantially from the previous survey (page 7), and our respondents expect the number to fall even more this year (page 9). We also saw improvements in our Threat Concern Index (page 18) and Security Concern Index (page 31). The former measures the overall level of concern about cyberthreats, and the latter measures the concern for inhibitors to IT security team success.

Survey Demographics

- **Responses received from 1,200 qualified IT security decision makers and practitioners**
- **All from organizations with more than 500 employees**
- **Representing 17 countries across North America, Europe, Asia Pacific, the Middle East, Latin America, and Africa**
- **Representing 19 industries**

2. **AI is taking center stage.** Artificial intelligence technologies are being incorporated into a very wide range of security solutions. They promise to increase the power of security professionals to detect and block attacks, respond to incidents, and find and remediate vulnerabilities. Security teams are looking at AI as a force multiplier that will make them more productive and effective (page 21). Survey respondents expect AI to be deployed in many ways to both enhance and defeat cybersecurity measures. A plurality thinks the positive and negative outcomes will be in balance. However, of the rest, significantly more believe the benefits to security teams will be greater than the benefits to threat actors, creating an overall "Advantage to Security" (page 25).

3. **Ransomware trends are changing direction.** Several persistent trends related to ransomware have turned around. Compared to our last survey, significantly fewer respondents reported that their organization had been victimized by ransomware. The percentage of affected organizations paying ransoms declined, and so did the number of organizations that paid ransoms and managed to recover their data. The reasons for these changes are complex, but we think we have untangled some of the threads (page 27).

Introduction

4. **Funding for security groups is not a problem.** A record number of security groups expect their budget to increase this year, and the size of the average expected budget increase grew (page 35).
5. **Cybersecurity experts are now sitting on boards.** We found that three out of five organizations have a member of the board of directors with cybersecurity experience. This has tremendous implications for the ways that security leaders and top executives interact (page 51).

About This Report

The CDR is the most geographically comprehensive, vendor-agnostic study of IT security decision makers and practitioners. Rather than compiling cyberthreat statistics and assessing the damage caused by data breaches, the CDR surveys the perceptions of IT security professionals, gaining insights into how they see the world.

Specifically, the CDR examines:

- The frequency of successful cyberattacks in the prior year and optimism (or pessimism) about preventing further attacks in the coming year
- The perceived impact of cyberthreats and the challenges organizations face in mitigating their risks
- The adequacy of organizations' security postures and their internal security practices
- The organizational factors that present the most significant barriers to establishing effective cyberthreat defenses
- Current investments in security technologies and those planned for the coming year
- The health of IT security budgets and the portion of the overall IT budget they consume

By revealing these details, we hope to help IT security decision makers and practitioners gain a better understanding of how their perceptions, concerns, priorities, and defenses stack up against those of their peers around the world. IT security teams can use the CDR's data, analyses, and findings to shape answers to many important questions, such as:

- Where do we have gaps in our cyberthreat defenses relative to other organizations?
- Have we fallen behind in our defensive strategy to the point that our organization is now the "low-hanging fruit" (i.e., likely to be targeted more often due to its relative weaknesses)?
- Are we on track with both our approach and progress in continuing to address traditional areas of concern while tackling the challenges of emerging threats?
- How does our level of spending on IT security compare to that of other organizations?
- Do other IT security practitioners think differently about cyberthreats and their defenses, and should we adjust our perspective and plans to account for these differences?

Another important objective of the CDR is to provide developers of IT security technologies and services with information they can use to better align their solutions with the concerns and requirements of potential customers. Our data can lead to better market traction and success for solution providers, along with better cyberthreat protection technologies for our resolute security professionals.

The findings of the CDR are divided into four sections:

Section 1: Current Security Posture

Our journey into the world of cyberthreat defenses begins with respondents' assessments of the effectiveness of their organization's investments and strategies relative to the

Introduction

prevailing threat landscape. They report on the frequency of successful cyberattacks, judge their organization's security posture in specific IT domains and security functions, and provide details on the IT security skills shortage. The data will help readers begin to assess:

- Whether, to what extent, and how urgently changes are needed in their own organization
- Specific countermeasures that should be added to supplement existing defenses

Section 2: Perceptions and Concerns

In this section, our exploration of cyberthreat defenses shifts from establishing baseline security postures to determining the types of cyberthreats and obstacles to security that most concern today's organizations. The survey respondents weigh in on the most alarming cyberthreats, barriers to establishing effective defenses, and high-profile issues such as ransomware and security for hybrid cloud environments. These appraisals will help readers think about how their own organization can best improve cyberthreat defenses going forward.

Section 3: Current and Future Investments

Organizations can ill afford to stand still when it comes to maintaining effective cyberthreat defenses. IT security teams must keep pace with changes occurring in business, technology, and threat landscapes. This section of the survey provides data on the direction of IT security budgets, and on current and planned investments in network security, endpoint security, application and data security, and security management and operations. Readers will be able to compare their organization's investment decisions against the broad sample and get a sense of what "hot" technologies their peers are deploying.

This year we added a special three-question section on positive and negative outcomes expected when security teams and threat actors deploy AI.

Section 4: Practices and Strategies

Mitigating today's cyberthreat risks takes more than investing in the right technologies. You must ensure those technologies are deployed optimally, configured correctly, and monitored adequately to give your organization a fighting chance to avoid being a front-page news story. In the final section of the survey our respondents provide information on how they are deploying and using leading-edge technologies and services such as security analytics and IT security delivered from the cloud. We also look at how IT security training and professional certification can help enterprises address the serious shortfall in skilled IT security staff.

Navigating This Report

We encourage you to read this report from cover to cover, as it's chock full of useful information. But there are three other ways to navigate through this report, if you are seeking out specific topics of interest:

- **Table of Contents.** Each item in the Table of Contents pertains to specific survey questions. Click on any item to jump to its corresponding page.
- **Research Highlights.** The Research Highlights page showcases the most significant headlines of the report. Page numbers are referenced with each highlight so you can quickly learn more.
- **Navigation tabs.** The tabs at the top of each page are clickable, enabling you to conveniently jump to different sections of the report.

Contact Us

Do you have an idea for a new topic that you'd like us to address next year? Or would you like to learn how your organization can sponsor next year's CDR? We'd love to hear from you! Drop us an email at research@cyber-edge.com.

Research Highlights

Current Security Posture

- **Yes, some things *are* getting better.** The percentage of organizations compromised by successful attacks declined for the third consecutive year (page 7).
- **Crazy optimistic about 2024.** The percentage of security professionals who think a successful attack is likely or very likely has fallen by 9.4% over two years, to 66.7% (page 9).
- **ICS and IoT are concerns.** Respondents are confident their organization can defend against attacks on SaaS applications and servers but are worried about application containers and industrial systems (page 11).
- **Doubts about four security functions.** Many respondents think their organization needs to improve app testing and development, detection of rogue insiders, user security awareness, and third-party risk management (page 13).
- **Still can't hire enough.** Despite recent layoffs at tech firms, enterprises are still facing a daunting shortage of experienced IT security people (page 15).

Perceptions and Concerns

- **Feeling better about threats.** Security teams are concerned about a lot of threats, but their level of concern for all 13 threat types has fallen (page 17).
- **Everyone experiences web and mobile attacks.** Web and mobile attacks don't just plague financial firms and online retailers – they affect nine out of 10 organizations (page 19).
- **AI will help the good guys.** Our respondents think AI technologies will be force multipliers for security teams (page 21).
- **AI will help the bad guys.** The respondents are also aware that threat actors will be employing AI for a wide variety of malicious activities (page 23).
- **AI advantage to security?** On balance, 50% more security professionals believe that AI will help the good guys than believe it will help the bad guys (page 25).
- **Ransomware U-turns.** Several ransomware trends have changed direction: fewer organizations were victimized, fewer ransoms were paid, and less data was recovered (page 27).
- **People problems.** The biggest barriers to successful cyber defense are people related: low security awareness among employees and lack of skilled security personnel (page 30).
- **Happiness can be (relatively) cheap.** Some factors that improve job satisfaction and employee retention are expensive, but other effective incentives aren't (page 32).
- **Security training works.** 87% of respondents agree that IT security training helps them do their jobs better (and only 3% disagree) (page 34).

Current and Future Investments

- **Security budgets are rising.** The mean annual increase in IT security budgets reached a record high of 5.7% (page 35).
- **A new king of the hill in network security.** Secure web gateways replaced advanced threat protection products as the most frequently installed network security technology (page 37).
- **Endpoint security workhorses.** Anti-malware, DLP, EDR, and EPP solutions are the most popular endpoint security products (page 39).
- **Three must-haves.** The "must-have" solutions for application and data security are database firewalls, web application firewalls, and API protection products (page 41).
- **AD for ZT.** For the third year running, Active Directory protection tops the list of security management and operations technologies. If you can't trust Active Directory, you can't trust your zero trust implementation (page 43).

Practices and Strategies

- **Put the Sec in DevSecOps.** Development groups are recognizing that security and DevSecOps practices really matter (page 45).
- **Partly cloudy forecast.** The percentage of security applications delivered from the cloud is growing, but acceptance varies widely by country and by industry (page 47).
- **Many uses for threat intelligence.** Security teams are finding many ways to leverage external threat intelligence (page 49).
- **Cybersecurity savvy on boards.** A surprising number of organizations (62.2%) have at least one member of the board of directors with a cybersecurity background (page 51).
- **Way past hype.** Nine relatively new technologies and architectures are in use or being implemented by at least 70% of organizations (page 53).

Section 1: Current Security Posture

Past Frequency of Successful Cyberattacks

How many times do you estimate that your organization's global network has been compromised by a successful cyberattack within the past 12 months?

In the 2023 CDR report, we said that IT security teams may have reached a turning point. After successful attacks increased steadily year after year, the curve seemed to have flattened out, and even started to reverse. Perhaps there is room for optimism, we thought. Perhaps we are not doomed to an endless cycle of bad news.

Well, our latest data strongly confirms that positive change in direction. The precentage of organizations compromised at least once by a successful cyberattack in the previous 12 months edged down from 86.2% in the 2021 CDR, to 85.3% in 2022, to 84.7% in 2023. In this survey, the decrease was more substantial, falling 3.2% to 81.5% (see the blue bars in Figure 1). While that is still high by historical standards, it shows that the tide has definitely turned.

Even more striking, the percentage of organizations experiencing six or more successful attacks dropped a whopping 11.2%, from 39.2% to 27.8% (see Figure 2 and the red bars in Figure 1). We haven't seen a figure that low since 2018.

It's too early to start celebrating, though. Organizations of all sizes are still exposed to thousands of low-level attacks every day. The financial, regulatory, and reputational costs of data breaches continue to rise. Ransom payments have soared as well (see page 28). But cybersecurity professionals can take satisfaction in the fact that they're blocking more attacks than in any year since 2020.

What is causing this turnaround? We suggest several factors:

- A significant number of work-from-home (WFH) employees returning to offices, where their devices are better protected from cyberattacks

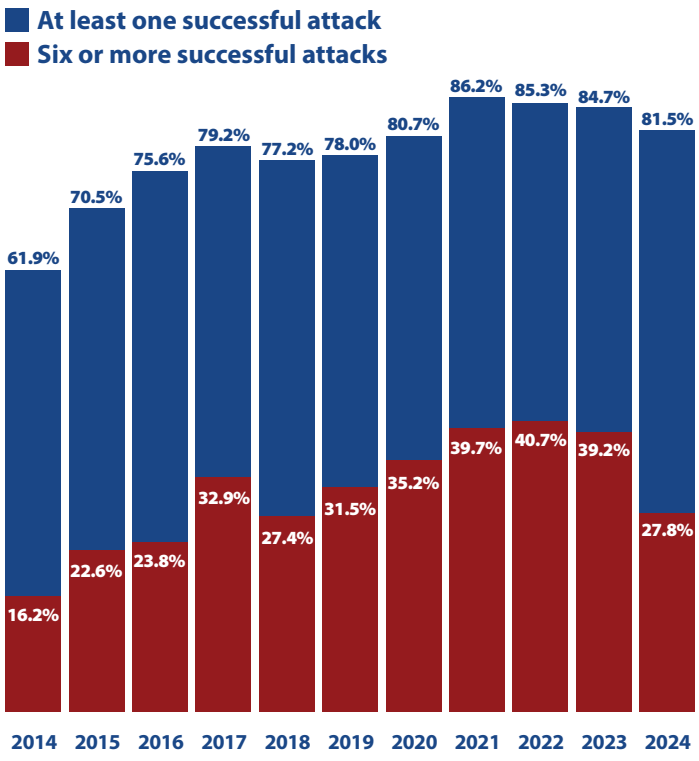


Figure 1: Percentage of organizations experiencing at least one successful attack and those experiencing six or more.

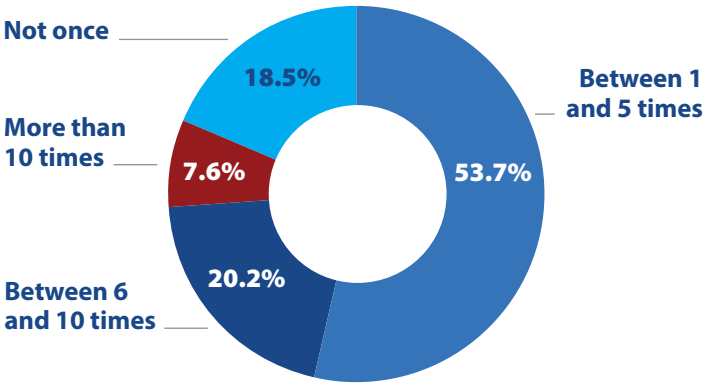


Figure 2: Frequency of successful cyberattacks in the past 12 months.

Section 1: Current Security Posture

- The payoff from large investments in zero trust, cloud security tools, advanced authentication, extended detection and response (XDR), and other innovative cybersecurity technologies (see page 53)
- More attention to basic security hygiene (vulnerability detection and patching), including investments in risk-based vulnerability management (RBVM) and cyber exposure management solutions
- Increased applications of AI and machine learning (ML) to cybersecurity tools (see pages 21-26).
- More investment in security awareness training for users and professional training for cybersecurity staffs
- More-effective cooperation between government law enforcement agencies, industry groups, and individual enterprises

It's worth keeping in mind that mileage may vary. The prevalence of successful attacks is not uniform across the globe or among industries.

For example, you might want to think twice before accepting a cybersecurity job in Mexico. A full 97% of organizations reported at least one compromise last year, and about half (52%) suffered six or more. Other countries where at least 85% of organizations experienced a successful attack were South Africa (89.6%), Colombia (87.5%), Spain (87.5%), and Brazil (85.3%). At the other end of the spectrum, 75.5% of Australian organizations reported one or more successful attacks, along with 72.9% of Japanese and 70.0% of Italian organizations (see Figure 3).

Of the major industries tracked in our survey, financial institutions suffered most frequently from successful attacks (presumably "because that's where the money is"), followed by telecom & technology firms, while manufacturing and retail were least affected (see Figure 4).

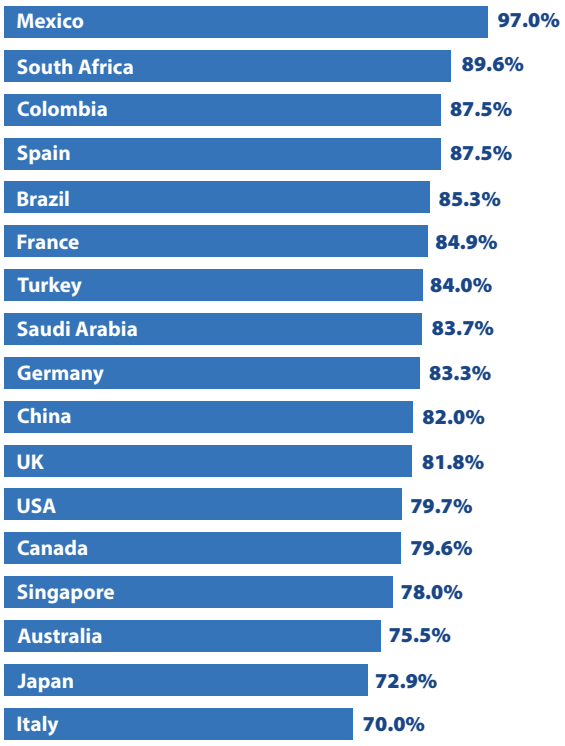


Figure 3: Percentage of organizations compromised by at least one successful attack in the past 12 months, by country.

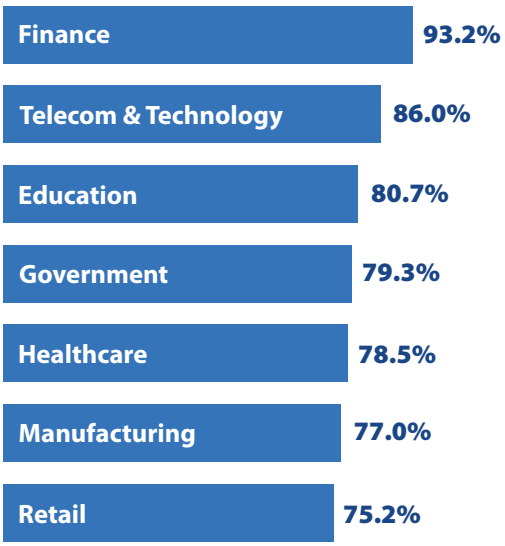


Figure 4: Percentage of organizations compromised by at least one successful attack in the past 12 months, by industry.

Future Likelihood of Successful Cyberattacks

What is the likelihood that your organization's network will become compromised by a successful cyberattack in 2024?

The positive trend we noted in the previous section extends to expectations for the coming year. The percentage of survey respondents who think a successful attack in 2024 is somewhat or very likely fell a substantial 5.1%, from 71.8% to 66.7%. The decline over two years, from the 2022 report to this one, is 9.4% (see the blue bars in Figure 5).

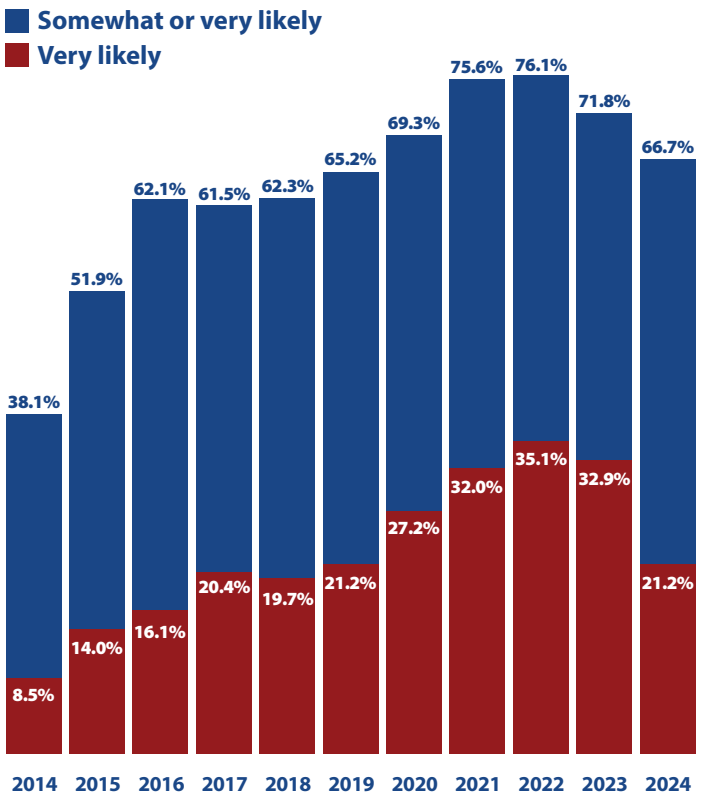


Figure 5: Percentage of organizations indicating that compromise by a successful cyberattack in 2024 is somewhat or very likely.

The pattern continues for those saying that one or more successful attacks are very likely. Their number dropped precipitously, from 32.9% to 21.2%.

These figures do raise an interesting question. If 81.5% of organizations experienced at least one compromise last year (Figure 1), is it reasonable that only 66.7% will undergo the same fate this year (Figure 5)? Optimism is a good thing. As the poet Alexander Pope wrote: "Hope springs eternal in the human breast." However, we think these forecasts involve a bit of wishful thinking.

When breaking down the predictions by country, it is interesting to note that those expecting the greatest number of successful attacks this year are all in Asia: China (84.0%), Singapore (81.6%), and Japan (79.2%) (see Figure 6). The least pessimistic are France (58.9%), Italy (57.1%), and South Africa (46.0%).

And maybe you do want to accept that job in Mexico, at least if you enjoy working with optimists. Although 97.0% of our respondents in Mexico reported being compromised last year, only 62.5% think the same thing will happen in 2024.

"Optimism is a good thing. As the poet Alexander Pope wrote: 'Hope springs eternal in the human breast.' However, we think these forecasts involve a bit of wishful thinking."

Section 1: Current Security Posture

When looking at organizations by size, the most worried respondents come from large enterprises with 10,000-24,999 employees. Almost three-quarters of respondents in that group (72.0%) expect one or more successful attacks.

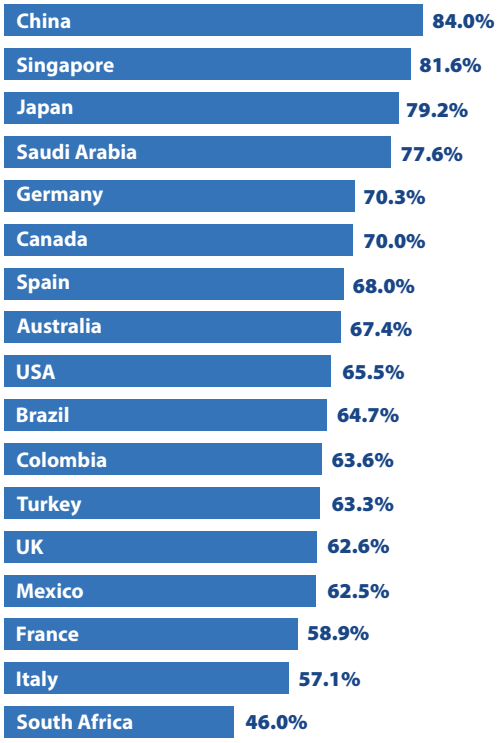


Figure 6: Percentage of organizations indicating that compromise by a successful cyberattack in 2024 is somewhat or very likely, by country.

Those in our other size categories, both smaller and larger, are a touch more optimistic, falling in the 64%-67% range (see Figure 7). We find that pattern in some of the other data as well. Organizations in the 10,000-24,999 employee range make very tempting targets for cybercriminals (for example, they have the deep pockets to pay large ransoms), but don't have quite the ultra-sophisticated defenses and specialized cybersecurity experts as the largest global enterprises.

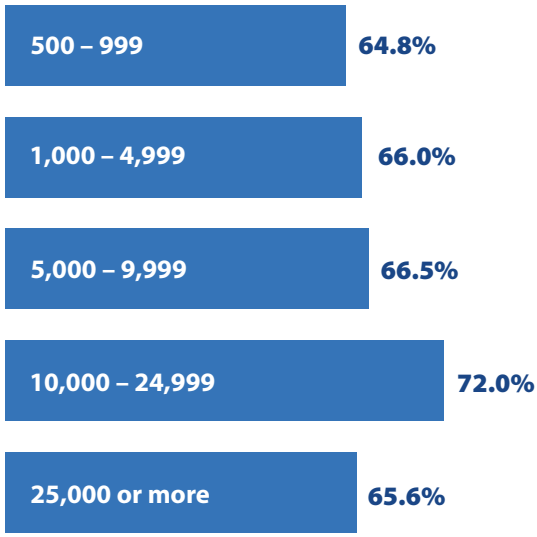


Figure 7: Percentage of organizations indicating that compromise by a successful cyberattack in 2024 is somewhat or very likely, by employee count.

