CYBEREDGE GROUP®

2025 Cyberthreat Defense Report

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

<< Research Sponsors >>

PLATINUM

CLOUDFLARE

Delinea

Google Cloud

ISC2

GOLD

ABSOLUTE

hackerone

illumio

Secureworks a SOPHOS company

SILVER

AGILEBLUE

Dataminr

INTEL471

KEEPER

MEDIA SPONSOR

SECURITY BUZZ

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.

More than 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 2025

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

1. **Have we turned the corner?** The percentage of organizations experiencing at least one successful cyberattack trended upward from our 2016 CDR to the 2021 edition. So did the percentage suffering from six or more. And so did the percentage of organizations that expected to be compromised at least once in the coming year. But those three metrics essentially plateaued between 2021 and 2023 and then dropped to a lower plateau in the 2024 report and this one. It's too early to let our guard down, but it does seem like the factors working in favor of cybersecurity teams (like large investments in cloud security during the COVID pandemic, the application of zero trust principles, a renewed interest in cybersecurity basics, and AI embedded in security products) are now matching or even outpacing the factors working for threat actors.

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 Coming Up Everywhere.** Our survey has one question specifically about AI, asking respondents about the strength of their preference for purchasing security products that feature AI technologies (see page 37). But AI comes up in many places in this report: as a force helping cybersecurity teams in their work (page 8), as a factor helping threat actors (page 17), as a tool to detect fraud and foil web application and mobile attacks (page 19), as a tool to filter out false positive alerts (page 24), as a technology embedded in secure email gateways to flag abnormal behaviors (page 42), and as the driver of a long-term arms race between threat actors and cybersecurity teams (page 57). In many ways this dynamic mirrors how enterprises are starting to benefit from AI: not by acquiring "AI products," but by leveraging AI capabilities embedded in security solutions and platforms.

3. **Twists and Turns for Ransomware.** It's hard to summarize the changing dynamics of ransomware this year. After rising for a decade, the percentage of organizations affected by ransomware fell for the second year in a row (good news ☺), but average ransom demands have continued to rise (bad news ☹). The percentage of victimized organizations that paid ransoms fell (probably good news ☺), but the percentage of ransom payers who recovered their data fell (bad news ☹). If you want to know the factors we think are behind these gyrations, see pages 20-22.

Introduction

4. **The Never-ending Skills Shortage.** The lack of experienced cybersecurity personnel has been a running theme in CDRs for years. In this report it comes up in a tie for first among factors inhibiting organizations from adequately defending themselves against cyberthreats (page 23) and as the biggest challenge for attack surface management (ASM) (page 25). Also, it turns out there is a huge demand worldwide for entry-level security fundamentals courses and certifications (see page 30), most likely because organizations that can't find enough experienced cybersecurity professionals in the marketplace are trying to train their own. While this shortage can be a big headache for cybersecurity managers, it also has a significant benefit: it provides incentives for adding more automation and autonomous decision-making capabilities to security products. In time, these will improve security and reduce the gap between cybersecurity jobs and the people who can perform them.

5. **Frameworks Are in Favor, Big Time.** A few years ago, many cybersecurity professionals derided cybersecurity frameworks and standards as incomplete and perpetually lagging real-world requirements. But that has changed. We found that 97% of organizations use at least one framework or standard to assess the effectiveness and compliance of their cybersecurity program. Which frameworks and standards from organizations such as the Cloud Security Alliance, NIST, the Center for Internet Security, and ISO are preferred? Find out on pages 49 and 50.

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.

Introduction

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 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. We also look at how IT security training and professional certification can help enterprises address the serious shortfall in skilled IT security staff.

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.

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.

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@cyberedgegroup.com.

Research Highlights

Current Security Posture

- **Over the hump.** The percentage of organizations experiencing a successful attack stayed a few notches below the recent peak (page 7).
- **A brighter future.** Expectations of future compromises fell for the fourth straight year (page 10).
- **Mobile devices least safe.** Among IT domains, cybersecurity teams are the least comfortable about the security posture of mobile devices (page 12).
- **Doubts about defenses.** Confidence in IT security capabilities slipped in 11 of 12 functional areas (page 14).