Section 1: Current Security Posture

Security Posture by IT Domain

On a scale of 1 to 5, with 5 being highest, rate your organization's overall security posture (ability to defend against cyberthreats) in each of the following IT components:

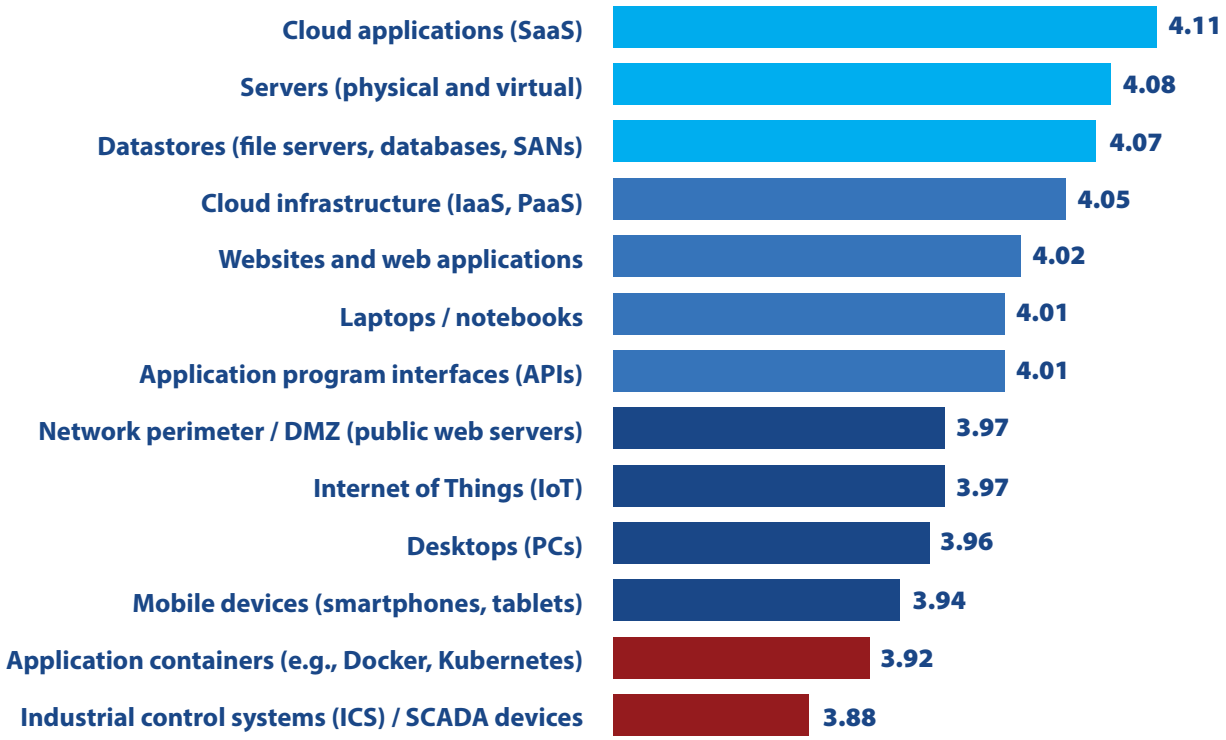


Figure 8: Perceived security posture by IT domain.

We asked the survey respondents to rate their organization's ability to defend itself across 13 IT domains.

Our security professionals were most comfortable about the security of SaaS applications, with a score of 4.11 (on a scale of 1 to 5, with 5 being the best possible security posture). This reflects a high level of confidence in SaaS vendors and their ability to protect cloud-based software. It's also a nod to the 91.6% of organizations that have already deployed SaaS security posture management (SSPM) solutions or are in the process of doing so (see page 53).

Respondents are also relatively satisfied with defenses for servers (4.08) and datastores such as file servers, databases, and storage area networks (4.07). In fact, datastores is one of only three areas where confidence increased from last year (more on that in a minute).

Section 1: Current Security Posture

At the opposite end of the list, industrial control systems (ICS)/SCADA devices remained the area with the lowest score for security posture (3.88). Security professionals continue to be concerned about the potential for attacks on manufacturing and operations technologies (OT), a lack of security solutions for that realm, and the challenges of integrating OT security with traditional data security. They may also be on edge because of the potential for attacks on industrial infrastructure as an outgrowth of national and regional conflicts (see page 59).

"A significant change from past years is the increase in concern about protecting application workloads in Docker and Kubernetes containers... This trend likely reflects a combination of the growing use of containerization for key applications and increased targeting of these workloads by threat actors."

A significant change from past years is the increase in concern about protecting application workloads in Docker and Kubernetes containers. This area fell from sixth place last year to twelfth in this survey. In fact, the score for containers decreased by .14, from 4.06 to 3.92, the biggest drop for any IT domain. This trend likely reflects a combination of the growing use of containerization for key applications and increased targeting of these workloads by threat actors.

Speaking of lower scores, this year confidence in security posture dropped in 10 of the 13 domains. That doesn't mean that there have been more successful attacks on those targets. Rather, it implies that, in the continuing parallel arms races in different areas of IT security, security professionals know they need to be increasingly vigilant if they want to stay ahead of the bad guys.

On the other hand, there was one positive surprise. Internet of Things (IoT) devices have been one of the top three areas of concern for several years. In this survey, they fell back to fifth from the bottom. Their score actually improved slightly from last year, going from 3.95 to 3.97. This reflects the introduction of new security solutions for IoT, as well as the ability of existing security product vendors to monitor and protect IoT devices.

Section 1: Current Security Posture

Assessing IT Security Functions

On a scale of 1 to 5, with 5 being highest, rate the adequacy of your organization's capabilities (people and processes) in each of the following functional areas of IT security:

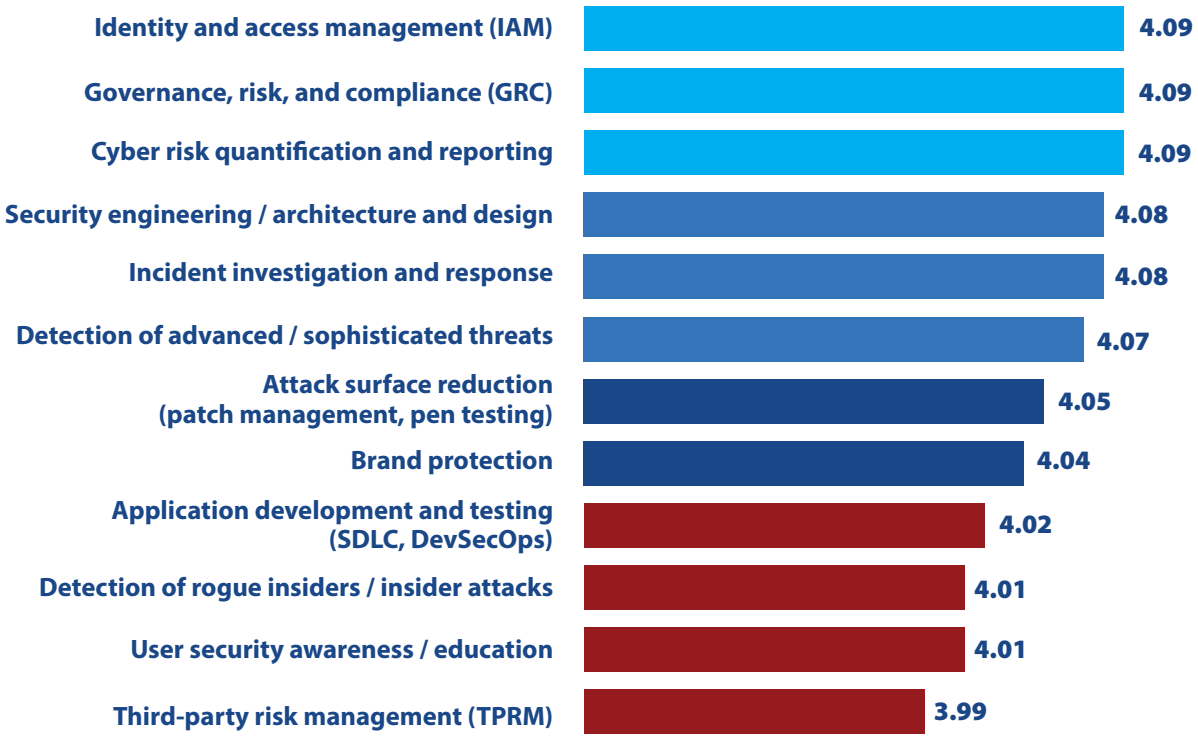


Figure 9: Perceived adequacy of functional security capabilities.

Confidence in the adequacy of defenses across functional areas of IT security fell significantly this year, declining in 11 of the 12 categories tracked.

The decline in scores was moderate in the categories at the top of the list. For example, the score for identity and access management (IAM) fell from 4.13 to 4.09, but that function continued in a tie for having the most satisfactory people and processes (see Figure 9).

Two other areas of IT security moved way up on the list this year. Governance, risk, and compliance (GRC) and cyber risk quantification and reporting jumped from sixth place and eighth place, respectively, to a three-way tie for first with IAM. Recently, enterprises have started putting a lot more emphasis on GRC and risk quantification. Part of this focus is attributable to evolving government regulations and industry standards that demand better governance and risk management. Part is

Section 1: Current Security Posture

due to CEOs and boards of directors now being held directly accountable for cybersecurity incidents, and therefore getting involved in IT security investment decisions. And part may be a result of boards of directors now including members with cybersecurity experience (see page 51).

However, the most striking finding for this question is the relative loss of confidence in the adequacy of security capabilities for the four functional areas at the bottom of the list.

Application development and testing (SDLC and DevSecOps) fell from second place last year, with a score of 4.13, to ninth in this survey, with a score of 4.02. Detection of rogue insiders dropped from fourth (score: 4.13) to tenth (score: 4.01).

The bottom two items on the list only slipped one place each from last year, but their scores declined significantly: user security awareness and education from 4.08 to 4.01 and third-party risk management (TPRM) from 4.07 to 3.99.

We don't think that defenses in these functions have objectively gotten worse, but security professionals are becoming more concerned that they are falling behind the pace of innovation shown by threat actors. Also, more organizations may have recognized the increased importance of improving application security, detecting insider attacks, educating users, and detecting malware in purchased devices and software, and decided that their existing defenses in these functions need improvement.

"Recently, enterprises have started putting a lot more emphasis on GRC and risk quantification. Part of this focus is attributable to evolving government regulations and industry standards... [part] is due to CEOs and boards of directors now being held directly accountable for cybersecurity incidents, and... part may be a result of boards of directors now including members with cybersecurity experience."

Section 1: Current Security Posture

The IT Security Skills Shortage

Select the roles/areas for which your organization is currently experiencing a shortfall of skilled IT security personnel. (Select all that apply.)

The security skills shortage is persistent, widespread, and consequential.

Our data indicates that the shortage of skilled IT security personnel eased a touch over the last 12 months but remains at high levels. As shown in Figure 10, the percentage of organizations experiencing a shortfall in at least one role fell slightly, from 86.6% to 85.8%, but that is still the third-highest figure since we started asking this question.

A similar picture emerges when we look at specific jobs (see Figure 11). For every security role in our survey, between a quarter and just over a third of organizations have openings they can't fill.

IT security administrators are the most sought-after (there is a shortfall in 35.4% of organizations). Close behind are IT security analysts, operators, and incident responders (32.4%) and IT security architects and engineers (32.3%). And almost as many organizations have vacancies in the remaining roles: IT security and compliance auditors (26.1%), DevSecOps engineers (25.6%), risk and fraud analysts (25.0%), and application security testers (24.6%). These numbers are all down from last year, but they are roughly in line with the findings from our 2020 and 2021 reports.

We think the modest declines are related to the workforce reductions in high-tech companies. Layoffs in large technology firms, including Amazon, Alphabet (Google), Microsoft, Meta (Facebook), Salesforce, LinkedIn, Discord, Snapchat, SAP, Spotify, and others, have made the news. Also, many medium-size and small businesses have cut staff to reduce expenses. Although many are retaining their cybersecurity experts, not all have been spared from the carnage.

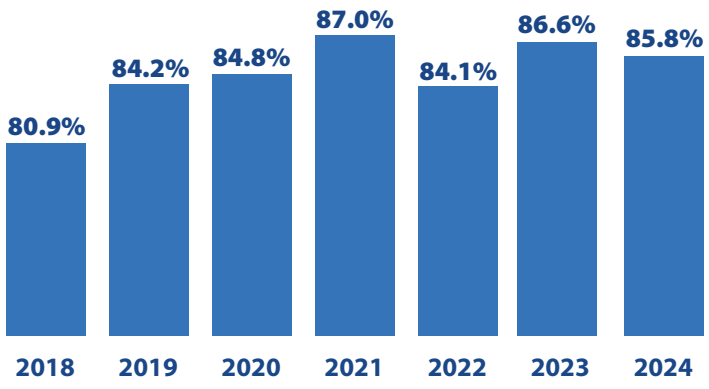


Figure 10: Percentage of organizations experiencing a shortfall of skilled IT security personnel in at least one role.

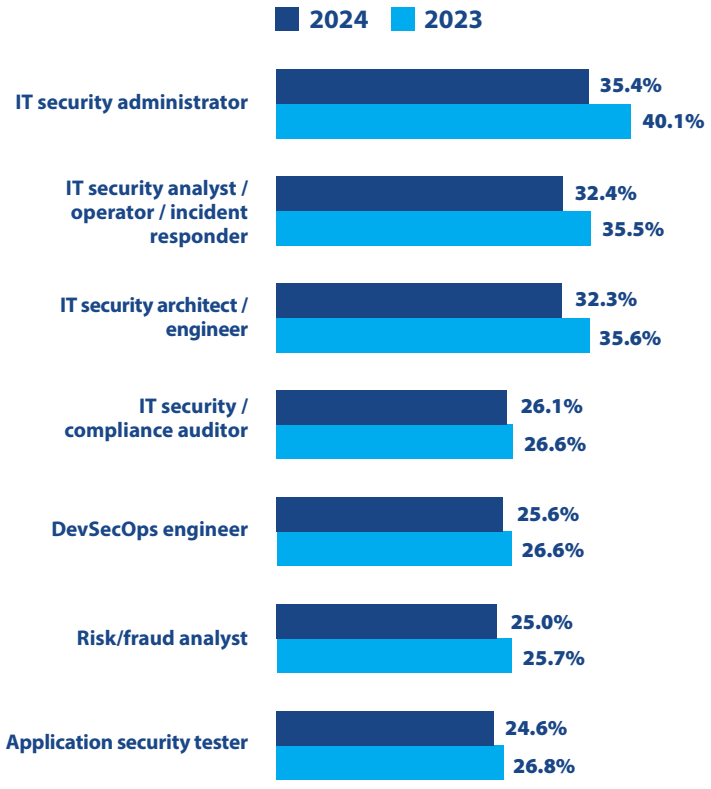


Figure 11: Cybersecurity skills shortage, by role.

Section 1: Current Security Posture

Are tech industry layoffs a bad sign for security professionals? And conversely, are they a good sign for hiring managers desperately trying to fill vacancies? We wouldn't advise anyone to get too excited, at least in the short term, because there is still a massive deficit in qualified staff. According to the 2023 ISC2 Cybersecurity Workforce Study, in 2023 the gap between the number of cybersecurity professionals that organizations require to defend themselves and the number of such personnel available actually increased by 12.6% worldwide – and 19.7% in North America.

"Are tech industry layoffs a bad sign for security professionals? And conversely, are they a good sign for hiring managers desperately trying to fill vacancies? We wouldn't advise anyone to get too excited, at least in the short term, because there is still a massive deficit in qualified staff."

Now, in the medium and long term, AI may have a significant impact on the shortage by increasing the productivity of cybersecurity workers, and perhaps even making some job descriptions obsolete. We discuss that hypothesis in The Road Ahead section of this report, on page 58.

Why did we say that the security skills shortage is consequential? You can see the evidence on page 30, which shows that a lack of skilled IT security personnel is currently the second-biggest factor inhibiting organizations from adequately defending themselves, second only to low security awareness among employees. It has been the #1 or #2 factor for eight years now.

Section 2: Perceptions and Concerns

Concern for Cyberthreats

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyberthreats targeting your organization.

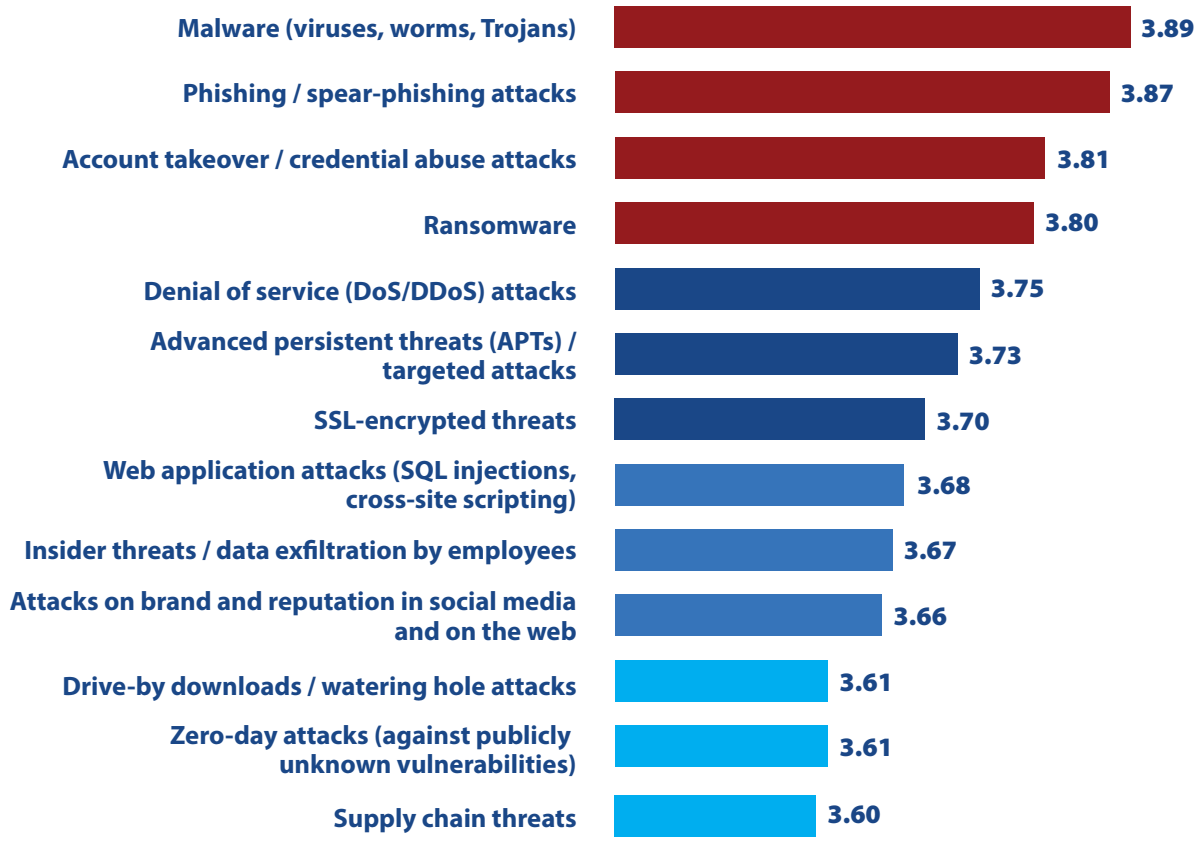


Figure 12: Relative concern for cyberthreats.

In every survey we ask our respondents to quantify their concern about a range of cyberthreats. This year's results provided more data indicating that their attitudes have changed decisively in a positive direction. Their overall level of concern decreased for every one of the 13 cyberthreats included in the question.

The "big four" cyberthreats continued to be malware (with a score of 3.89, on a scale of 1 to 5, with 5 being extremely concerned), phishing (3.87), account takeover and credential abuse attacks (3.81), and ransomware (3.80) (see Figure 12). These were in the same order as last year, except that phishing and account takeover swapped the #2 and #3 spots.

Section 2: Perceptions and Concerns

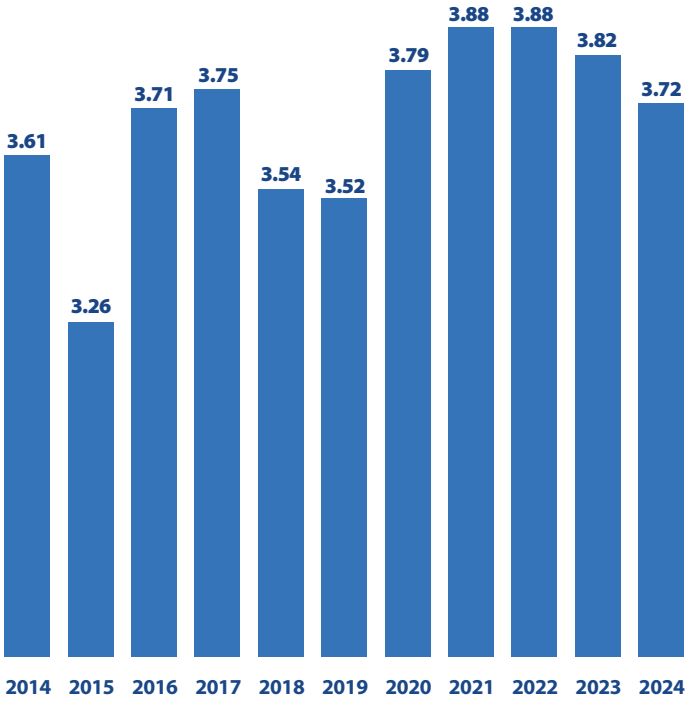


Figure 13: Threat Concern Index, depicting overall concern for cyberthreats.

"In every survey we ask our respondents to quantify their concern about a range of cyberthreats. This year's results provide more data that their attitudes have changed decisively in a positive direction. Their level of concern decreased for every one of the 13 cyberthreats included in the question."

However, the scores for account takeover attacks and ransomware declined substantially compared to typical year-to-year movements on this question. The score for account takeover attacks fell by .14 and ransomware declined by .10.

Given the heavy press coverage of ransomware, this last figure might seem surprising. But you can find the explanation on pages 27-29. Although the median ransom amount increased substantially last year, the percentage of organizations affected by a ransomware attack, and the percentage paying a ransom, both decreased.

Denial of service attacks, advanced persistent threats, SSL-encrypted threats, web application attacks, insider threats, and attacks on brand and reputation continued to be serious concerns, with scores between 3.66 and 3.75. However, except for the first, those scores declined between .08 and .13 from the last survey. Denial of service attacks were the exception, down only .02.

What do these declines add up to? Every year we average the concern scores for all the cyberthreat types into what we call our Threat Concern Index. As shown in Figure 13, the overall concern for cyberthreats has fallen for two years running, from a record high of 3.88 in the 2022 CDR, to 3.82 in the 2023 edition, to 3.72 this year.

Last year we attributed the decrease in the Threat Concern Index to workers returning to offices with more security in place than in homes, increased investment by organizations in ML, AI, and other advanced technologies, and the widespread implementation of zero trust frameworks. We think those are still the primary drivers of the more-positive attitude we see in this data.

Section 2: Perceptions and Concerns

Concern for Web and Mobile Attacks

Which of the following attacks on your web and mobile applications are most concerning? (Select up to three.)

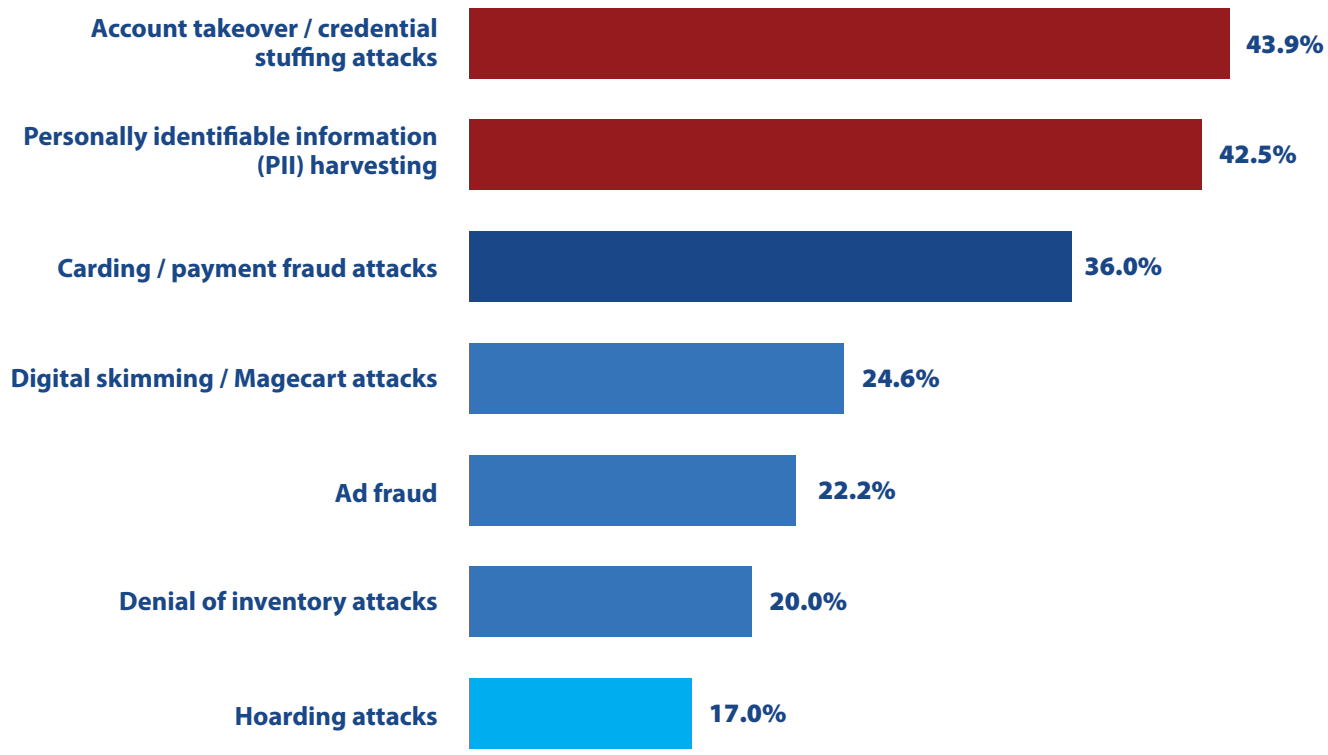


Figure 14: Most-concerning web and mobile application attacks.

Web and mobile application attacks are particularly menacing to enterprises that transact business on the web and through mobile apps, especially financial institutions and retailers that can lose substantial sums to online fraud. But these attacks can affect any organization that handles customer, client, or constituent data. Threat actors employ web and mobile application attacks to steal credentials and personal information, which they can then use to impersonate victims to carry out data breaches, identity theft, and other crimes. The problem is made worse when people reuse the same passwords for multiple personal and work accounts.

We asked respondents to select the three web and mobile application attacks that most concern them (or to say that their organization is not affected by any of these attacks). The results are shown in Figure 14.

What did we learn? In this group, the greatest concern today is account takeover (ATO) and credential stuffing attacks, which use stolen and leaked passwords and email addresses to break into networks and applications. These were cited by 43.9% of the respondents. This was a substantial increase from last year's figure

Section 2: Perceptions and Concerns

of 40.2% (an increment of 3.7%, to be precise). The widespread use of these attacks is prompting more consumer- and client-facing organizations to adopt two-factor and passwordless authentication methods, despite the added inconvenience to users.

Attacks that harvest personally identifiable information (PII) moved down from first place in the last survey to second in this one. However, the number of citations was essentially the same (42.5% versus 42.3%), indicating that worries about these threats have not abated.

The other five attack types maintained the same order as in the last report. The biggest change was a reduction in the percentage of respondents citing digital skimming and Magecart attacks, which fell 4.8%, from 29.4% of organizations to 24.6%.

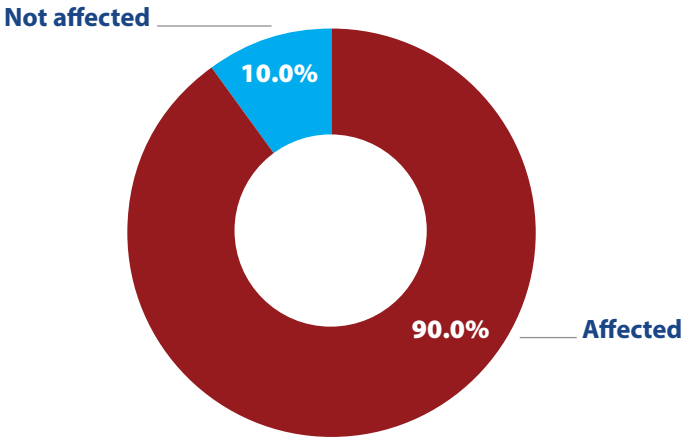


Figure 15: Organizations affected by a web or mobile application attack.

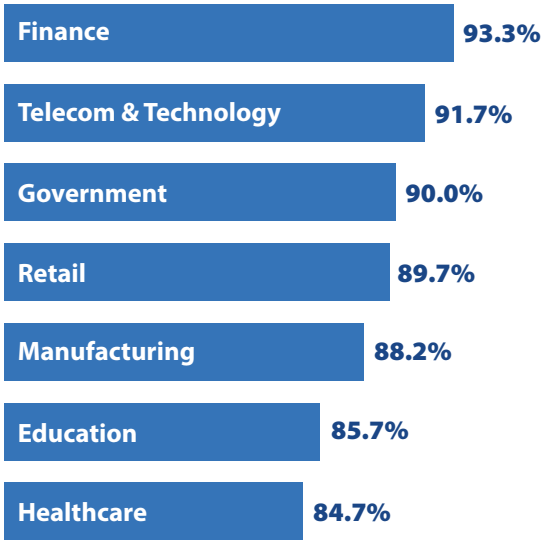


Figure 16: Organizations affected by a web or mobile application attack, by industry.

We mentioned that web and mobile application attacks can harm any organization that interacts with customers, clients, or constituents. And that turns out to be nearly all of them. As shown in Figure 15, 90.0% of organizations have been threatened by these attacks.

In fact, when we break down results by line of business, the distance between the most affected major industries – finance and telecom & technology – and the least affected – education and healthcare – is less than 9% (see Figure 16).

Section 2: Perceptions and Concerns

Positive Outcomes of AI

Cybersecurity industry analysts predict that advancements in artificial intelligence (AI), including machine learning (ML) and generative AI (e.g., ChatGPT), will benefit IT security teams. Which of the following positive outcomes of AI do you predict will impact your organization the most? (Select up to three.)

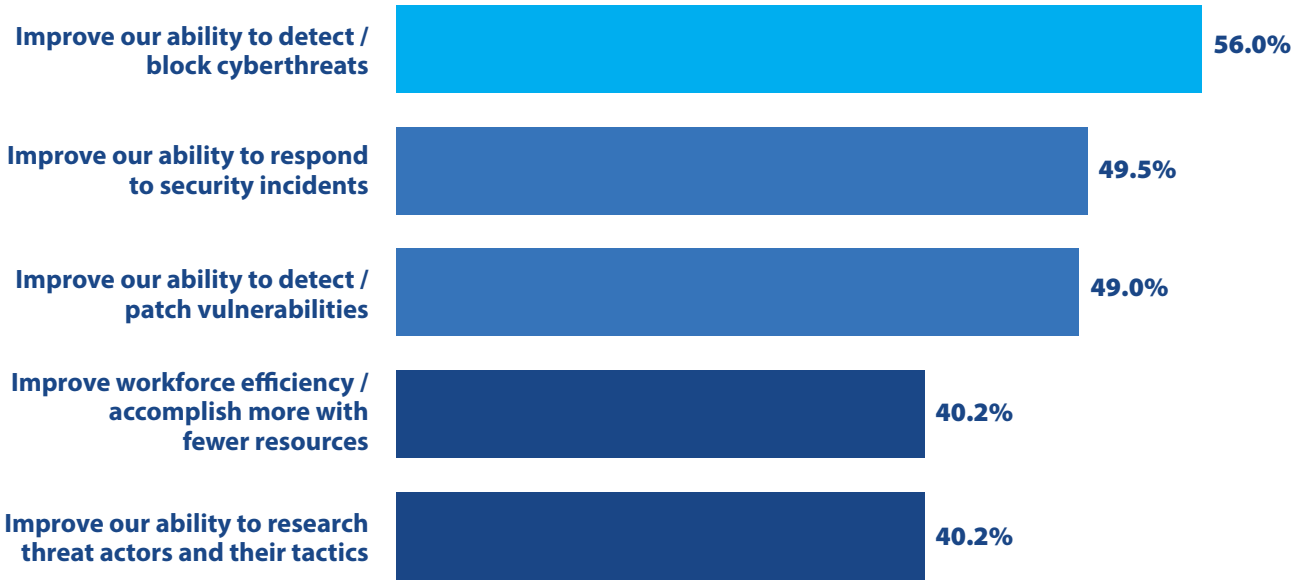


Figure 17: Positive outcomes for security teams from AI.

One of the hottest topics in technology right now is artificial intelligence. People are wondering, will AI be a boon or a bane? Will it become a valuable servant of humanity, or a malicious overlord bent on destroying our species? And most important, how will it affect my job?

We are just as curious as the next person, so we added a special three-question section about AI to this survey. We asked how AI technologies will enhance the work of security teams, how it will be employed by threat actors, and whether on balance AI will benefit security teams or threat actors more.

When asked to select the top three ways technologies such as ML and generative AI will benefit IT security teams, the most common response, by a wide margin, was "Improve our ability to detect/block cyberthreats." This was selected by 56.0% of our respondents (see Figure 17). At a time when attack surfaces are expanding and threat actors are bombarding our networks with an endless variety of probes and assaults, defenders are looking to AI to sort through mountains of hay to find, prioritize, and where appropriate, swiftly block, the hidden needles.

Section 2: Perceptions and Concerns

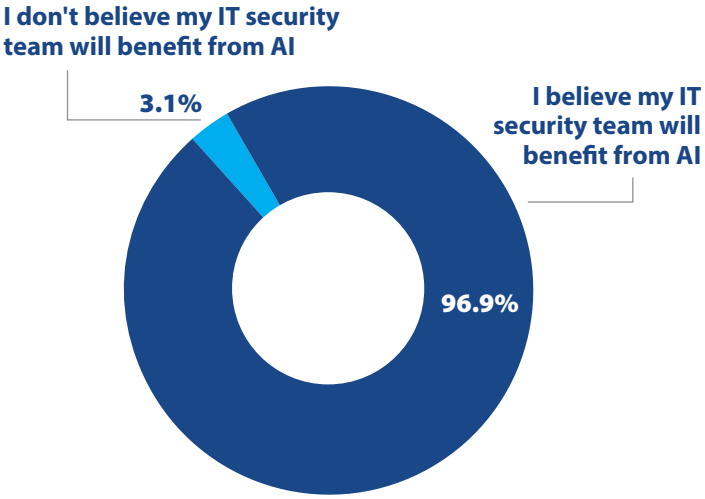


Figure 18: Belief that security teams will benefit from AI.

In second place, selected by about half of respondents, is "Improve our ability to respond to security incidents" (49.5%). Incident response often involves sifting through a great deal of information to figure out what systems have been affected, what changes have been made and actions taken by attackers, and what steps to take to contain attacks. AI can certainly help security teams perform that work faster and more accurately, potentially before attacks do any damage.

The third item on the list is "Improve our ability to detect/patch vulnerabilities" (49.0%). This is another security area that involves a lot of data analysis and pattern recognition, and AI technologies can greatly increase their effectiveness.

Next comes "Improve workforce efficiency/accomplish more with fewer resources," selected by two of five respondents (40.2%). It reflects the hope that AI technologies can be a force multiplier for overworked security teams, making them more efficient and productive. This outcome would go a long way toward mitigating the cybersecurity skills shortage that has plagued IT groups for many years (page 15).

Rounding out the selections, also at 40.2%, is "Improve our ability to research threat actors and their tactics." Again, this view speaks to the ability of AI technologies to recognize patterns in large masses of data.

The fact that all five benefits were selected by at least 40% of the respondents shows that AI technologies are going to be applied across a wide spectrum of cybersecurity use cases, not just in one or two niches.

Our data also reveals that AI skeptics are rare. Only 3.1% of respondents selected "I don't believe my IT security team will benefit from AI" (see Figure 18).

"People are wondering, will AI be a boon or a bane? Will it become a valuable servant of humanity, or a malicious overlord bent on destroying our species? And most important, how will it affect my job? We are just as curious as the next person, so we added a special three-question section about AI to this survey."

Section 2: Perceptions and Concerns

Negative Outcomes of AI

Cybersecurity industry analysts also predict that advancements in artificial intelligence (AI), including nefarious chatbots (e.g., WormGPT, FraudGPT, DarkBART), will improve how cyberthreat actors operate. Which of the following negative outcomes of AI do you predict will impact your organization the most? (Select up to three.)

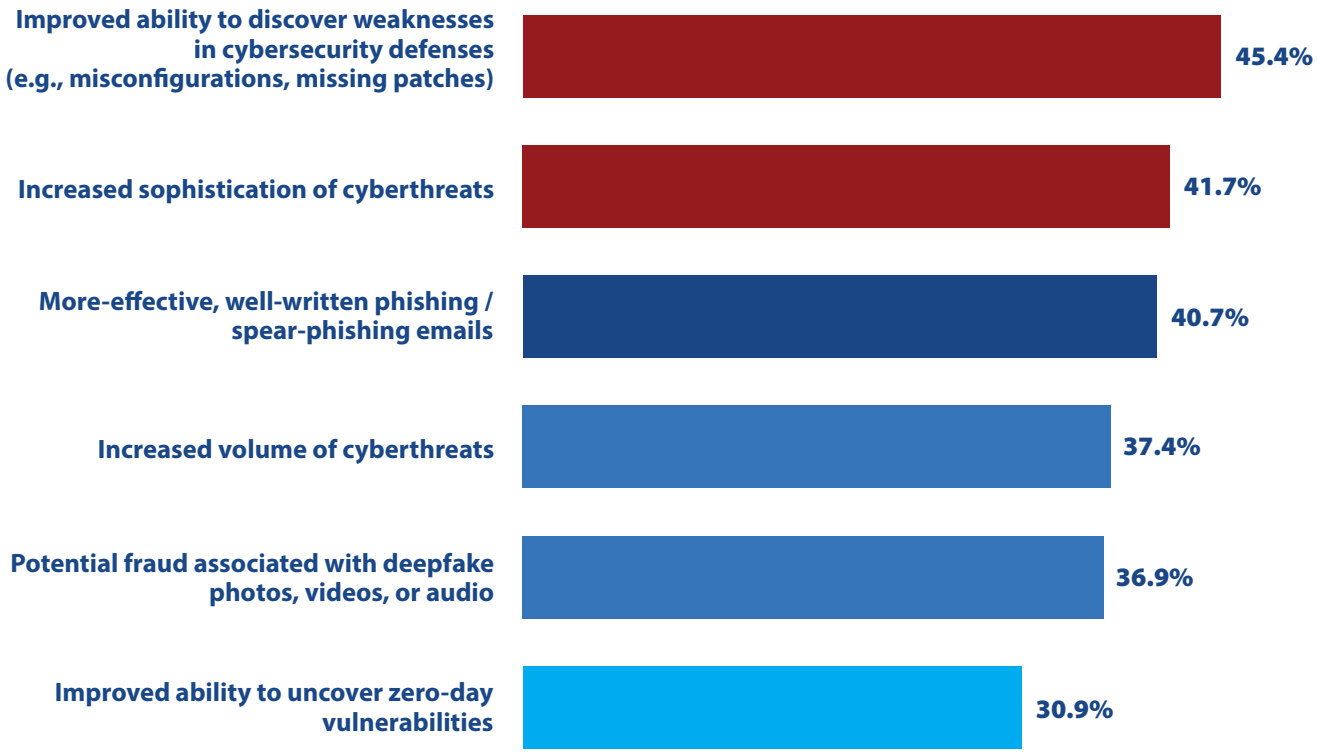


Figure 19: Negative outcomes of AI used by threat actors.

And now, the other side of the coin. If AI can be a friend to IT security teams, can it also be a minion of evildoers?

When asked to select the top three ways that AI technologies could make cyberthreat actors more effective, the most popular answer was "Improved ability to discover weaknesses in cybersecurity defenses," chosen by 45.4% of respondents. Cybercriminals and state-sponsored hackers spend a lot of time searching for unpatched software and devices, misconfigured systems, badly coded applications, unprotected data stores, and other vulnerabilities. AI can make their job a lot easier.

In second place was "Increased sophistication of cyberthreats," selected by 41.7%. There is a danger that AI tools can learn the tricks and techniques of the very best (or should we say the very worst) black hat coders and criminal planners, and then give their powers to every run-of-the-mill gang.

Section 2: Perceptions and Concerns

The third choice was "More effective, well-written phishing/spear-phishing emails," picked by 40.7%. Remember the days when you could identify phishing emails based on bad grammars and mispelings? Today, a simple ChatGPT prompt can instantly produce messages written in the style of your CFO (see Figure 20). Maybe now the tipoff is that the email is *better* written than the ones you get from the CFO.

"Today, a simple ChatGPT prompt can instantly produce messages written in the style of your CFO. Maybe now the tipoff is that the email is *better* written than the ones you get from the CFO."

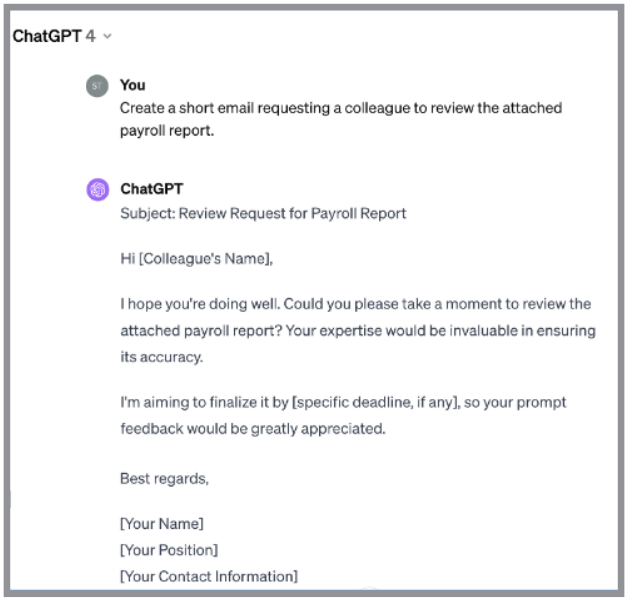


Figure 20: Phishing email created by ChatGPT from a simple prompt.

Rounding out the list were "Increased volume of cyberthreats" (37.4%), "Potential fraud associated with deepfake photos, videos, or audio" (36.9%), and "Improved ability to uncover zero-day vulnerabilities" (30.9%).

These responses show that our security professionals expect a wide variety of negative use cases for AI and ML, just as they anticipate an assortment of positive use cases.

And just as very few are skeptical of the power of AI for security teams, only a handful (3.6%) agreed with the statement, "I don't believe cyberthreat actors will benefit from AI" (see Figure 21).

The clear consensus: prepare for a complex AI battlefield, with IT security teams and cyberthreat actors challenging each other across a wide range of domains.

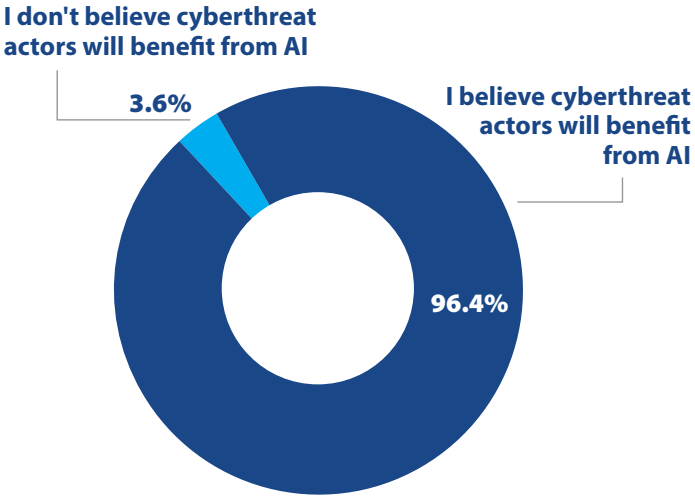


Figure 21: Belief that threat actors will benefit from AI.

Section 2: Perceptions and Concerns

Net Impact of AI on Cybersecurity

Ultimately, who do you believe will benefit more from advancements in artificial intelligence (AI) – IT security teams (with improved defenses) or cyberthreat actors (with improved tactics)?

So, if AI is going to be used extensively by both IT security teams and cyberthreat actors, who is going to come out ahead?

Our respondents are divided. The largest group (40.6%) think the opposing sides will benefit about equally. The next biggest band (35.6%) are the optimists who believe that IT security teams will benefit more. But the party of pessimists who predict that cyberthreat actors will benefit more is also large: 23.8% (see Figure 22).

To net out the positive and negative sentiments, we defined a measure called "Advantage to Security," which is the difference between the percentage of optimists and the percentage of pessimists. For our total sample, that works out to 11.8% (35.6% minus 23.8%).

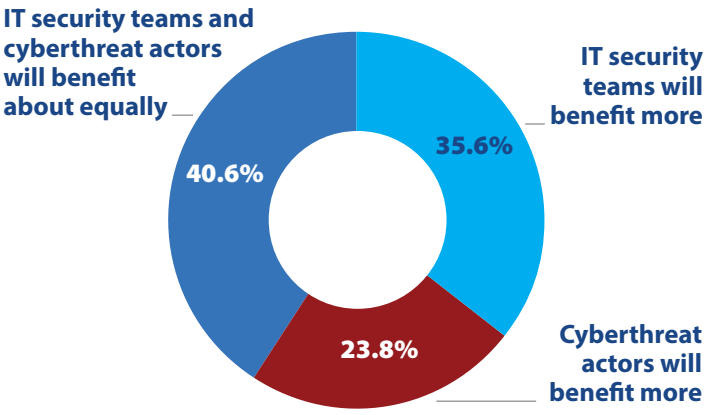


Figure 22: Belief in who will benefit more from AI, security teams or threat actors.