Perceptions and Concerns

- **The not-so-fabulous four.** Respondents are most concerned about malware, phishing, ransomware, and account takeovers – again (page 16).
- **Everyone's exposed on the web.** Every major industry suffers from attacks against web and mobile applications (page 18).
- **Fewer firms paying ransoms.** The number of organizations victimized by ransomware that pay the ransom has fallen 22% over three years (page 20).
- **To err is human.** Low security awareness among employees and lack of skilled security personnel continue to undermine cybersecurity efforts (page 23).
- **Surfaces count.** Cybersecurity teams are paying attention to the concept of attack surfaces but must work hard to protect them (page 25).
- **Cloud complexity.** Organizations are struggling to cope with the challenges of defending hybrid multi-cloud environment (page 27).
- **Certifications boost careers.** Cybersecurity professionals see a lot of value in training and cybersecurity certifications (page 29).

Current and Future Investments

- **Fair share.** The percentage of IT budgets allocated to information security has held steady over the last five years (page 31).
- **Budgets growing.** Respondents expect their organization's cybersecurity budget to increase a healthy 4.3% this year (page 33).
- **Identity security is a thing now.** Organizations outline their priorities for improving identity security this year (page 35).
- **AI inside.** Four out of five security teams have a moderate or strong preference for security products that feature AI technologies (page 37).
- **MSSPs still popular.** Most organizations outsource some security functions to MSSPs, but they are being a little more selective (page 39).
- **The perimeter hasn't disappeared.** Organizations continue to invest in security products to control access to their networks (page 41).
- **Signature defenses.** Installations of signature-based anti-malware technology increased last year (page 43).
- **App and data security standouts.** Database and web application firewalls are must-haves, API protection is big, and bot management is on the radar (page 45).
- **Security management must-haves.** Active Directory protection, patch management, and security configuration management continue their reign as security management and operations essentials (page 47).

Practices and Strategies

- **Embracing frameworks and standards.** 97% of organizations use at least one framework or standard to assess the effectiveness and compliance of their cybersecurity program (page 49).
- **In zero trust we trust.** 86% of organizations believe that implementing zero trust network access (ZTNA) has improved their ability to defend against sophisticated threats (page 51).
- **What boards need to know.** Assessments of cybersecurity program maturity or effectiveness lead the list of information cybersecurity groups are presenting to their organization's board of directors (page 53).
- **New stars rising.** We updated our list of emerging IT security technologies and architectures being embraced by cybersecurity teams (page 55).

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?

The bleeding has stopped. We've stabilized at partly cloudy. Although we can't yet see the light at the end of the tunnel, at least it's not getting any darker.

We haven't found exactly the right metaphor (obviously), but if you look at Figure 1 you will get the idea.

Of the 1,200 organizations responding to our survey each year, the percentage compromised at least once by a successful cyberattack in the previous 12 months climbed fairly steadily from 75.6% in the 2016 CDR to 86.2% in 2021, plateaued for the next two surveys, then dropped to a lower plateau of 81.5% in 2024 and 81.6% this year.