As shown in Figure 23, the Advantage to Security varies greatly across countries. Australians have a far cheerier outlook than anyone else, with 43.8% saying security teams would benefit more and only 12.5% giving the edge to cyberthreat actors (net advantage to security teams: 31.3%). At the other end of the spectrum, Italians are almost evenly divided, giving security teams only a 2.0% advantage.

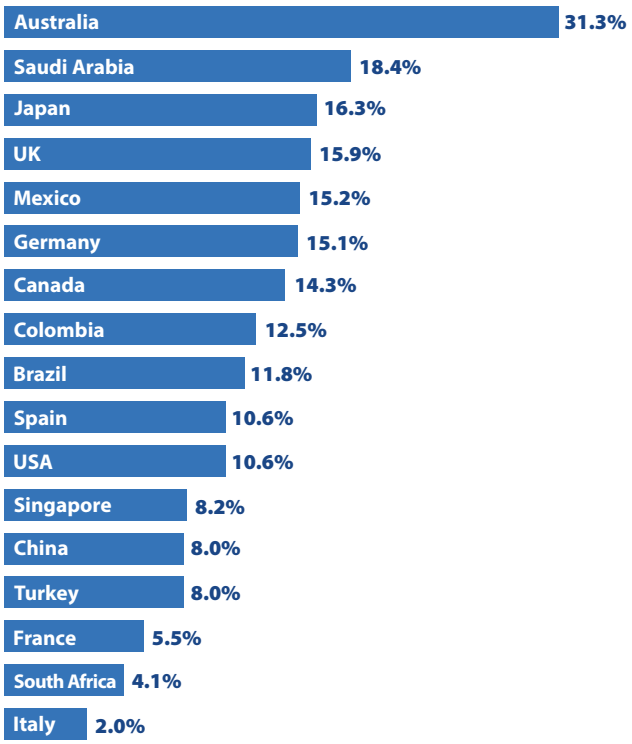


Figure 23: "Advantage to Security," by country

Section 2: Perceptions and Concerns

The difference in outlook by industry is even greater. The AI enthusiasts in retail, technology, and education show a net advantage to security teams of 21.9%, 20.7%, and 20.7%. In contrast, the worrywarts in government and finance actually show an Advantage to Security deficit; that is, more of them believe that AI will, on balance, help cyberthreat actors than the other way around (see Figure 24).

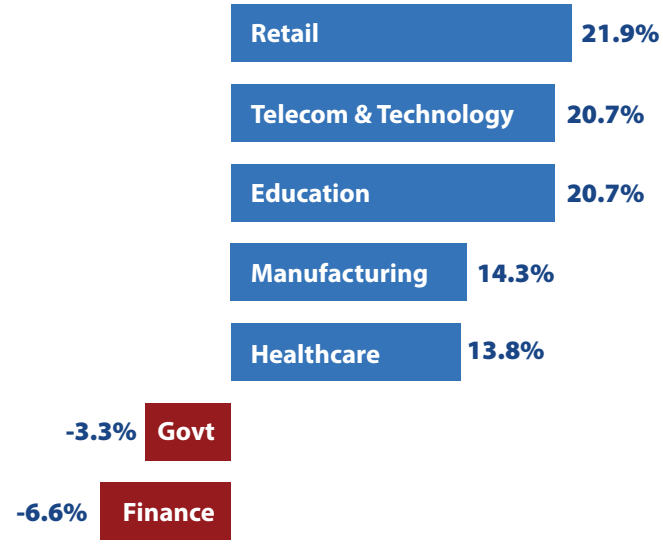


Figure 24: "Advantage to Security," by industry.

When we break down responses by organization size, we find that respondents from smaller organizations show the greatest net advantage to security teams: 17.5% for organizations with 500-999 employees and 13.2% for organizations with 1,000-4,999, versus 5.5% to 11.8% for the other size tiers. We think the smaller firms are counting on AI to multiply the power of their limited staffs and supply specialized knowledge they might not otherwise be able to access.

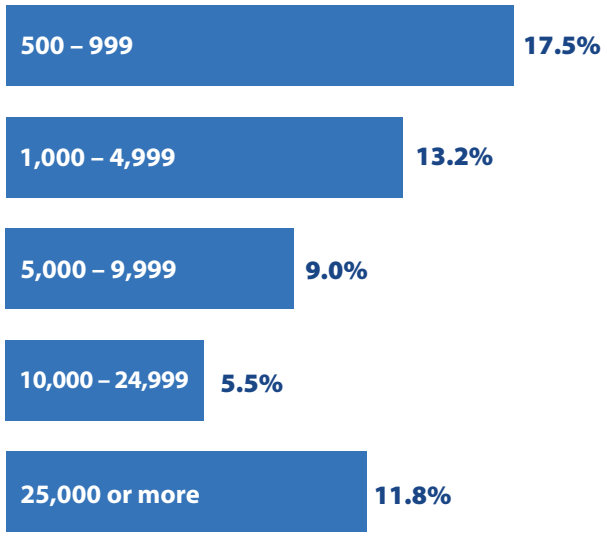


Figure 25: "Advantage to Security," by employee count.

Section 2: Perceptions and Concerns

Responding to Ransomware

If victimized by ransomware in the past 12 months, did your organization pay a ransom (using Bitcoins or other anonymous currency) to recover data?

The dynamics of the ransomware "market" are complex. The number of successful attacks, the size of ransoms demanded, and the percentage of victimized organizations that elect to pay ransoms can gyrate based on multiple reinforcing and offsetting factors. These include the changing capabilities and motivations of ransomware gangs; the nature of attacks (now typically including two or three types of extortion); the ability of organizations to block, contain, or recover from attacks; pressures from outside parties such as law enforcement agencies and cyber insurance companies; and issues of trust.

So, it may not be easy to unsnarl the tangled threads of cause and effect over the last year – but we can try.

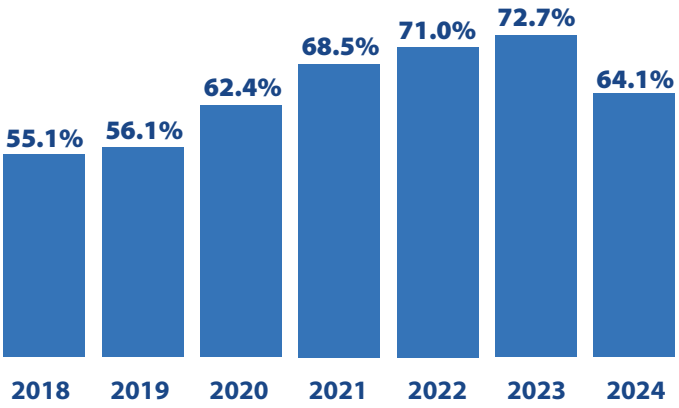


Figure 26: Percentage of organizations victimized by ransomware.

During 2023, some of the major trends in ransomware activities we had been tracking suddenly changed direction. To start with, after increasing steadily for five years, the percentage of organizations victimized by ransomware abruptly fell from 72.7% to 64.1% (see Figure 26).

We believe this reversal was caused by several factors:

- Organizations have invested in monitoring and security tools to quickly detect and contain ransomware attacks before they do serious damage (in part because these capabilities are required to obtain cyber insurance policies).
- With more workers returning to the office post-COVID 19, the attack surface has shrunk somewhat.
- Ransomware gangs are targeting fewer, larger enterprises and spending less time on small and medium-sized organizations.

Why would a ransomware gang attack fewer targets? The members might decide to go after large enterprises that could be induced to pay million-dollar or multi-million-dollar ransoms. But to extract large payments from sophisticated organizations, the gang would need to research each victim, develop techniques to overcome advanced defenses, exfiltrate data as well as encrypt files, carry out prolonged negotiations, etc. This approach might result in a high return on investment from attacking targets with deep pockets but would lose money if applied to smaller victims.

Section 2: Perceptions and Concerns

There is indeed evidence for this dynamic. According to ransomware experts at Coveware, the average ransom payment soared from $408,644 in the fourth quarter of 2022 to $568,705 in the fourth quarter of 2023, and was even higher (up to $850,700) in the second and third quarters of 2023 (see Figure 27). And the firm found that the average size of victimized organizations grew during much of the same period (see the Coveware July 2023 and October 2023 quarterly reports).

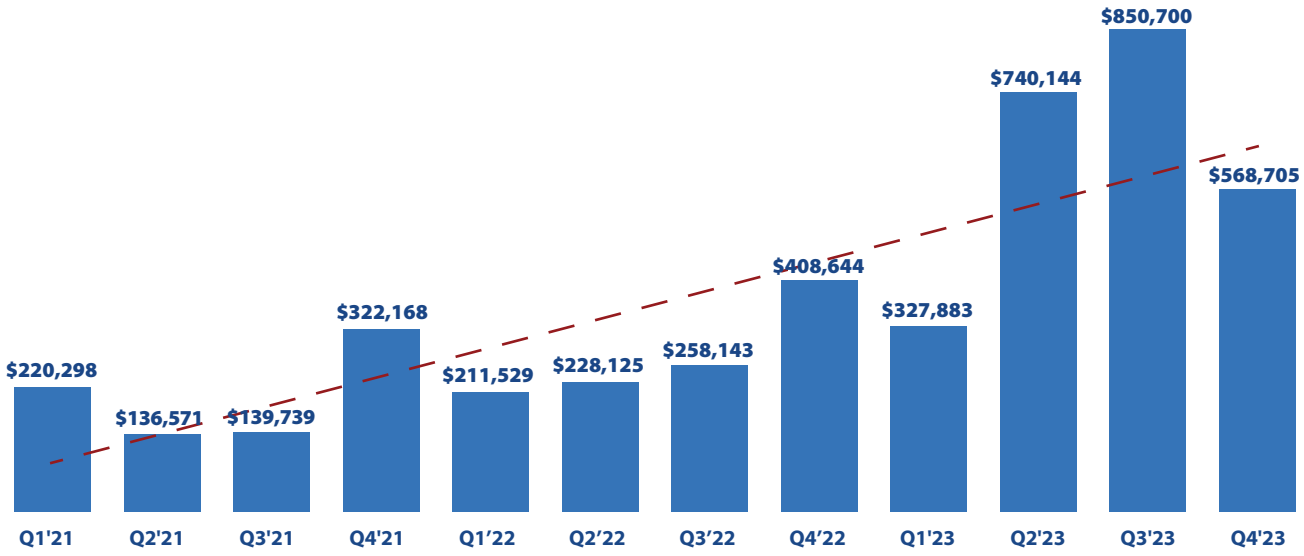


Figure 27: Average ransom payments, by quarter (data source: Coveware Quarterly Ransomware Reports).

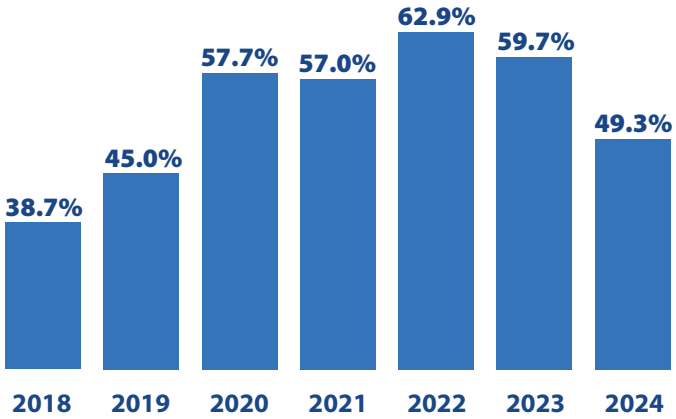


Figure 28: Percentage of victimized organizations paying ransoms.

Now for our second turnaround. The percentage of organizations affected by ransomware that decided to pay ransoms rose steadily between the 2018 and 2022 CDRs, declined slightly in the 2023 report, and fell sharply this year from 59.7% to 49.3% (see Figure 28).

Section 2: Perceptions and Concerns

There are at least three factors behind this change in attitude toward ransom payments:

- Organizations have been investing in tools that support secure, reliable backups and faster recovery to increase their resiliency, allowing them to restart operations faster.
- Government and law enforcement agencies discourage payments and are threatening to enforce measures such as the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) advisory prohibiting ransom payments to criminal and terrorist organizations.
- Enterprises no longer trust ransomware gangs to honor their agreements to keep data breaches secret and help ransom payers recover their data.

And our final U-turn: of organizations that paid ransoms, the percentage that ultimately recovered data fell from 72.7% to 57.0% (see Figure 29). It appears that ransomware gangs are more frequently failing to honor their agreements to help victims recover data.

In terms of industries, those most often victimized by ransomware attacks are finance (86.7%), telecom & technology (72.0%), and education (61.4%). Retail (54.7%) and government (47.5%) are affected least often (see Figure 30).

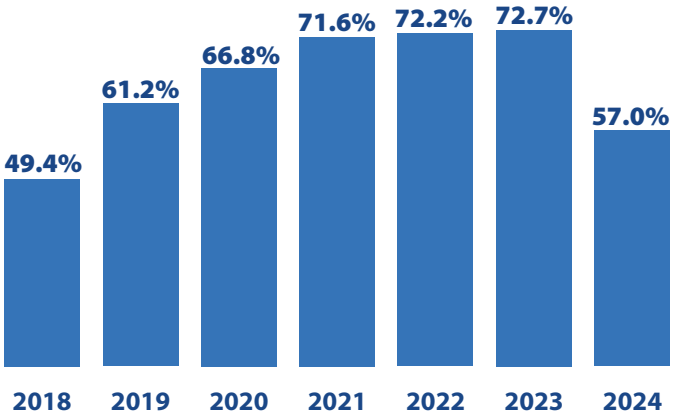


Figure 29: Percentage of ransom payers that recovered data.

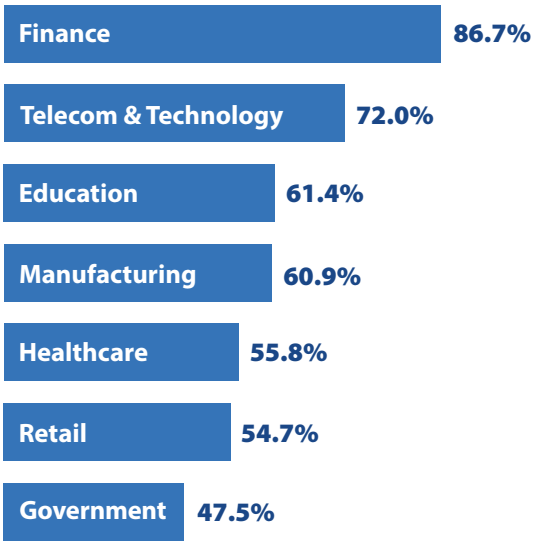


Figure 30: Percentage of organizations victimized by ransomware in the last 12 months, by industry.

Section 2: Perceptions and Concerns

Barriers to Establishing Effective Defenses

On a scale of 1 to 5, with 5 being highest, rate how each of the following inhibit your organization from adequately defending itself against cyberthreats.

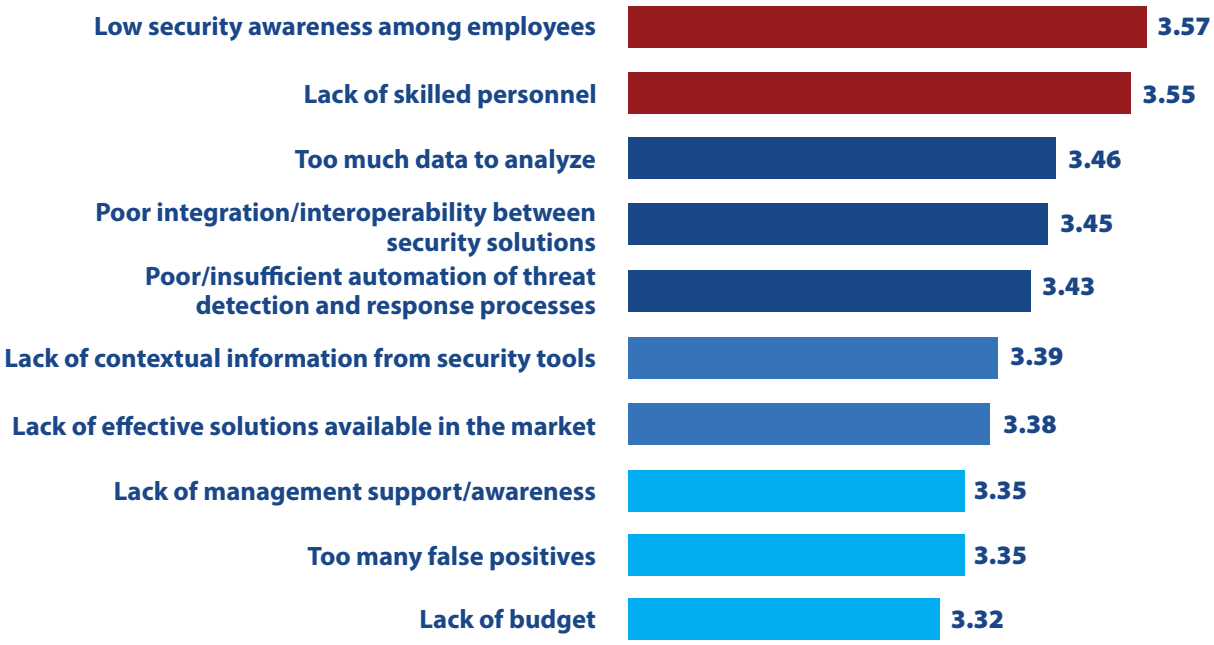


Figure 31: Inhibitors to establishing effective cyberthreat defenses.

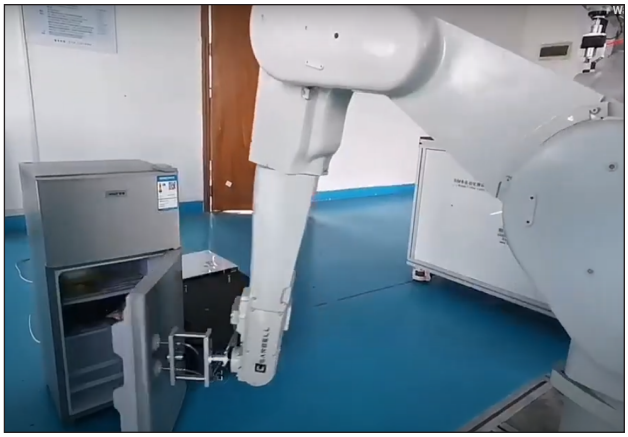


Figure 32: Testing a refrigerator door for weak points.

Have you ever seen the video of the robot arm in a factory test lab that endlessly opens and shuts a refrigerator door to test its durability? The activity looks silly, but it's a key part of a continuous improvement program. One goal of the test is to find out how many times the door can be opened and closed before something fails. The more important objective, though, is to identify the weak points: are they the hinges, the gaskets, the magnets that hold the door closed, or some less-visible part? The factory then tweaks the design of the least-robust components or makes them from stronger materials. Often these adjustments produce major improvements in product life and quality at a low cost.

Section 2: Perceptions and Concerns

The same principle applies to IT security organizations. If you identify what is holding back effective security, you can prioritize strengthening those weak links. You might try vulnerability scanning, penetration testing, and… asking people on the front lines.

That's why every year we query security professionals about the factors that inhibit their organizations from adequately defending themselves against cyberthreats (see Figure 31).

The biggest barriers to successful defense continue to be "Low security awareness among employees" (3.57 on a scale of 1 to 5) and "Lack of skilled personnel" (3.55). Those two have been trading places at the top of the list for several years. In fact, it has become abundantly clear that people problems – training and hiring – are bigger obstacles than any single technical challenge.

Although the exact order of the other factors has varied in recent years, the general picture has remained the same. Our respondents are particularly concerned about "Too much data to analyze" (3.46), "Poor integration/interoperability between security solutions" (3.45), and "Poor/insufficient automation of threat detection and response processes" (3.43).

We can also learn a lot from the factors near the bottom of the list. It appears that few cybersecurity groups are suffering from ignorant or indifferent management. "Lack of management support/awareness" and "Lack of budget" are in the third-from-last and last places. It is also worth noting that "Too many false positives" has fallen to second-to-last. We think that problem is being tamed by improvements in security analytics, possibly with the help of new applications of AI.

When we compare these results to our last survey's, we see another sign that IT security professionals are feeling better. For the second straight year, their level of concern went down for every single category of inhibitor covered in this question. Our Security Concern Index, which is the combined average of the scores for all 10 of the factors, fell a substantial .15, down to 3.43. That's the lowest level since the 2019 CDR (see Figure 33).

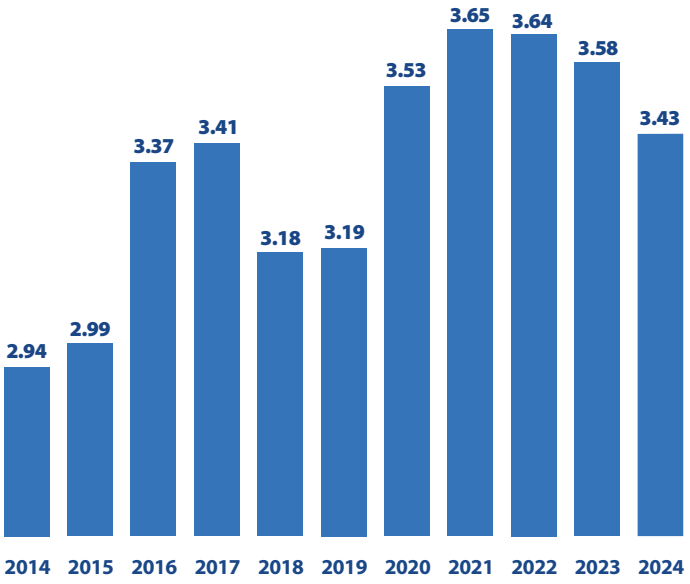


Figure 33: Security Concern Index, depicting the average rating of security inhibitors.

Section 2: Perceptions and Concerns

Factors That Improve Job Satisfaction

Which of the following would help improve your overall job satisfaction in your company's IT security organization? (Select up to five.)

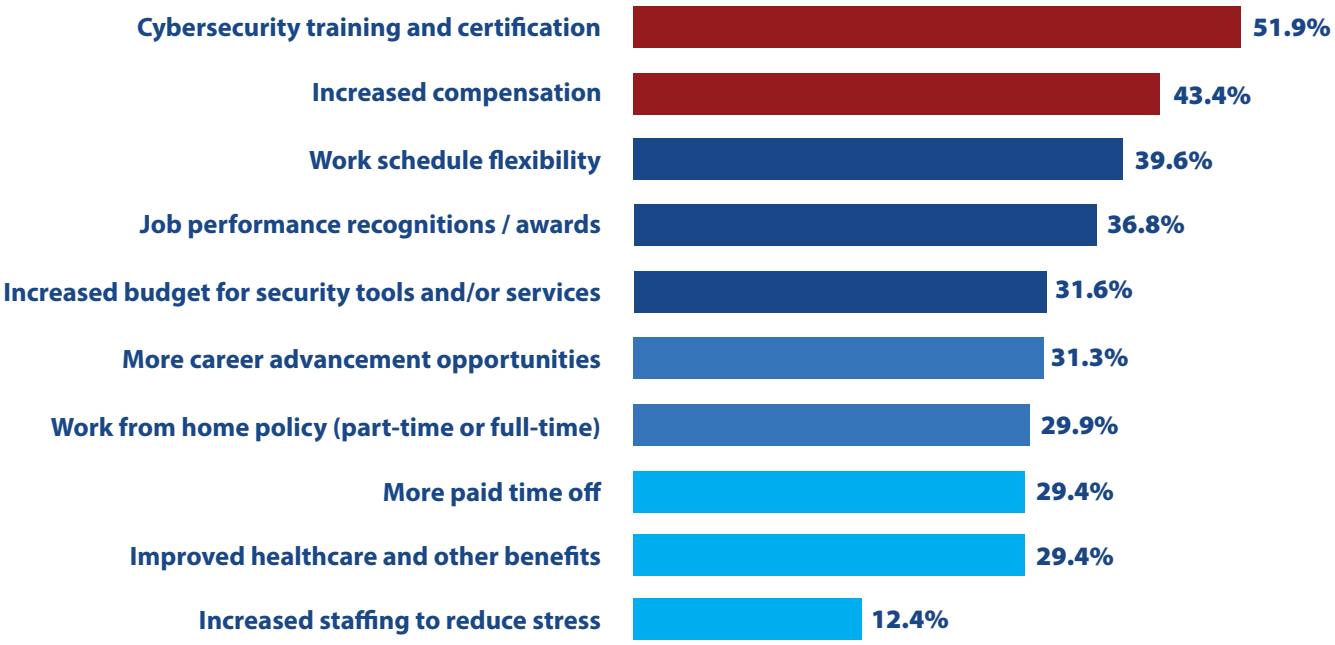


Figure 34: Factors that would improve job satisfaction in the IT security organization.