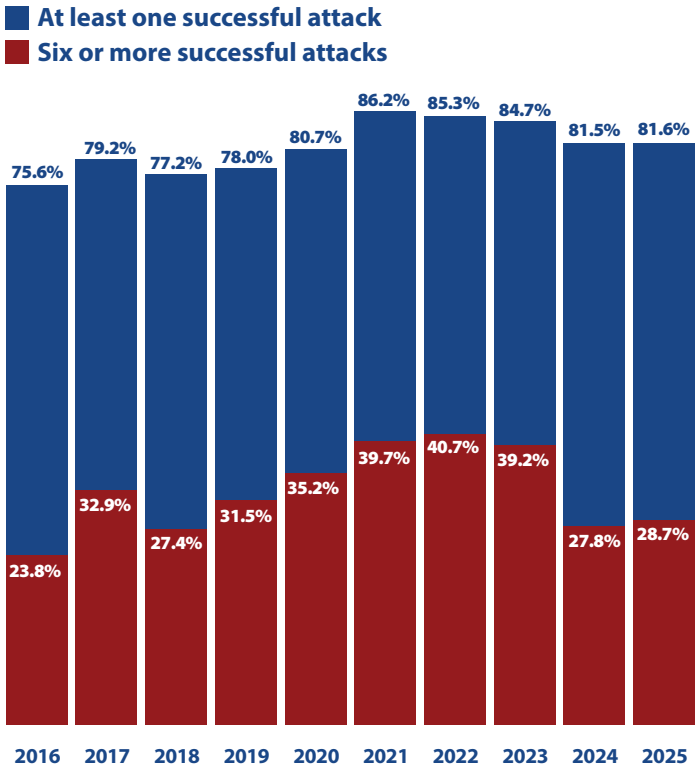

Figure 1: Percentage of organizations experiencing at least one successful attack and those experiencing six or more.

The pattern for the percentage of organizations experiencing six or more successful attacks (the red bars in Figure 1) was roughly the same. It climbed from 2016 to 2021, flattening out for two years, then dropping to a significantly lower plateau for the past two reports.

Figure 2 shows a breakdown of the frequency of successful attacks for this year: just over half of organizations (53.0%) experienced between one and five, 20.8% suffered between six and 10, an unfortunate 7.9% were afflicted by more than 10, and a lucky 18.4% reported none.

However, we can't say the patient is in perfect health, the sun is shining brightly, or we have emerged from the tunnel. The number of organizations being hit by cyberattacks is still at a high level, and with new threats emerging continuously, including those using AI, this is no time for cybersecurity professionals to let down our guard. But at least we can say that we have held the line, stanched the flood, turned the corner…okay, okay, no more metaphors.

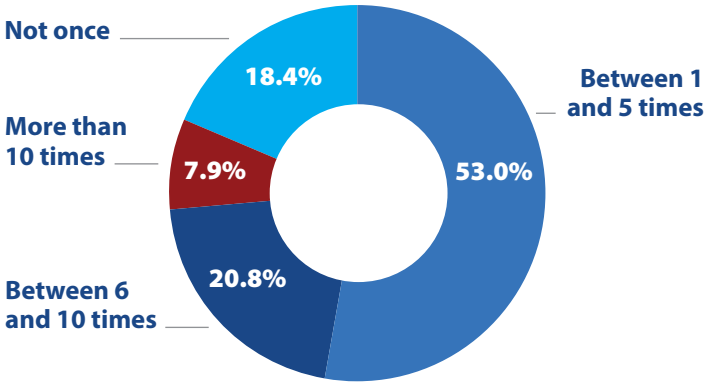

Figure 2: Frequency of successful cyberattacks in the past 12 months.

Section 1: Current Security Posture

What factors and trends account for the pattern shown in Figure 1? Negative factors from 2016 to 2021 included:

- Increasingly sophisticated attacks from cybercriminals and state-sponsored hackers
- Additional incentives for cybercrime driven by the development of new ways to monetize data breaches
- The growth of marketplaces and ecosystems on the dark web that allow threat actors to specialize, share techniques and tools, sell and rent infrastructure to each other, and create ever-larger virtual organizations

All these were capped by the COVID pandemic, which increased attack surfaces by pushing work out to poorly protected remote locations and homes.

Trends helping cybersecurity teams regain control after 2021 include:

- Remote workers returning to offices
- Benefits from the large investments in network and cloud security tools made in response to the challenges of COVID, as well as investments in the advanced technologies discussed on page 55
- The widening application of best practices encouraged by zero trust principles and mandated by frameworks from standards bodies and government agencies
- More attention to cybersecurity basics, including security hygiene, identity management, security awareness training for users, and training for cybersecurity professionals
- AI capabilities embedded in security products and services

There are some interesting variations by country and by organization size in the data on successful attacks.

For example, job stress is probably highest in the four countries where at least nine of 10 organizations experienced a successful attack in the past year: Colombia (96.9%), Turkey (93.9%), South Africa (93.7%), and Mexico (90.6%). Stress levels are probably a little lower in the five countries where the successful attack rate is under 80%: Australia (78.7%), Germany (77.5%), the United States (74.8%), Italy (72.0%), and Canada (71.7%) (see Figure 3).