A running theme in this report is the shortage of skilled cybersecurity personnel (page 15) and its impact on organizations' ability to adequately defend themselves against cyberthreats (page 30).

Well, when we talk about problems, we like to suggest solutions. So this year we added a question to our survey about factors that would improve job satisfaction among IT security staff, potentially improving recruiting and retention (see Figure 34).

The item selected most often was cybersecurity training and certification, which was cited by 51.9% of the respondents. Cybersecurity personnel value ongoing training because it enables them to keep up with new security technologies and concepts so that they can do their jobs better (and be rewarded for better performance).

Not surprisingly, increased compensation was also a high priority, at number two (43.4%).

Section 2: Perceptions and Concerns

But budget-conscious security leaders take note: there are ways to make your team happier without breaking the bank. In fact, "soft" rewards were third and fourth on the list. Work schedule flexibility was selected by 39.6% of the respondents, and job performance recognitions/awards by 36.8%.

Other incentives frequently selected included increased budget for security tools and/or services (31.6%), more career advancement opportunities (31.3%), a part-time or full-time work-from-home policy (29.9%), and improved healthcare coverage and other benefits (29.4%).

Here's the takeaway. When it comes to improving job satisfaction and staff retention, soft incentives like training, flexible schedules, and recognition are at least as influential as increased compensation and traditional benefits.

"When it comes to improving job satisfaction and staff retention, soft incentives like training, flexible schedules, and recognition are at least as influential as increased compensation and traditional benefits."

Section 2: Perceptions and Concerns

Value of Classroom and Online IT Security Training

Describe your agreement with the following statement: "Classroom and/or online IT security training have helped me better protect my organization and/or my customers' critical assets."

Were you surprised that half of the survey respondents selected "Cybersecurity training and certification" as one of the best ways to improve job satisfaction (page 32)? Here is more data that supports that finding.

We asked our security professionals to describe their agreement with the statement: "Classroom and/or online IT security training have helped me better protect my organization and/or my customers' critical assets." Responses were strongly in favor of this proposition: a full 41.5% of respondents strongly agree, and another 45.7% somewhat agree (see Figure 35).

And that agreement is nearly unanimous and widely distributed. Only a modest 9.8% have no opinion, and a minuscule 3.0% disagree. The percentage of respondents who somewhat or strongly agree exceeded 80% in 14 of the 17 countries and all seven of the major industries in our survey.

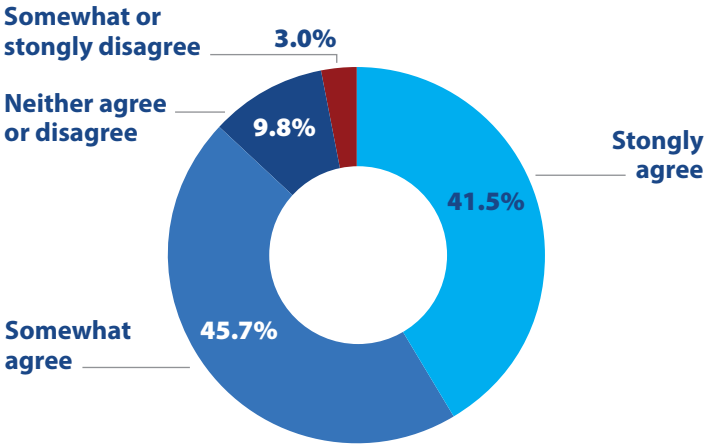


Figure 35: Agreement with the statement: "Classroom and/or online IT security training have helped me better protect my organization and/or my customers' critical assets."

Section 3: Current and Future Investments

IT Security Budget Change

Do you expect your employer's overall IT security budget to increase or decrease in 2024?

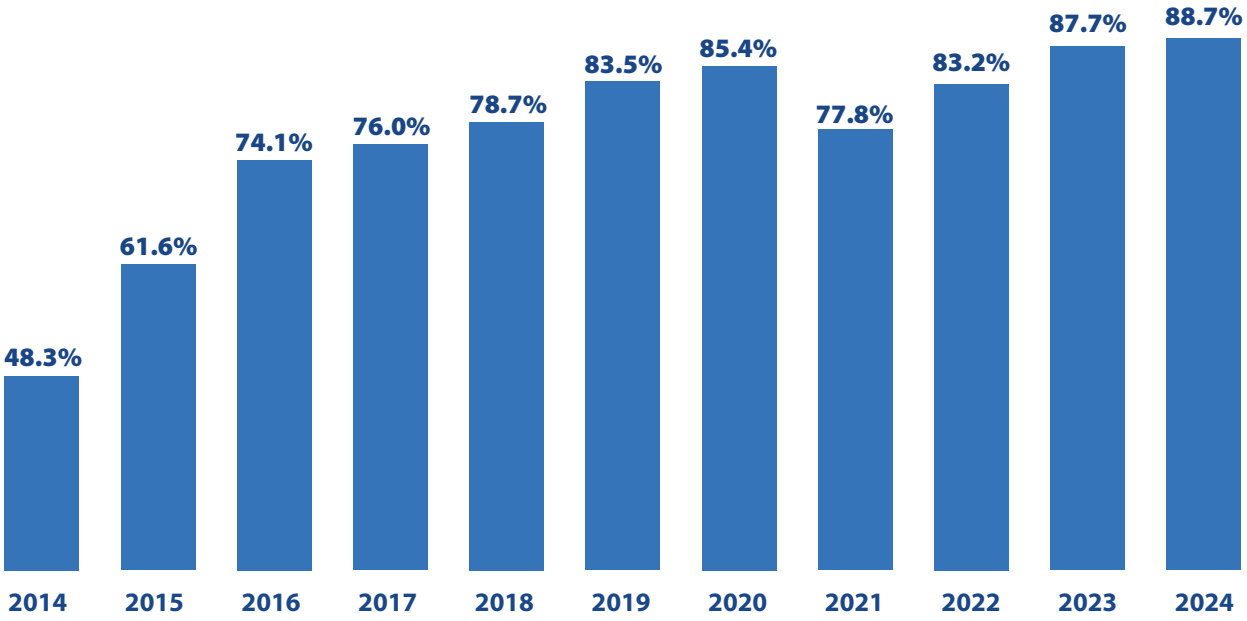


Figure 36: Percentage of organizations with rising security budgets.

You might think that slowing economic growth in certain parts of the world and large layoffs in some industries would cause IT security budget growth to slow or reverse in at least a few sectors in the coming year. But on the contrary, survey respondents pretty much across the board are expecting healthy, even record IT security budget growth.

The percentage of IT security groups predicting an increase in their budget in the year ahead has gone up every year since we started conducting our survey except for one (2021, because of COVID). This year that figure reached a new height: 88.7% (see Figure 36). Only a tiny minority (3.0%) are expecting their budget to go down in 2024. The rest (8.3%) think their budget will stay about the same.

Let's think about that for a moment. Leaving aside general economic trends, in any given year a significant percentage of businesses and government agencies retrench because of competition, reduced funding, higher interest rates, increasing raw material prices, supply chain problems, post-merger cost cutting, bad management decisions, and innumerable other issues. Yet 97% are coming up with the cash to maintain or increase their cybersecurity budgets. Clearly, top management and boards of directors have gotten the message that IT security is a top priority and an area where they absolutely must keep getting better.

In addition, the average (mean) increase in IT security budgets reached a record this year: 5.7%. That compares favorably with increases of 5.3% last year and 4.6% the year before (see Figure 37). Not only have budgets been going up recently, they have been rising at a faster rate.

Section 3: Current and Future Investments

Also, expected budget increases are fairly consistent across major industries (ranging from 5.0% in education to 6.4% in finance – see Figure 38) and across company sizes (from 5.5% for organizations with more than 25,000 employees to 6.0% for organizations with 10,000 to 25,000 – see Figure 39).

Finally, among organizations expecting an increase, more than half (54.6%) anticipate budget growth between 5% and 10%. And about one in five (19.9%) are predicting an increase of 10% or more (Figure 40).

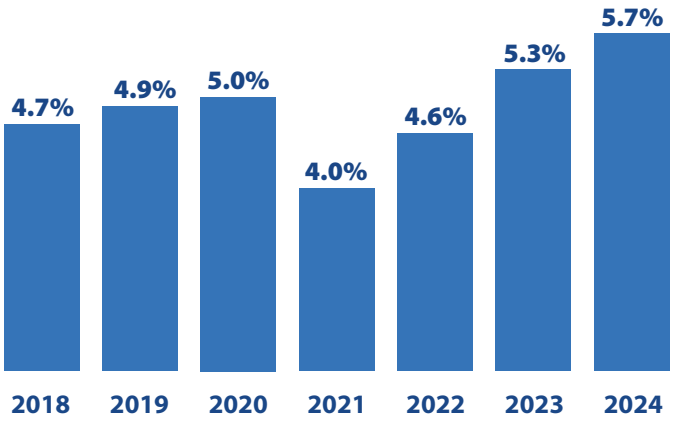


Figure 37: Mean annual increase of IT security budgets.

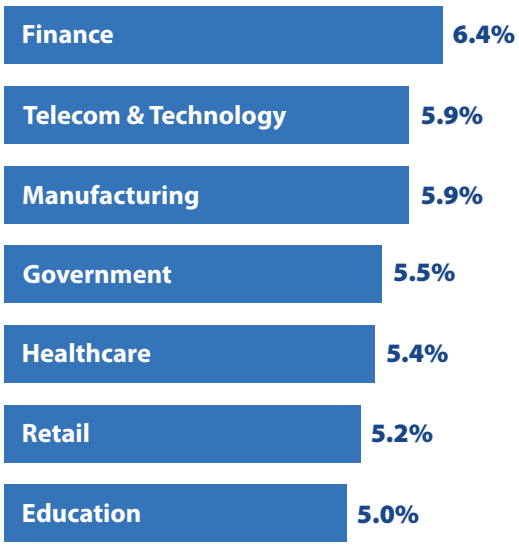


Figure 38: Mean security budget increase, by industry.

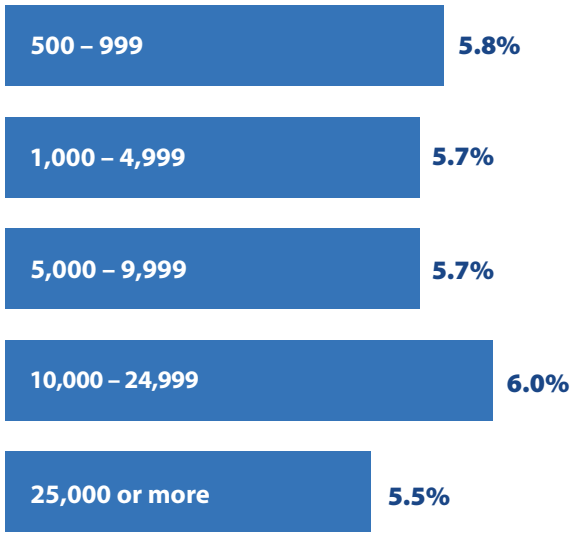


Figure 39: Mean security budget increase, by employee count.

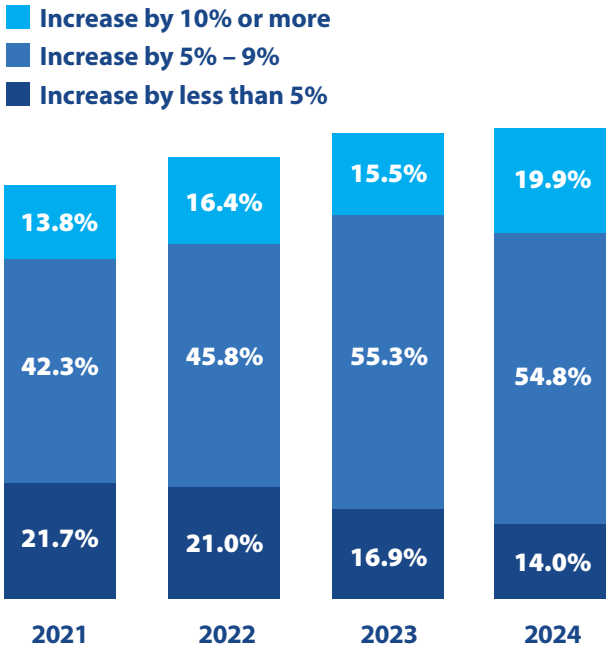


Figure 40: Breakdown of annual increase in IT security budgets (excludes organizations with declining or flat budgets).

Section 3: Current and Future Investments

Network Security Deployment Status

Which of the following network security technologies are currently in use or planned for acquisition (within 12 months) by your organization?

	Currently in use	Planned for acquisition	No plans
Secure web gateway (SWG)	57.8%	31.1%	11.1%
Intrusion detection / prevention system (IDS/IPS)	56.8%	32.1%	11.1%
Secure email gateway (SEG)	56.7%	32.6%	10.7%
Data loss / leak prevention (DLP)	55.8%	31.9%	12.3%
Network access control (NAC)	55.4%	33.6%	11.0%
SSL/TLS decryption appliances / platform	52.8%	34.2%	13.0%
Advanced threat prevention (sandboxing, ML/AI)	52.0%	38.6%	9.4%
Denial of service (DoS/DDoS) prevention	50.3%	35.1%	14.6%
Next-generation firewall (NGFW)	44.3%	41.8%	13.9%
Network behavior analysis (NBA) / NetFlow analysis	43.6%	38.5%	17.9%
Deception technology / distributed honeypots	36.6%	40.6%	22.8%

Table 1: Network security technologies in use and planned for acquisition.

Network security remains a cornerstone of IT security. True, we no longer believe it can keep out all the bad guys, all the time. We know some will get through by exploiting vulnerabilities, or careless users, or insecure code, or something else. But strong network security solutions:

- Block a large percentage of scans and attacks, including most of the less-sophisticated ones
- Collect data about attack-related events that is essential for incident response and remediation
- Frustrate some threat actors and cause them to turn their attention to easier targets

So, if you are a security professional, it is helpful to know the network security technologies your peers are using today and the ones they plan to deploy in the near future.

At first glance, the most striking finding in Table 1 is the sharp drop by "Advanced threat prevention (sandboxing, ML/AI)" from first place last year to seventh place this year in the "currently in use" column. The percentage of organizations with these products installed is still substantial – 52.0% – but it's down from 56.8% in the last survey. However, we are pretty sure that security groups are not disappointed with this class of technology. Instead, capabilities like sandboxing and AI-driven malware analysis are being incorporated into broader network security solutions rather than being deployed as separate products.

Section 3: Current and Future Investments

"So which network security technology is the new king of the hill? That would be secure web gateway (SWG)... Over the last four years, SWG has jumped from seventh place, to fifth place, to third place, and now to first place on our list."

So, which network security technology is the new king of the hill? That would be secure web gateway (SWG). As enterprises expand their web-based interactions with customers, suppliers, business partners, and government agencies, they need to filter, block, and monitor more suspicious web traffic based on corporate policies. This scenario has made SWG a rising star among network security technologies. Over the last four years, it has jumped from seventh place, to fifth place, to third place, and now to first place on our list. It is currently installed in 57.8% of organizations.

Four other network security technologies are in use in at least 55% of organizations.

Intrusion detection and prevention systems (IDS/IPS) continue to be a mainstay for detecting a wide variety of network-borne attacks. Installations rose 3.7% since the last survey, reaching 56.8%. Secure email gateway (SEG) technology plays a critical role identifying and blocking emails that contain malicious content and dangerous attachments. It is in use in 56.7% of enterprises.

Data loss (or leak) prevention (DLP) focuses on preventing sensitive information from leaving the network. Network access control (NAC) ensures external systems can't log onto secure networks unless they meet specific requirements, for example, having up-to-date operating systems and several security solutions installed and running. DLP and NAC have reached the level of "must have" security solutions, in use in 55.8% and 55.4% of organizations, respectively. These figures represent increases of 4.6% and 4.5% compared to the previous survey.

What network security technologies are most often planned for acquisition over the next 12 months? Next-generation firewall (NGFW) was cited most often (41.8%), followed by deception technology/distributed honeypots at 40.6%. Deception solutions create fake computing environments, complete with network segments, user accounts, devices and servers, applications, databases, and file stores, and observe how threat actors try to find and exfiltrate data. They divert attackers away from real information assets and give security teams front-row seats to observe their techniques.

Next: endpoint security technologies in use and planned for acquisition (page 39).

Section 3: Current and Future Investments

Endpoint Security Deployment Status

Which of the following endpoint security technologies are currently in use or planned for acquisition (within 12 months) by your organization?

	Currently in use	Planned for acquisition	No plans
Basic anti-virus / anti-malware (threat signatures)	70.3%	24.0%	5.7%
Data loss / leak prevention (DLP)	59.1%	30.2%	10.7%
Endpoint detection and response (EDR)	57.7%	30.4%	11.9%
EPP / Advanced anti-virus / anti-malware (machine learning, behavior monitoring, sandboxing)	54.9%	35.6%	9.5%
Browser or Internet isolation / micro-virtualization	54.7%	32.5%	12.8%
Disk encryption	54.0%	33.4%	12.6%
Digital forensics / incident resolution	46.8%	38.1%	15.1%
Deception technology / honeypot	37.3%	44.7%	18.0%

Table 2: Endpoint security technologies in use and planned for acquisition.

Threat actors and security solution vendors are struggling for control of endpoints and the applications that run on them. While once defenders were mostly concerned with detecting malware files, now they also must worry about fileless malware and other threats that inject malicious code into registries and legitimate applications, use scripts and native utilities to launch attacks, and gain administrator privileges to disable security features.

Among endpoint security solutions currently in use, basic anti-virus/anti-malware products remain by far the most common (see Table 2). They examine files to see if they match the signature of known malware, and they are employed in more than two-thirds of the organizations in our survey. Of course, we're pretty sure 100% of organizations scan for malware on endpoints, but increasingly those capabilities are included as one component of EDR and EPP solutions. In fact, the percentage of organizations running standalone basic anti-malware packages has declined from 74.2% two years ago, to 72.6% last year, to 70.3% in the current survey.

The second most frequently installed endpoint security technology is endpoint data loss (or leak) protection (DLP). Products in this field examine outgoing emails and documents to determine if they contain sensitive information such as financial account numbers, Social Security numbers, and other PII and intellectual property. They then apply policies to take actions like blocking the export of the information or encrypting it before transmission. Endpoint DLP is currently installed at 59.1% of organizations, up 3.0% from the previous survey.

Section 3: Current and Future Investments

In third and fourth places are endpoint detection and response (EDR) and endpoint protection platform (EPP) technologies. EDR solutions combine a variety of tools to monitor endpoints and detect malware and events associated with attacks. EPP solutions usually include EDR features plus additional capabilities for analysis and threat hunting. EDR and EPP solutions are installed in 57.7% and 54.9% percent of organizations, respectively.

The fifth technology in the currently in use column is "Browser or Internet isolation/micro-virtualization." Products in this area typically run browser or application sessions in an isolated space so that users can visit websites and open emails and documents without allowing attackers to access their computers or mobile devices. This is an up-and-coming technology; it actually showed the biggest gain in installations among endpoint security offerings, increasing by 3.8% to reach 54.7%.

The leaders in the "planned for acquisition" area were deception technology/honeypot and digital forensics, planned by 44.7% and 38.1% of organizations, respectively.

Next: application and data security (page 41).

Section 3: Current and Future Investments

Application and Data Security Deployment Status

Which of the following application- and data-centric security technologies are currently in use or planned for acquisition (within 12 months) by your organization?

	Currently in use	Planned for acquisition	No plans
Database firewall	62.8%	25.7%	11.5%
Web application firewall (WAF)	60.8%	29.8%	9.4%
API gateway / protection	60.0%	32.9%	7.1%
Database activity monitoring (DAM)	55.6%	33.4%	11.0%
Application container security tools/platform	54.3%	35.7%	10.0%
Cloud access security broker (CASB)	50.8%	35.1%	14.1%
Application delivery controller (ADC)	48.3%	36.6%	15.1%
File integrity / activity monitoring (FIM / FAM)	46.9%	39.5%	13.6%
Runtime application self-protection (RASP)	45.2%	37.9%	16.9%
Static/dynamic/interactive application security testing (SAST / DAST / IAST)	44.8%	39.3%	15.9%
Third-party code analysis	41.4%	39.6%	19.0%
Bot management	36.0%	43.7%	20.3%

Table 3: Application and data security technologies in use and planned for acquisition.

This year there are three application and data security technologies that we would characterize as must-haves because they are in use in at least 60% of organizations: database firewall, web application firewall (WAF), and API gateway and protection products (see Table 3).

Database firewall and WAF each moved up a notch, from second and third last year to first and second this year. Both saw the percentage of installations increase: the former increased by 2.7% to 62.8% and the latter jumped by 5.4% to 60.8%. The heightened popularity reflects a growing interest by security professionals in monitoring and protecting individual databases and web applications.

Solutions to control traffic through APIs fell from first to third place on the list. But that change was due to increased use of database firewalls and WAFs. Installations of API gateways and protection solutions stayed about the same, declining slightly from 60.6% to 60.0%. With an increasing amount of application traffic flowing through APIs, we expect these solutions to gain new adherents over the coming years.

Section 3: Current and Future Investments

The technologies in the fourth through sixth positions retained the same order and increased usage. Installations of database activity monitoring (DAM) products grew by a very healthy 3.9% to reach 55.6%. Application container security tools and platforms rose by 3.5%, to 54.3%. And installations of cloud access security brokers (CASB) inched up by 0.6%, to 50.8%.

Bot management is not installed as often as the other applications in this sector, but it is the leader in planned acquisitions, at 43.7%. Controlling traffic from bots is a priority because of their use in ransomware, spam, DDoS attacks, and other threats.

Other technologies widely planned for acquisition this year include third-party code analysis, file integrity/activity monitoring (FIM/FAM), and application security testing (SAST/DAST/IAST).

We now turn to our final table in this survey, which covers current use and planned acquisition of security management and operations technologies (page 43).

"This year we have three application and data security technologies that we would characterize as 'must-haves' because they are in use in at least 60% of organizations: database firewall, web application firewall (WAF), and API gateway and protection products."

Section 3: Current and Future Investments

Security Management and Operations Deployment Status

Which of the following security management and operations technologies are currently in use or planned for acquisition (within 12 months) by your organization?

	Currently in use	Planned for acquisition	No plans
Active Directory protection	56.7%	32.9%	10.4%
Patch management	55.9%	32.4%	11.7%
Security configuration management (SCM)	54.6%	32.7%	12.7%
Cyber risk quantification / scorecard	54.1%	33.9%	12.0%
Security information and event management (SIEM)	53.2%	34.0%	12.8%
Vulnerability assessment/management (VA / VM)	51.3%	38.5%	10.2%
Penetration testing / attack simulation software	50.3%	37.0%	12.7%
Advanced security analytics (e.g., with machine learning, AI)	46.7%	42.7%	10.6%
Threat intelligence platform (TIP) or service	45.9%	39.7%	14.4%
Security orchestration, automation, and response (SOAR)	45.8%	39.4%	14.8%
Full-packet capture and analysis	45.6%	39.8%	14.6%
User and entity behavior analytics (UEBA)	43.7%	39.0%	17.3%

Table 4: Security management and operations technologies in use and planned for acquisition.

For the third year running, Active Directory protection is the security management and operations technology most widely in use, at 56.7% of organizations (see Table 4). Active Directory manages identity information about people, and increasingly also about non-human "users" such as IoT devices, industrial control systems, and modularized software services. Attacks on Active Directory are picking up. In addition, organizations implementing zero trust frameworks need to feel confident about using identity information in Active Directory (or equivalent enterprise directories) to assess how much access to resources each user account should be given. These reasons add up to making Active Directory protection a critical enabler of identity management.

The old warhorse, patch management, moved from fourth place in the last survey to second place in this one. It is in use in 55.9% of organizations (up from 50.5% last year). We think a lot of renewed interest in patch management comes from the need to prevent ransomware gangs and other cybercriminals from infiltrating networks through unpatched third-party devices and software, a la the SolarWinds hack.

Section 3: Current and Future Investments

In third place is security configuration management (SCM), installed in 54.6% of organizations. With more and more security applications and devices enforcing more and more regulatory and company policies, it is very important to keep security configurations straight. And of course, when policies are changed, you want to be able to deploy those changes quickly across your entire computing environment.

Other security management and operations technologies in use in more than half of organizations are cyber risk quantification/scorecard (54.1%), security information and event management (SIEM) (53.2%), vulnerability assessment/management (VA/VM) (51.3%), and penetration testing/attack simulation software (50.3%).

The leaders in the "Planned for Acquisition" category are "Advanced security analytics," "Full packet capture and analysis," "Threat intelligence platforms (TIP) or services," and "Security orchestration, automation, and response (SOAR)" solutions.

"For the third year running, Active Directory protection is the security management and operations technology most widely in use... Attacks on Active Directory are picking up. In addition, organizations implementing zero trust frameworks need to feel confident about using identity information."

Section 4: Practices and Strategies

Benefits of DevSecOps Practices

Which of the following have been the biggest benefits of DevSecOps practices for your organization? (Select up to three.)

We returned to a question about DevSecOps practices last asked in the 2021 CDR. DevSecOps (a term that combines "development," "security," and "operations") refers to integrating security design, security features, and security testing into Agile application development and deployment processes. Examples include introducing security requirements in the design phase of applications; adding security features to the code during the main development process instead of trying to retrofit them into nearly finished applications; and ensuring that new applications, updates, and patches are rigorously tested for security defects. These practices both improve security and speed up development and deployment cycles.

At least, that is the theory. What have been the most important benefits in practice? And have those changed over the last three years? We're glad you asked.

There hasn't been much change at the top of the list. The two benefits cited most often, "Increased speed of deploying application updates" and "Increased speed of deploying new applications" are the same in the 2024 CDR as they were three years ago (see Figure 41). The frequency with which they were selected changed only slightly, from 47.2% to 45.8% for accelerating updates, and from 45.8% to 45.6% for speeding up new applications.

It's not surprising that these are popular benefits because, let's be frank, most application development teams are more motivated by quickly delivering new functional features than by addressing security requirements.

However, we see evidence of one noteworthy change in attitudes between the 2021 and 2024 surveys: respondents selecting "Fewer application security vulnerabilities/risks" as a big benefit jumped 5.5%, from 38.5% to 44.0% (which is only slightly behind the top two benefits). In other words, development groups are acknowledging that DevSecOps practices lead to significant improvements in security that benefit organizations roughly as much as accelerating the delivery of updates and new applications.

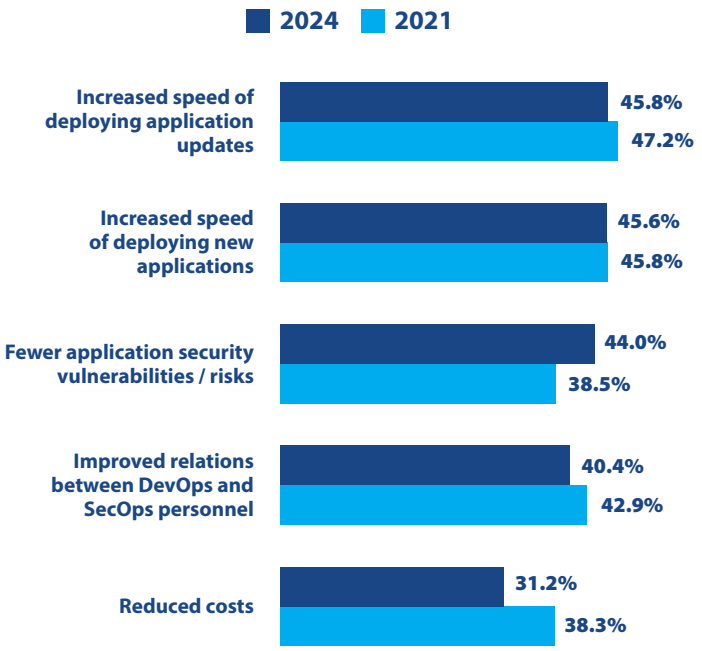


Figure 41: Benefits of adopting DevSecOps practices.

The final two benefits on our list, "Improved relations between DevOps and SecOps personnel" and "Reduced costs," continue to be cited as benefits by many organizations, but somewhat less frequently than in the 2021 survey.

Section 4: Practices and Strategies

Our data also captures the percentage of organizations that have implemented DevSecOps practices: 91.1% (see Figure 42). This confirms their popularity. By industry, DevSecOps practices are implemented most widely in retail (94.0%), healthcare (92.9%), and manufacturing (92.2%), and least often in education (88.9%) and government (88.1%) (see Figure 43).

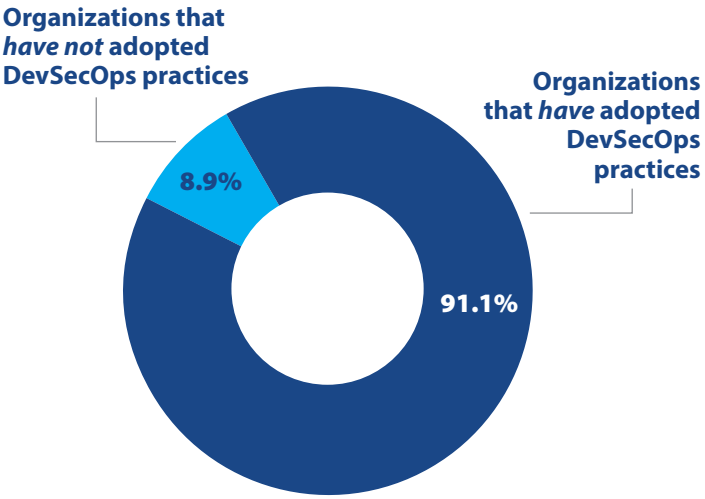


Figure 42: Percentage of organizations that have adopted DevSecOps practices.

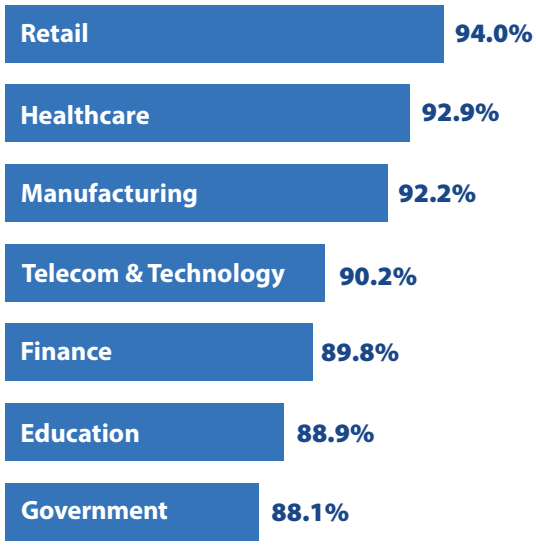


Figure 43: Percentage of organizations that have adopted DevSecOps practices, by industry.

"[W]e see evidence of one noteworthy change in attitudes: respondents selecting "Fewer application security vulnerabilities/risks" as a big benefit jumped 5.5%... development groups are acknowledging that DevSecOps practices lead to significant improvements in security and this benefits organizations roughly as much as accelerating the delivery of updates and new applications."

Percentage of Security Applications and Services Delivered Via the Cloud

What percentage of your information security applications and services is delivered via the cloud?

To compare current responses, we revived another question from earlier surveys: "What percentage of your information security applications and services is delivered via the cloud?"

The mean across all respondents increased from 35.7% in the 2020 CDR to 40.1% in this one (see Figure 44). That result is not surprising, given the long-term trend toward delivery of more applications and services of all kinds via the cloud. Not only does cloud delivery relieve enterprises of the burdens of hosting software on their own premises, cloud-based applications are much more scalable, allowing them to expedite handling of compute-intensive tasks (of which there are many in security).

But this is one topic where the breakdowns by country and industry showed significant variations.

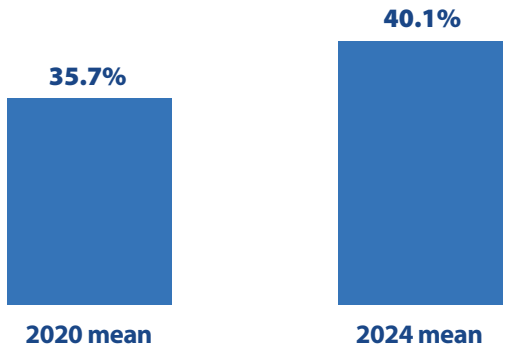


Figure 44: Percentage of security applications and services delivered via the cloud.

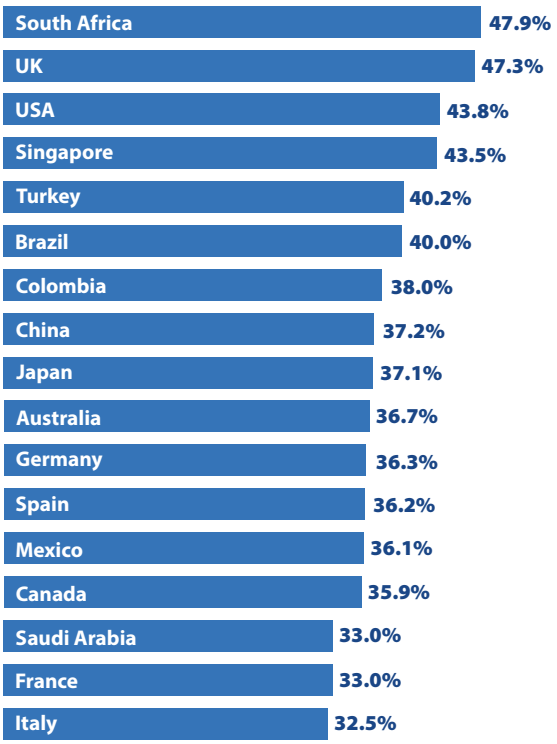


Figure 45: Percentage of security applications and services delivered via the cloud, by country.

Results varied quite a bit by country. As shown in Figure 45, cloud delivery is most common in South Africa (47.9%), the United Kingdom (47.3%), the United States (43.8%), and Singapore (43.5%). Usage in these countries is significantly higher than in Canada (35.9%), Saudi Arabia (33.0%), France (also 33.0%), and Italy (only 32.5%).

Section 4: Practices and Strategies

Differences are also apparent across industries (see Figure 46). Manufacturers and retailers use cloud-based services the most (45.7% and 43.8%, respectively). Financial institutions and government agencies are lagging adopters (37.1% and 33.6%), no doubt because many are subject to regulations that require sensitive information (access credentials as well as data) to remain on premises.

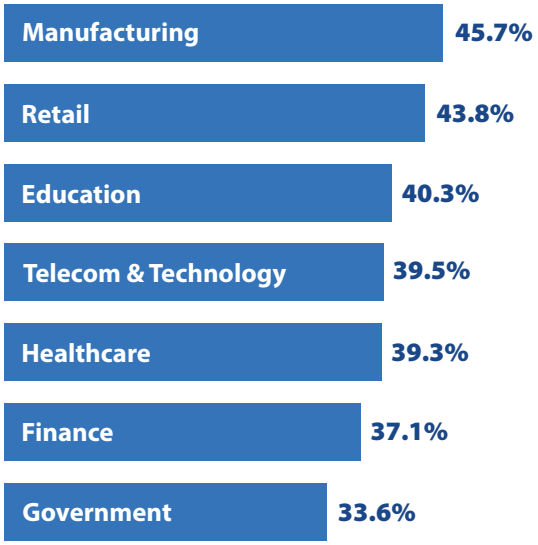


Figure 46: Percentage of security applications and services delivered via the cloud, by industry.

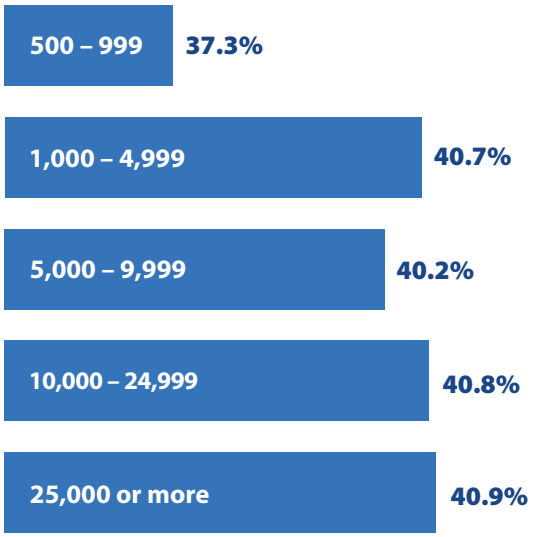


Figure 47: Percentage of security applications and services delivered via the cloud, by employee count.

Interestingly, organizations of different sizes were very consistent, with one major exception (see Figure 47). Our four tiers of organizations with 1,000 or more employees all reported between 40.2% and 40.9% of their security applications and services are coming through the cloud, a range of only 0.7%. The outlier was organizations with 500-999 employees. The figure there was significantly lower: 37.3%. It appears that many small organizations still prefer to run security solutions in their own data centers.

Section 4: Practices and Strategies

How Organizations Leverage External Threat Intelligence

How does your organization leverage external threat intelligence? (Select all that apply.)

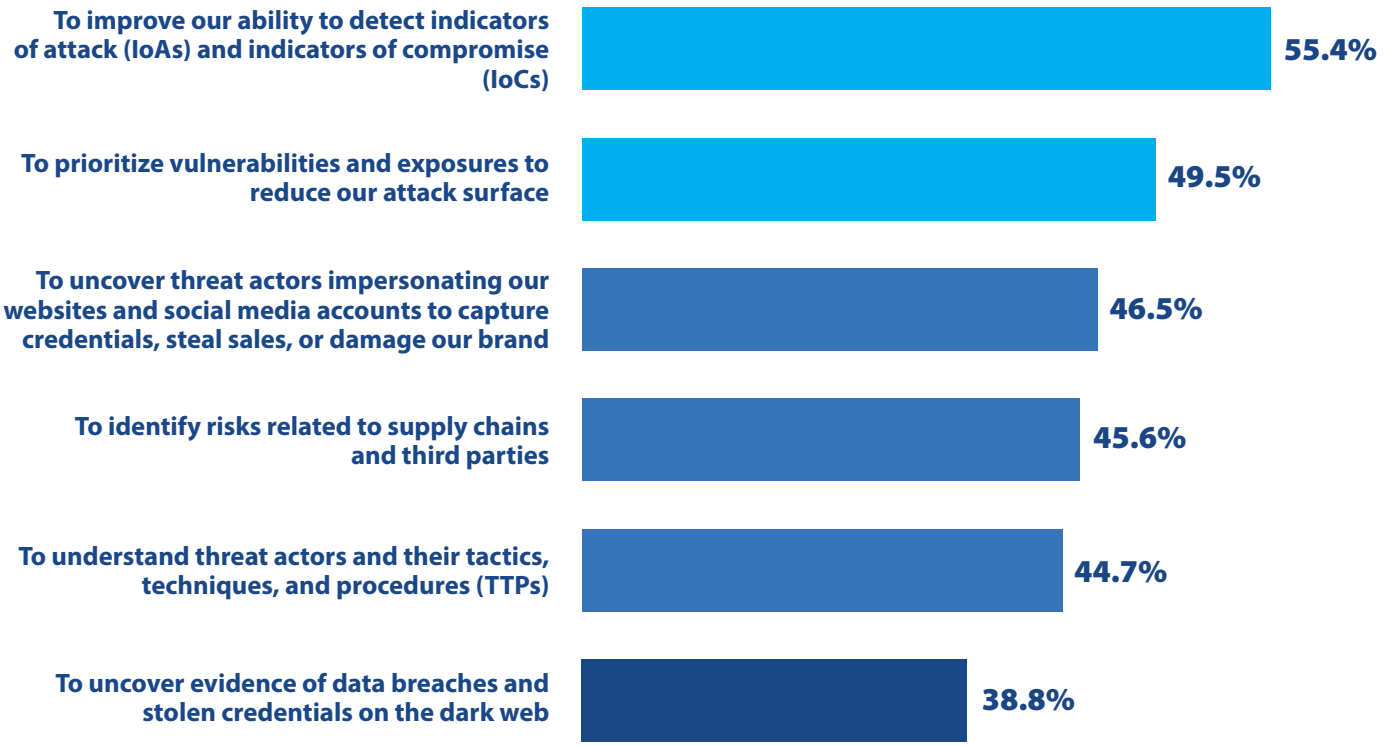


Figure 48: How organizations are leveraging external threat intelligence.

We have observed more and more cybersecurity vendors advertising the fact that their solutions employ threat intelligence for tasks like making better context-based authentication decisions and automatically prioritizing alerts. But what about enterprise IT security groups? We wanted to know how they are leveraging external threat intelligence (by "external," we mean sourced outside of the organization's own infrastructure).

The most common use of threat intelligence is "To improve our ability to detect indicators of attack (IoAs) and indicators of compromise (IoCs)," cited by 55.4% of respondents (see Figure 48). This result reflects the fact that operational and technical threat intelligence sources, such as databases of vulnerabilities, malware signatures, and indicators of attacks, are critical raw materials for many enterprise security products (such as firewalls, IDS/IPS systems, anti-malware products, and security analytics tools).

Section 4: Practices and Strategies

Number two on the list is "To prioritize vulnerabilities and exposures to reduce our attack surface" (49.5%). Threat intelligence informs security teams about newly discovered weaknesses they need to look for in their infrastructure. And because not all threats are equally serious or affect everyone, intelligence helps prioritize the ones to focus on for detection and remediation.

The third major use of threat intelligence is "To uncover threat actors impersonating our websites and social media accounts" (46.5%). This relates to "brand protection" or "digital brand protection." Brand protection involves detecting and taking down websites, social media accounts, and mobile apps resembling an organization's real digital assets. These fake assets are created by cybercriminals to defraud customers, steal account numbers and access credentials, or sell counterfeit goods. Threats to the brand also involve social media posts and accounts created by hackers who impersonate the organization's employees to spread disinformation. It takes specialized skills and tools to find these websites and social media accounts, so most enterprises that are worried about them rely on external threat intelligence suppliers.

Other important use cases are obtaining intelligence about vulnerabilities and compromises at vendors and other supply chain partners (valuable information for third-party risk management, or TPRM), and understanding threat actor groups' tactics, techniques, and procedures (TTPs) (critical intelligence for incident response and threat hunting).

Discovering data breaches and stolen credentials on the dark web is not as common as the other use cases in this list. However, we think more organizations will make use of that kind of threat intelligence in the future.

Our data also shows that external threat intelligence is clearly a must-have. Almost all organizations in our survey (97.3%, to be precise) are leveraging it for one or more of these use cases (see Figure 49).

Figure 49: Percentage of organizations that leverage external threat intelligence.

Section 4: Practices and Strategies

Board Members with a Cybersecurity Background

Does at least one member of your company's board of directors have a cybersecurity background?

There have been a lot of stories in the press about the elevation of cybersecurity to a board-level issue. There are also discussions about IT security getting "a seat at the table" with upper management and boards. But is that really happening?

The short answer: yes, a lot. In our survey, 62.2% of respondents at organizations that have a board of directors said that at least one member has a cybersecurity background (see Figure 50).

Do security professionals think it makes a difference to have a board member with cybersecurity experience? Our data shows that most do. Of the respondents who said their organization did not have one, roughly four of five said it would help. Only 19.6% said they didn't think it would make a difference (see Figure 51).

The fact that three out of five boards include a person with knowledge about cybersecurity challenges and technology is extremely important. It means there is likely to be a champion among the directors for cybersecurity budget and staffing requests, and someone who can help non-technical board members understand the issues and trade-offs involved. This scenario also improves communication in the other direction by providing someone who can help IT groups better understand the point of view of company leaders and the role of cybersecurity in supporting the organization's business initiatives.

The percentage of organizations with cybersecurity experience on their boards differs significantly across countries (see Figure 52). The leaders are Brazil (90.3%), Mexico (87.9%), and China (86.0%), while the laggards are Germany (51.4%), Italy (43.8%), and Canada (43.5%).

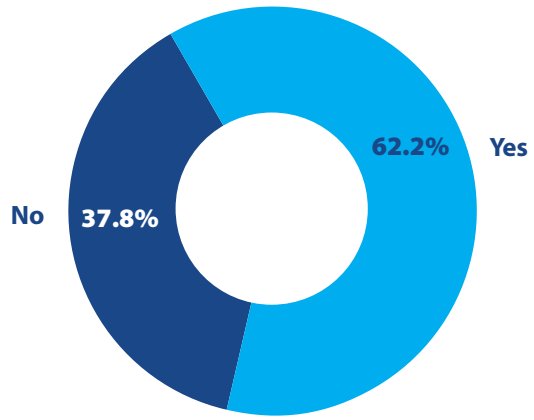


Figure 50: Answer to question "Does at least one member of your company's board of directors have a cybersecurity background?" (Excludes organizations that don't have a board of directors.)

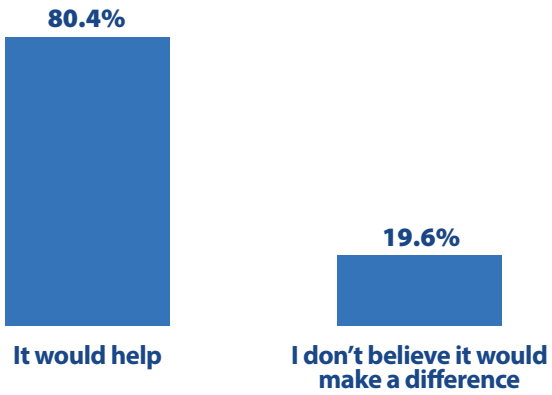


Figure 51: Would having a board member with a cybersecurity background make a difference? (Includes only organizations with a board of directors that doesn't include a member with a cybersecurity background.)

Section 4: Practices and Strategies

Across major industries, board representation is highest in technology (68.8%), manufacturing (66.9%), and finance (65.0%), and lowest in healthcare (48.9%) and government (44.4%) (see Figure 53). Of course, we would expect government agencies to be outliers because they don't have the same type of boards as commercial enterprises.

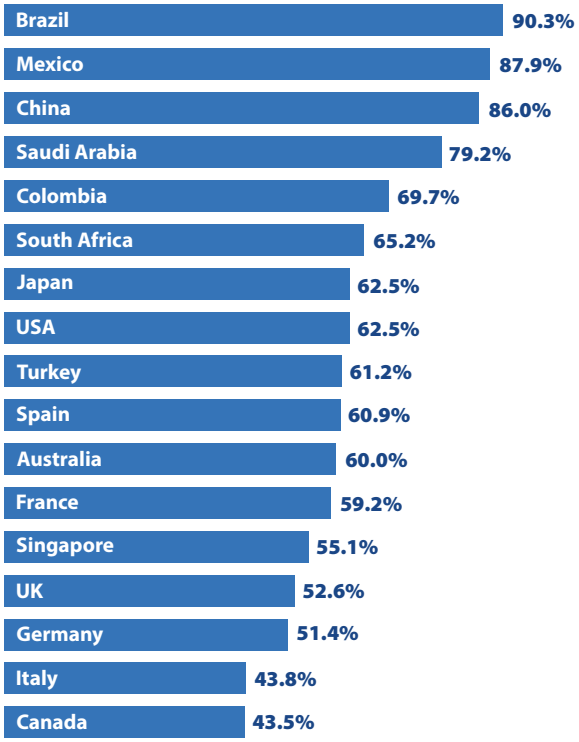


Figure 52: Organizations with a member of the board with a cybersecurity background, by country.

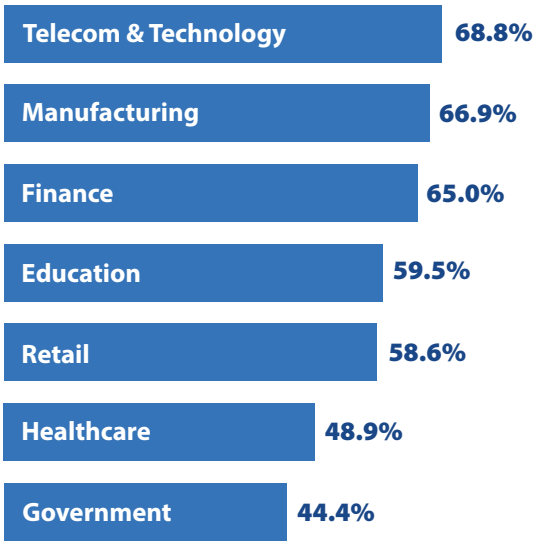


Figure 53: Organizations with a member of the board with a cybersecurity background, by industry.

"There are discussions of IT security getting 'a seat at the table' with upper management and boards. But is that really happening? The short answer: yes, a lot. In our survey, 62.2% of respondents at organizations that have a board of directors said that at least one member has a cybersecurity background."

Section 4: Practices and Strategies

Emerging IT Security Technologies and Architectures

Describe your organization's deployment plans for each of the following emerging IT security technologies/architectures.

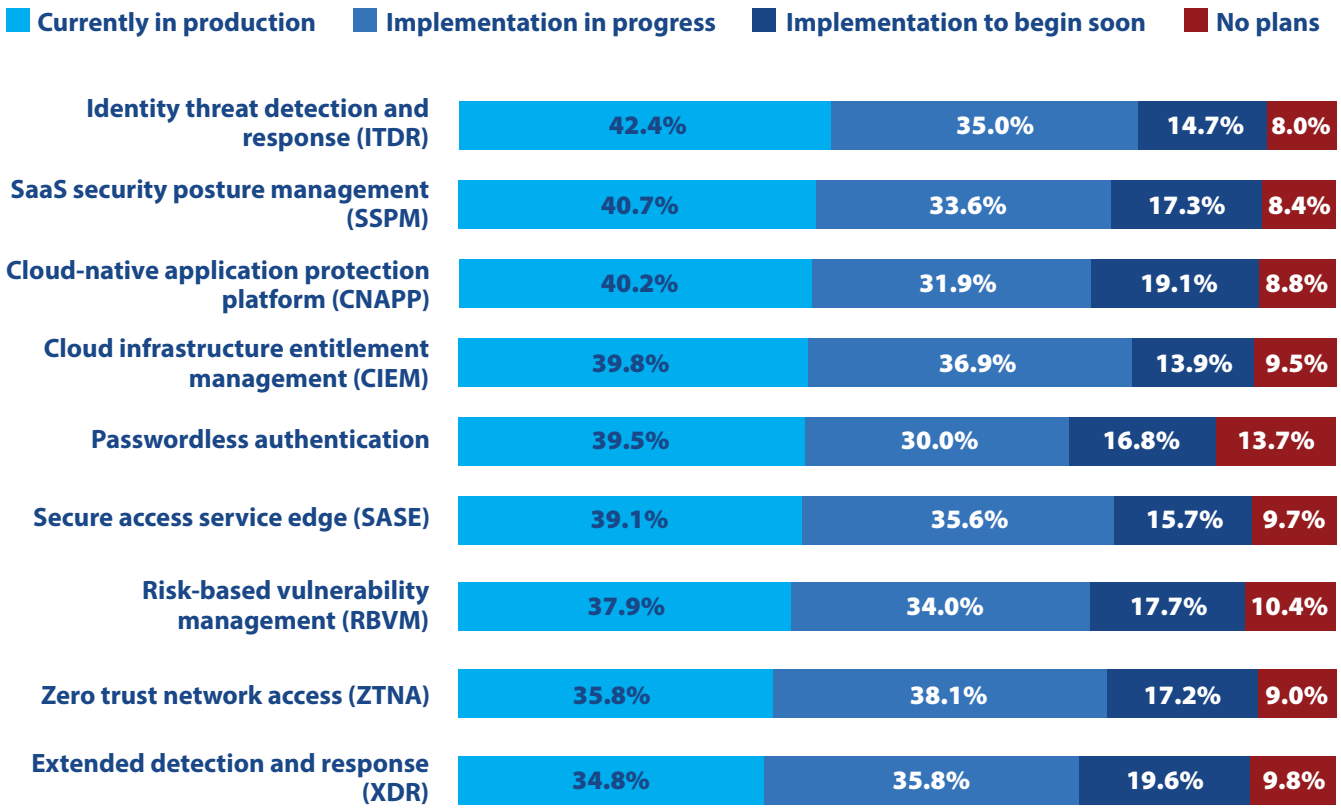


Figure 54: Plans for implementing emerging IT security technologies and architectures.

The final question in this survey examines how many organizations have implemented, or plan to implement, nine emerging IT security technologies and architectures (see Figure 54).

The technology farthest along in deployment is identity threat detection and response. ITDR solutions protect identity information and identity stores that are central to identity management and zero trust security. ITDR is currently in production in 42.4% of organizations, and implementation is in progress in 35.0% more.

By the way, you may have noticed that eight of the nine technologies and architectures discussed here have names so long that we almost always refer to them by their acronyms.

Second on the list is SaaS security posture management. SSPM products monitor and manage security issues in SaaS applications. They are in production in 40.7% of organizations and are being implemented in an additional 33.6%.

Section 4: Practices and Strategies

Next come two technologies that enhance security in cloud environments. A cloud-native application protection platform (CNAPP) combines a variety of capabilities for monitoring and managing security of cloud-based applications, and promoting DevSecOps practices for developing secure cloud applications. A cloud infrastructure entitlement management (CIEM) product manages identities and entitlements for cloud-based applications and services. CNAPP and CIEM solutions are in production in 40.2% and 39.8% of organizations, and are being implemented in 31.9% and 36.9% more, respectively.

Passwordless authentication (hey, no acronym needed!), as the name suggests, provides authentication without relying on passwords, usually through the use of biometrics and special keys. Eliminating passwords improves security dramatically while making life easier for users. Passwordless authentication is currently in production in 39.5% of organizations and implementation is in progress at 30.0% more.

Secure access service edge architectures combine SD-WAN networking services with a variety of security tools to ensure secure communications for distributed offices and users. The in-production and being-implemented figures for SASE are 39.1% and 35.6%.

Risk-based vulnerability management (RBVM) solutions not only discover but also prioritize and remediate unpatched systems, misconfigurations, and other vulnerabilities. Of the organizations in this survey, 37.9% are using RBVM now and 34.0% are working on deployment.

Zero trust network access (ZTNA) refers to technologies and architectures that assess all access requests based on multiple risk factors and control access based on the principle of least privilege. ZTNA frameworks are currently deployed in 35.8% of organizations and implementation is in progress in 38.1% more.

Extended detection and response (XDR) products combine multiple security tools that work together to detect attacks and provide data so organizations can respond faster. They are in production in 34.8% of organizations and are being implemented in 35.8% more.

One note on reading Figure 54. Because the chart sequences the items in this question based on their "currently in production" percentage, some of the technologies and architectures getting the most press attention from security professionals appear in the middle or near the bottom of the list. However, the picture changes if you look at their rates for "implementation in progress." For example, ZTNA has the most implementations in progress, with XDR and SASE in the third and fourth positions by that measure.

Ten Years Behind Us – Looking Back on a Decade of CDR Data

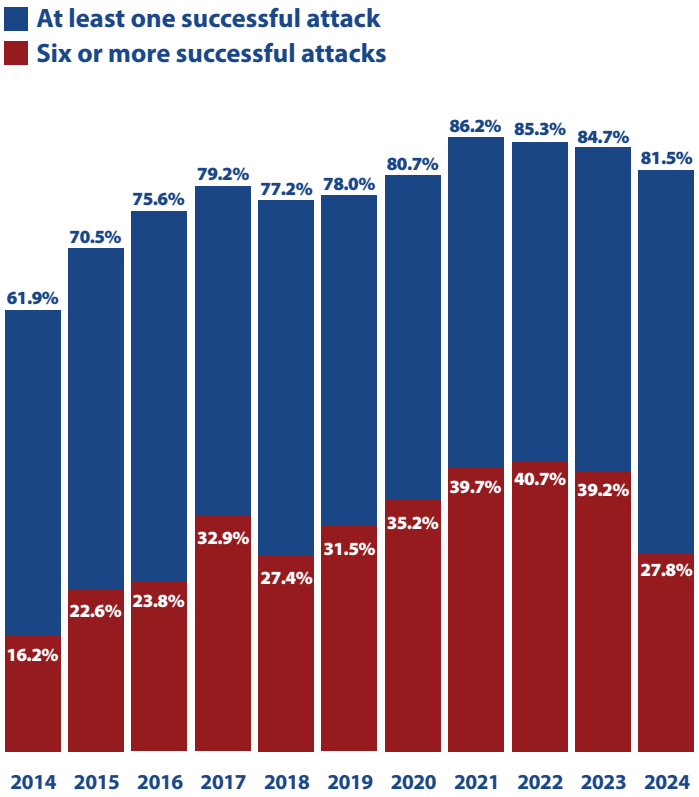
Tired of lying in the sunshine staying home to watch the rain.
You are young and life is long and there is time to kill today.
And then one day you find ten years have got behind you.
No one told you when to run, you missed the starting gun.

– Lyrics from *Time* by Pink Floyd

We now have 10 years of Cyberthreat Defense Reports behind us. CyberEdge published the first one in the spring of 2014. Every year since then we have introduced some new questions and retired others, but we kept a core set of topics that have carried through since 2014. We thought it would be interesting to see how the answers to three of those questions have changed over the decade, and what those changes tell us about the state of cyber defense.

How many times do you estimate that your organization's global network has been compromised by a successful cyberattack within the past 12 months?

This has been one of the cornerstone questions of the CDR since the beginning. The chart at right (also presented as Figure 1 on page 7) shows how many organizations have experienced one or more attacks, and how many have been victimized by six or more. There was a strong upward trend from 2014 through 2021, indicating that threat actors were pulling ahead in their arms race with defenders during that period. Then, in the 2022 CDR the trend lines flattened, and have decreased over the last two years. Although successful attacks remain at a historically high level, the data demonstrates an extremely important turning point (assuming the downward trend persists).

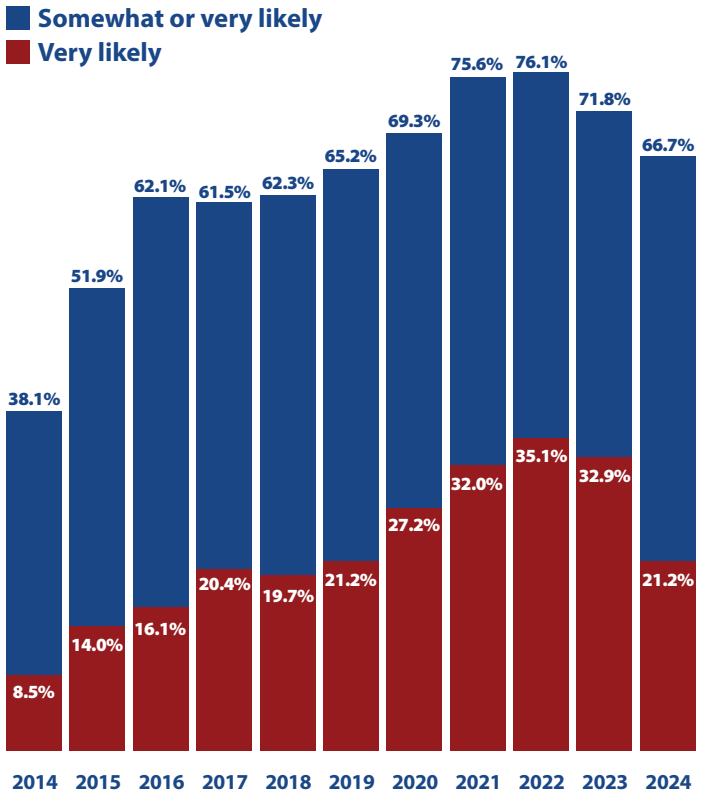


Percentage of organizations experiencing at least one successful attack and those experiencing six or more. (Figure 1 on page 7)

Ten Years Behind Us – Looking Back on a Decade of CDR Data

What is the likelihood that your organization's network will become compromised by a successful cyberattack in 2024?

The chart at right (also shown as Figure 5 on page 9) is about expectations for the coming year. In retrospect, it is amazing how optimistic we were in 2014: only 8.5% of respondents thought a successful attack was "very likely"! However, from 2015 to 2022 expectations rapidly adjusted to the reality of the increasing successes of threat actors. Now the tide appears to be turning, although if we compare Figure 1 (actual successful attacks) with Figure 5 (expected successful attacks), it looks like expectations for improvement may be overshooting reality.



Percentage of organizations indicating that compromise by a successful cyberattack in 2024 is somewhat or very likely. (Figure 5 on page 9)

Ten Years Behind Us – Looking Back on a Decade of CDR Data

On a scale of 1 to 5, with 5 being highest, rate your organization's overall security posture (ability to defend against cyberthreats) in each of the following IT components.

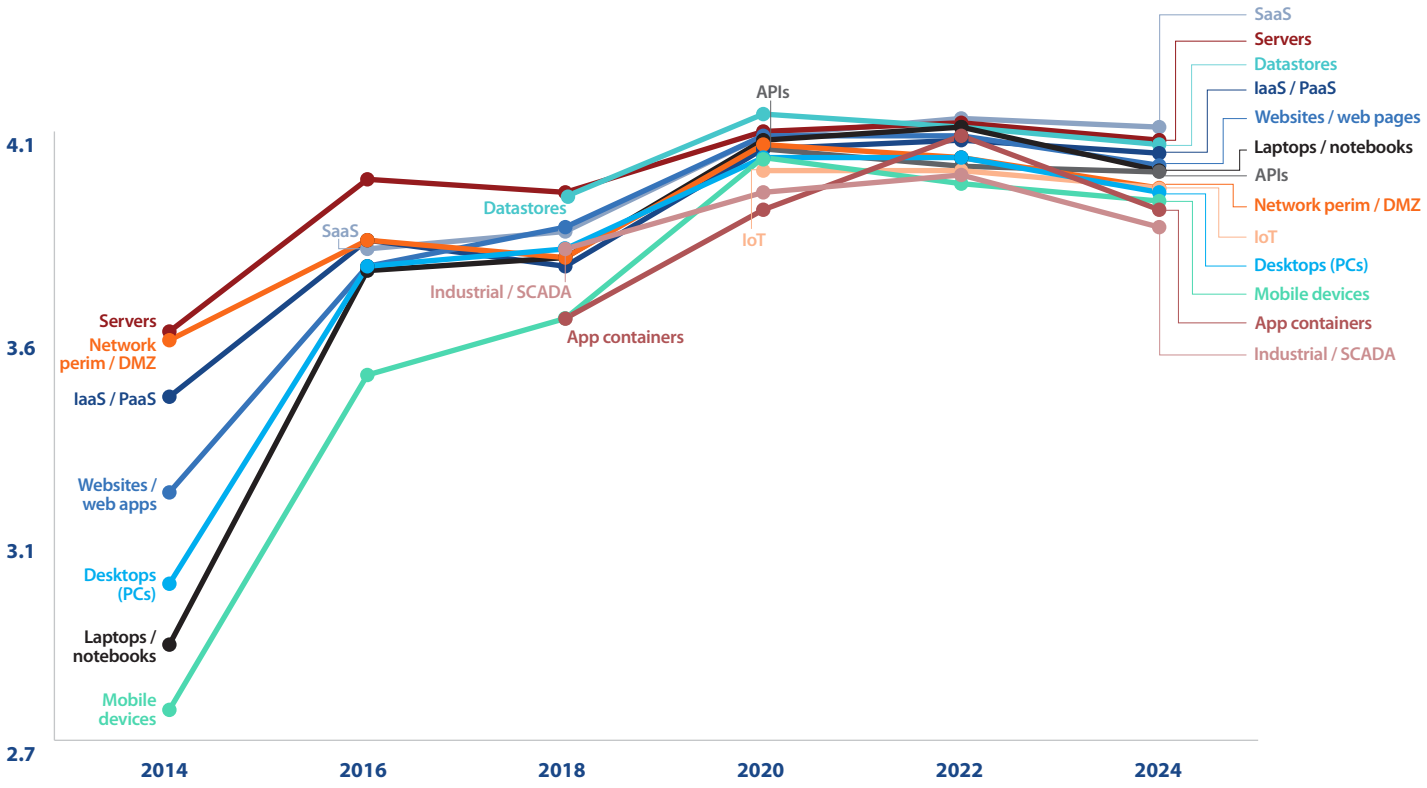


Figure 55: Perceived security posture by IT domain: On a scale of 1 to 5, with 5 being highest, rate your organization's overall security posture (ability to defend against cyberthreats) in each of the following IT components.

Figure 55 contains a lot of data – the perceived security posture across 13 IT domains for 10 years. But it points to a few interesting patterns:

- Confidence in security posture moved up dramatically between 2014 and 2020. Since then, various domains have changed places on the list, but overall levels of confidence in the security posture of different domains have remained about the same.
- The range of scores has narrowed dramatically between 2014 and 2024. In 2014 scores ranged between 2.77 and 3.64, a span of .97. In 2024 the range is between 3.88 and 4.11, a span of only .23. We think the reason is that security groups have been investing in products and processes to shore up the weakest areas, as well as making improvements in technologies to protect mobile and remote devices and individual workstations.

The Road Ahead

AI Swords and Shields

The impact of artificial intelligence is just now starting to be felt. There is no doubt that AI technologies will transform existing cyber battlegrounds between threat actors and security teams. Our survey includes input from security professionals about likely uses and abuses of AI (see pages 21-26). However, it is very likely AI will also have effects that few people, if any, can anticipate. We are paying very close attention to these developments, and so should everyone concerned with cybersecurity.

AI and Cybersecurity Jobs

All of us should be asking ourselves, "Could AI do my job?"

Most security professionals should not be overly concerned, for two reasons:

- Many cybersecurity jobs require knowledge, judgment, and experience that cannot be replicated by AI, at least not yet.
- There is still a significant shortage of experienced cybersecurity people (see pages 15 and 30), so even in areas where AI boosts productivity, the immediate effect will be to bring supply and demand into balance, rather than to cause layoffs.

However, some cybersecurity jobs involve tasks that AI can perform very effectively. Examples are collecting and classifying data, looking for vulnerabilities in configurations and code, and carrying out incident response playbooks and remediation processes.

There is little doubt that security groups will look to leverage AI in these areas. But when that happens, we believe they should make a strong effort to retrain affected security professionals so they can fill vacancies in roles that AI can't take over. Retraining will be cost-effective (not to mention good for morale) compared to laying off people in one area while running expensive searches to hire outsiders.

New Regulations Taking Effect

Enough about probabilities and contingencies. Let's talk about some inevitabilities. A bunch of new regulations and industry standards (or major revisions) have come into force recently or will do so soon. Among them:

U.S. Securities and Exchange Commission rules requiring public companies to make additional disclosures about the nature, scope, and timing of material cybersecurity incidents, as well as to report annually on their cybersecurity risk management, strategy, and governance. The SEC also adopted rules requiring foreign private issuers to make comparable disclosures. The new rules go into effect at different times in 2024.

The Payment Card Industry Data Security Standard (PCI DSS) v4.0 includes a load of new requirements for ecommerce companies, financial institutions, and other firms that handle payment card data. The new rules relate to secure authentication, identity and access management, encryption, web application protection, risk management, compliance testing and reporting, and other areas. Some of the new requirements become active on March 31, 2024, and others on March 31, 2025.

The European Union Network and Information Security 2 (NIS2) Directive expands the scope of EU cybersecurity rules to cover more companies, requires more incident reporting, and adds requirements for companies to address security risks related to supply chains and supplier relationships, among other changes. In addition, top executives will have to take responsibility for their organization's cybersecurity maturity. EU member states will have until October 17 to pass national legislation to enforce the provisions.

The EU Digital Operational Resilience Act (DORA) covers cybersecurity and risk management for financial institutions and their third-party service providers operating in the EU. A new draft of technical standards extends rules covering protection, detection, containment, recovery, and repair capabilities for information and communication technology. The compliance deadline is January 17, 2025.

The Road Ahead

These and other regulatory updates, and the increased transparency mandated by some of them, will force many organizations to add or upgrade security technologies and processes.

Hot War, Cold War, Proxy War, Cyberwar

We sincerely hope that none of what we are about to discuss happens. But today there is a risk that an active military conflict, or a behind-the-scenes struggle between nations, or the activities of rebels or terrorists supported by a regional power, will spill over to active fighting in cyberspace.

The nature and dimensions of such cyberwars are hard to predict. But if they occur, they are likely to involve a combination of disruption and disinformation. Also, the "blast radius" could be much wider than most people realize.

There are quite a few potential targets:

In the opposing country

- Political leaders
- Military organizations
- Companies in the defense industrial base (DIB)
- Transportation and infrastructure firms
- Media and communications outlets
- Financial institutions

In other countries

- Political leaders who back the opposing country
- Military organizations that funnel weapons and ammunition to the opposing country
- Financial institutions involved in funding or handling cash flows for the opposing country
- Companies that supply the opposing country's DIB
- Media and communications outlets that support the opposing country
- Transportation and infrastructure firms that carry supplies to the opposing country
- Ecommerce companies, retailers, fast food and packaged food companies, energy producers, telecom and technology firms, pharmaceutical companies, automakers, professional services firms, arts and entertainment organizations, etc., which are perceived as supporting the opposing country, its military, or its ideology.

In short, nearly every large organization, everywhere, even with no obvious link to politics or defense work, could become a target.

What are the implications? Organizations of all types should look carefully at the possibility that they might be targeted by participants in a hot, cold, or proxy war. They should consider what regions, what types of threats (such as DDoS attacks, attempts to steal intellectual property, attacks on operations, or misinformation and propaganda spread through counterfeit or compromised websites and social media accounts), and what monetary and reputational costs could be involved. Some organizations may only need to broaden the scope of existing risk management or geopolitical intelligence activities, but others might want to create a new working group or steering committee to assess the contingencies.

Again, we *hope* this exercise won't be needed, but we *fear* that lack of preparation could have unexpected costs.

Appendix 1: Survey Demographics

This year's report is based on survey results obtained from 1,200 qualified participants hailing from 17 countries (see Figure 56) across six major regions (North America, Europe, Asia Pacific, Latin America, the Middle East, and Africa). Each participant has an IT security job role (see Figure 57). This year, 37.6% of our respondents held CIO, CISO, or other IT security executive positions.

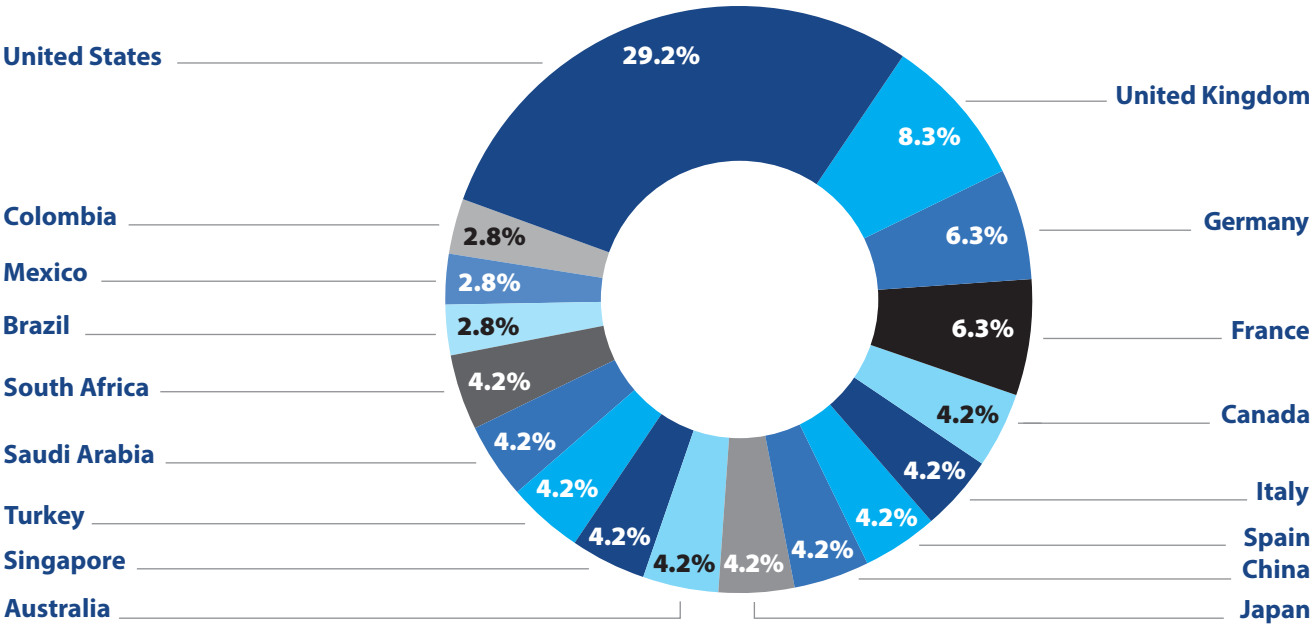


Figure 56: Survey participants by country.

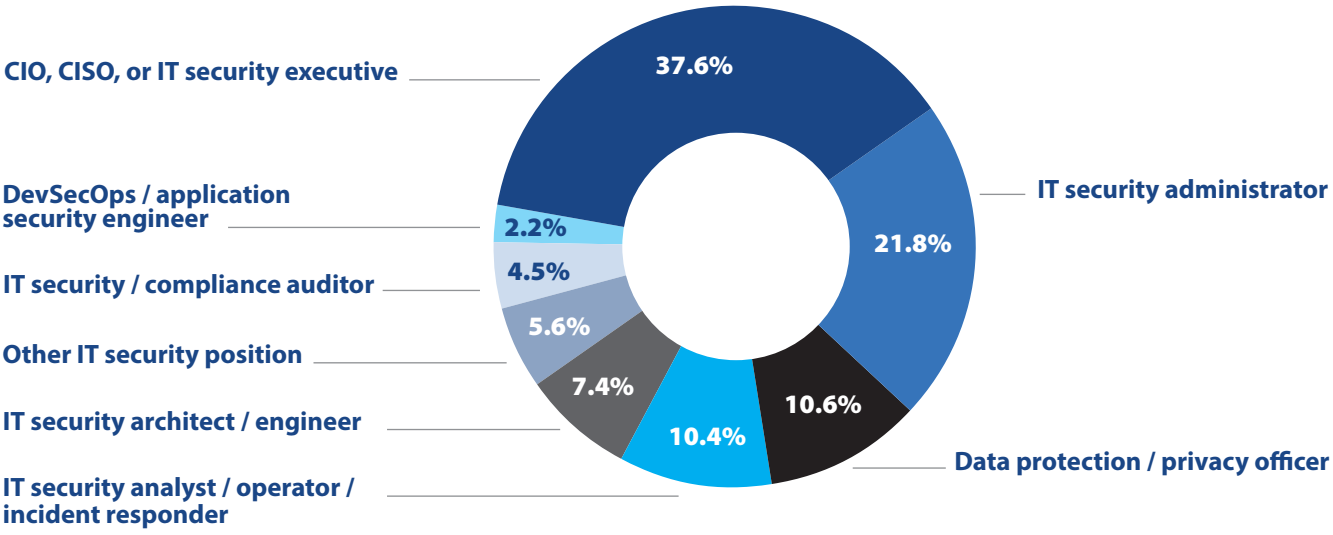


Figure 57: Survey participants by IT security role.

Appendix 1: Survey Demographics

This study addresses perceptions and insights from research participants employed with commercial and government organizations with 500 to 25,000+ employees (see Figure 58). A total of 19 industries (plus "Other") are represented in this year's study (see Figure 59). The big 7 industries – education, finance, government, healthcare, manufacturing, retail, and telecom & technology – accounted for two-thirds of all respondents. No single industry accounted for more than 15.3% of participants.

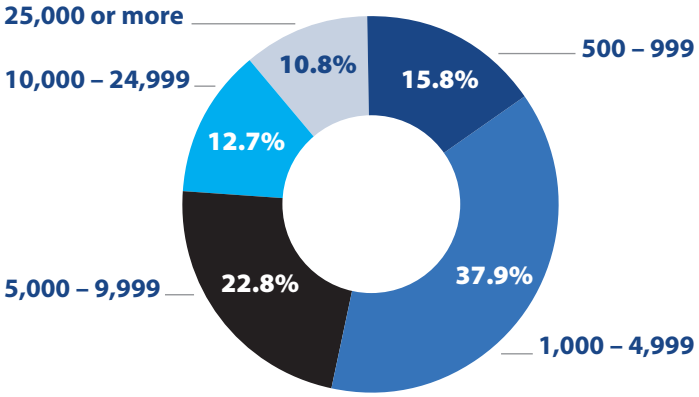


Figure 58: Survey participants by organization employee count.

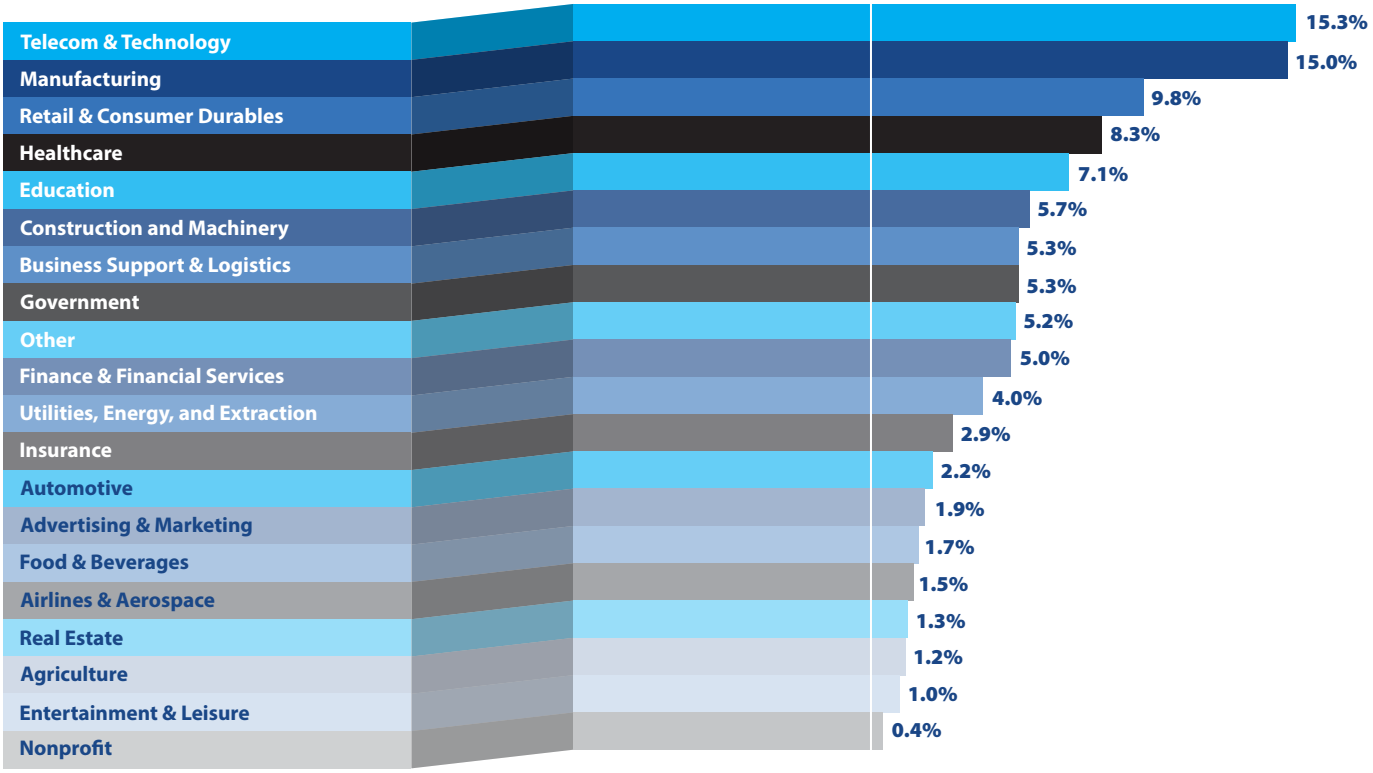


Figure 59: Survey participants by industry.

Appendix 2: Research Methodology

CyberEdge developed a 27-question, web-based, vendor-agnostic survey instrument in partnership with our research sponsors. The survey was completed by 1,200 IT security professionals in 17 countries and 19 industries in November 2023. The global margin of error for this research study (at a standard 95% confidence level) is 3%. All results pertaining to individual countries and industries should be viewed as anecdotal, as their sample sizes are much smaller. CyberEdge recommends making actionable decisions based on global data only.

All respondents had to meet two filter criteria: (1) they had to have an IT security role; and (2) they had to be employed by a commercial or government organization with a minimum of 500 global employees.

At CyberEdge, survey data quality is paramount. CyberEdge goes to extraordinary lengths to ensure its survey data is of the highest caliber by following these industry best practices:

- Ensuring that the right people are being surveyed by (politely) exiting respondents from the survey who don't meet the respondent filter criteria of the survey (e.g., job role, job seniority, company size, industry)
- Ensuring that disqualified respondents (who do not meet respondent filter criteria) cannot restart the survey (from the same IP address) in an attempt to obtain the survey incentive
- Constructing survey questions in a way that eliminates survey bias and minimizes the potential for survey fatigue
- Only accepting completed surveys after the respondent has provided answers to all of the questions
- Ensuring that respondents view the survey in their native language (e.g., English, German, French, Spanish, Japanese, Chinese)
- Randomizing survey responses, when possible, to prevent order bias
- Adding "Don't know" (or comparable) responses, when possible, so respondents aren't forced to guess at questions they don't know the answer to
- Eliminating responses from "speeders" who complete the survey in a fraction of the median completion time
- Eliminating responses from "cheaters" who apply consistent patterns to their responses (e.g., A,A,A,A and A,B,C,D,A,B,C,D)
- Ensuring the online survey is fully tested and easy to use on computers, tablets, and smartphones

CyberEdge would like to thank our research sponsors for making this annual research study possible and for sharing their IT security knowledge and perspectives with us.

Appendix 3: Research Sponsors

CyberEdge is grateful for its Platinum, Gold, and Silver sponsors, for without them this report would not be possible.

Platinum Sponsors

Cloudflare | www.cloudflare.com

Cloudflare is the leading connectivity cloud company. It empowers organizations to make their employees, applications and networks faster and more secure everywhere, while reducing complexity and cost. Cloudflare's connectivity cloud delivers the most full-featured, unified platform of cloud-native products and developer tools, so any organization can gain the control they need to work, develop, and accelerate their business.

CyberArk | www.cyberark.com

CyberArk is the global leader in identity security. Centered on intelligent privilege controls, CyberArk provides the most comprehensive security offering for any identity – human or machine – across business applications, distributed workforces, hybrid cloud environments and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

Google Cloud | cloud.google.com

Make Google part of your security team with Mandiant frontline experts, intel-driven security operations, and a secure cloud platform — all supercharged by AI. Google Cloud Security helps organizations address their security challenges with many of the same capabilities Google uses to keep more people and organizations safe online than anyone else in the world: frontline intelligence and expertise, a modern, intel-driven security operations platform, and a secure-by-design cloud foundation. AI enhances all of these components, personalizing intelligence for your business, automating manual tasks, and assisting security professionals in effectively addressing complex cases.

Imperva | www.imperva.com

Imperva, a leading global cybersecurity company, protects and provides secure, data-driven insights to businesses worldwide. Imperva's advanced technology defends critical systems from cyber threats, ensuring the safety of business operations. Imperva's solutions offer robust protection for applications and APIs anywhere, delivering unparalleled security without compromising operational efficiency. With a commitment to innovation and customer-centric service, Imperva empowers businesses to thrive in an increasingly digital world.

ISC2 | www.isc2.org

ISC2 is an international nonprofit membership associate focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, ISC2 offers a portfolio of credentials that are a part of a holistic, pragmatic approach to security. Our association of candidates, associates and members, more than 600,000 strong, is made up of certified cyber, information software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is support by our commitment to educate and reach the general public through our charitable foundation – *The Center for Cyber Safety and Education™*.

Proofpoint | www.proofpoint.com

Proofpoint is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 80 percent of the Fortune 100, rely on Proofpoint for human-centric security to mitigate their most critical risks across email, the cloud, social media and the web.

Appendix 3: Research Sponsors

Gold Sponsors

BlueCat Networks | www.bluecatnetworks.com

BlueCat helps enterprises achieve their network modernization objectives by delivering innovative products and services that enable networking, security, and DevOps teams to deliver change-ready networks with improved flexibility, automation, resiliency, and security. BlueCat's growing portfolio includes services and solutions for automated and unified DDI management, network security, multicloud management, and network observability and health. BlueCat's DDI management platform was recognized as a market leader and outperformer in GigaOm's 2022 and 2023 Radar reports.

Delinea | www.delinea.com

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, granting access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies.

OpenText | www.opentext.com

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

SailPoint Technologies | www.sailpoint.com

SailPoint equips the modern enterprise to effortlessly manage and secure access to applications and data through the lens of identity – at speed and scale. As the category creator, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency. SailPoint helps the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.

ThreatX | www.threatx.com

ThreatX is managed API and application protection, *from edge to runtime,* that lets you secure them with confidence, not complexity. It blocks botnets and advanced attacks in real time, helping organizations keep attackers at bay without lifting a finger.

Tufin | www.tufin.com

Tufin provides a single platform for network and cloud security teams to simplify the management of security policies across today's complex, multi-vendor hybrid networks. The platform gives some of the largest companies in the world the end-to-end visibility and automation tools necessary to swiftly provide new access, enable fast and secure application deployment, and ensure continuous compliance and audit readiness. Tufin's proven solutions have helped more than 2,900 customers across industries including healthcare, financial services, utilities, telecommunications and retail to quickly identify and mitigate network risks.

Appendix 3: Research Sponsors

Silver Sponsors

Axiad | www.axiad.com

Axiad delivers security-first authentication technologies that help organizations protect users, machines, assets, and interactions. Axiad customers optimize their cybersecurity posture while they navigate underlying IT complexities, from cloud to on-prem to hybrid infrastructures, and maintain overarching regulatory requirements like FedRAMP, CMMC and AAL3. Axiad's unique password-less orchestration features, like MyCircle and Airlock, remove friction and overhead from enterprise-wide authentication management. The company's flagship offering, Axiad Cloud, is a comprehensive, secure, and integrated authentication platform that supports the widest range of credentials in the industry including FIDO, mobile MFA, Windows Hello for Business, YubiKeys, smart cards, TPM and biometrics.

Legit Security | www.legitsecurity.com

Legit is a new way to manage your application security posture. With Legit, enterprises get a cleaner, easier way to manage and scale application security, and address risks from code to cloud. Built for the modern SDLC, Legit tackles the toughest problems facing security teams. Fast to implement and easy to use, Legit lets security teams protect their software factory from end to end, gives developers guardrails that let them do their best work safely, and delivers metrics that prove the success of the security program. This approach means teams can control risk across the business – and prove it.

Netwrix | www.netwrix.com

Netwrix champions cybersecurity to ensure a brighter digital future for any organization. Netwrix's innovative solutions safeguard data, identities, and infrastructure reducing both the risk and impact of a breach for more than 13,500 organizations across 100+ countries. Netwrix empowers security professionals to face digital threats with confidence by enabling them to identify and protect sensitive data as well as to detect, respond to, and recover from attacks.

Phosphorus Cybersecurity | www.phosphorus.io

Phosphorus Cybersecurity® is the leading CPS Protection Platform delivering a proactive approach to discovery and security management for the expanding IoT, OT, IIoT, and IoMT attack surface. Our Unified xIoT Security Management Platform is designed to safely secure, manage, and operate the growing world of unknown and unmanaged Cyber-Physical Systems. The agentless, software-based platform provides unmatched Intelligent Active Discovery and security management across every industry environment and vertical—delivering high-fidelity discovery and risk assessment, proactive hardening and remediation, comprehensive security management, and real-time operational health monitoring.

Picus Security | www.picussecurity.com

At Picus, we help organizations continuously validate the effectiveness of their security controls so that they can obtain a holistic view of their security posture and take swift action to strengthen it. As the pioneer of Breach and Attack Simulation (BAS), our technology is trusted by security teams worldwide to deliver actionable insights and recommendations needed to enhance threat prevention and detection 24/7. To minimize breaches, we believe that security control validation must be an essential part of SecOps and have developed Picus' "The Security Validation Platform," which provides granular and actionable insights for operational and executive teams and optimizes return on investment and keeps the risk of getting breached consistently low.

Reveal Security | www.reveal.security

Reveal Security quickly and accurately detects identity threats post-authentication in and across SaaS applications and cloud services. The Reveal Security ITDR platform is the only solution in the market based on patented Identity Journey Analytics™ technology that uses unsupervised machine learning to continuously analyze the activity of human and machine identities in applications and detect anomalies. This approach delivers a superior level of accuracy and context, reduces alert volumes by orders of magnitude, and enables the business to respond quickly before a material breach can occur.

Appendix 4: About CyberEdge Group

Founded in 2012, CyberEdge Group is the largest research, marketing, and publishing firm to serve the IT security vendor community.

CyberEdge's highly acclaimed Cyberthreat Defense Report (CDR) and other single- and multi-sponsor survey reports have garnered numerous awards and have been featured by both business and technology publications alike, including *The Wall Street Journal, Forbes, Fortune, USA Today, NBC News, ABC News, SC Magazine, DarkReading,* and *CISO Magazine.*

CyberEdge has cultivated its reputation for delivering the highest-quality survey reports, analyst reports, white papers, and custom books and eBooks in the IT security industry. Our highly experienced, award-winning consultants have in-depth subject matter expertise in dozens of IT security technologies, including:

- Advanced Threat Protection (ATP)
- Application Security
- Cloud Security
- Data Security
- Deception Technology
- DevSecOps
- DoS/DDoS Protection
- Endpoint Security (EDR & EPP)
- ICS/OT Security
- Identity and Access Management (IAM)
- Intrusion Prevention System (IPS)
- Managed Security Services Providers (MSSPs)
- Mobile Application Management (MAM)
- Mobile Device Management (MDM)
- Network Behavior Analysis (NBA)
- Network Detection & Response (NDR)
- Network Forensics
- Next-generation Firewall (NGFW)
- Patch Management
- Penetration Testing
- Privileged Account Management (PAM)
- Risk Management/Quantification
- Secure Access Service Edge (SASE)
- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Security Analytics
- Security Configuration Management (SCM)
- Security Information & Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)
- Software-defined Wide Area Network (SD-WAN)
- SSL/TLS Inspection
- Supply Chain Risk Management
- Third-party Risk Management (TPRM)
- Threat Intelligence Platforms (TIPs) & Services
- User and Entity Behavior Analytics (UEBA)
- Unified Threat Management (UTM)
- Virtualization Security
- Vulnerability Management (VM)
- Web Application Firewall (WAF)
- Zero Trust Network Access (ZTNA)

For more information about CyberEdge and our services, call us at 800-327-8711, email us at info@cyber-edge.com, or connect to our website at www.cyber-edge.com.

CyberEdge Acceptable Use Policy

CyberEdge Group, LLC ("CyberEdge") encourages third-party organizations to incorporate textual and graphical elements of this report into presentations, reports, website content, product collateral, and other marketing communications without seeking explicit written permission from CyberEdge, provided such organizations adhere to this acceptable use policy.

The following rules apply to referencing textual and/or graphical elements of this report:

1. **Report distribution.** Only CyberEdge and its authorized research sponsors are permitted to distribute this report for commercial purposes. However, organizations are permitted to leverage the report for internal uses, including training.
2. **Source citations.** When citing a textual and/or graphical element from this report, you must incorporate the following statement into a corresponding footnote or citation: "Source: 2024 Cyberthreat Defense Report, CyberEdge Group, LLC."
3. **Quotes and excerpts.** Quotes and excerpts extracted from this report must not be modified in any way. Rephrasing is not permitted.
4. **Figures and tables.** Figures and tables extracted from this report must not be modified in any way. Artwork for figures and tables for the most recent Cyberthreat Defense Report are available for download at no charge on the CyberEdge website at https://www.cyber-edge.com/cdr.
5. **No implied endorsements.** CyberEdge does not endorse technology vendors. Cited CyberEdge content should never be used to imply favor from CyberEdge.

If you have questions about this policy or would like to incorporate content from this report in a manner not addressed by this policy, submit an email to research@cyber-edge.com.