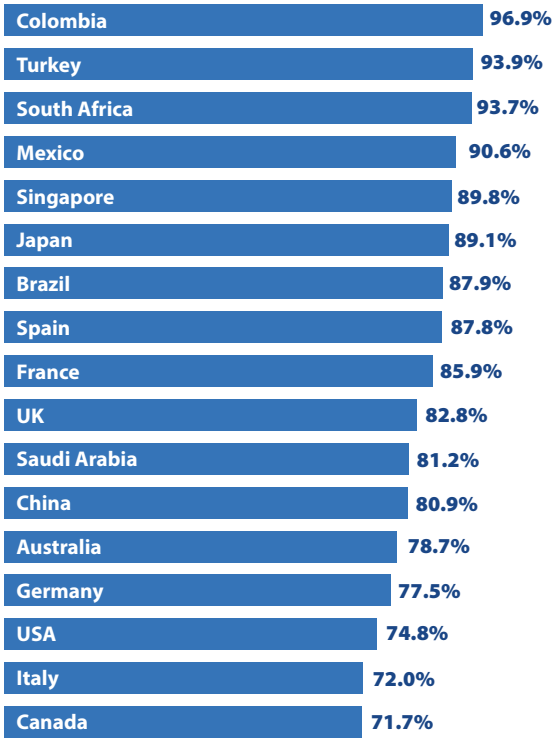

Figure 3: Percentage of organizations compromised by at least one successful attack in the past 12 months, by country.

Section 1: Current Security Posture

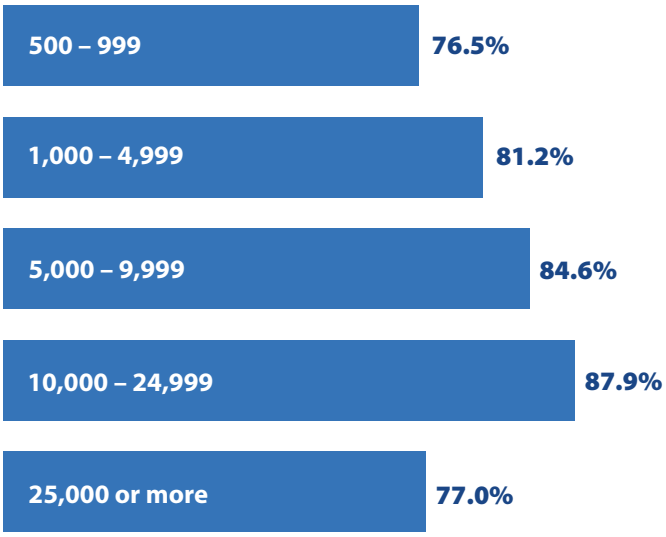

Figure 4: Percentage of organizations compromised by at least one successful attack in the past 12 months, by number of employees.

Looking at size (Figure 4), there is a steady increase in successful attack percentages in organizations from the smallest represented in our survey (500-999 employees) to the second-largest category (10,000-24,999 employees). However, the rate then drops significantly when we get to the largest organizations, with at least 25,000 employees. This pattern probably reflects the fact that, although as firms get larger and offer more-lucrative targets to attackers, the very largest global organizations have the most cybersecurity specialists and invest in the most state-of-the-art defenses.

What does the future hold? We are cautiously optimistic that the slow improvements since 2021 can be maintained, provided cybersecurity teams, vendors, and standards bodies keep up their current levels of effort.

"We can't say the patient is in perfect health, the sun is shining brightly, or we have emerged from the tunnel...but at least we can say that we have held the line, stanched the flood, turned the corner…okay, okay, no more metaphors."

Future Likelihood of Successful Cyberattacks

What is the likelihood that your organization's network will become compromised by a successful cyberattack in 2025?

In the previous section we asked our respondents to report on successful cyberattacks in the past year. In this section, we ask about the likelihood of one or more successful attacks occurring in the current year.

The pattern is roughly the same: rising, leveling out, then falling back a bit. Specifically, the percentage predicting a successful attack in the coming 12 months increased from 62.1% in 2016 to 76.1% in the 2022 CDR and has since fallen in steps to 64.0% (see Figure 5).

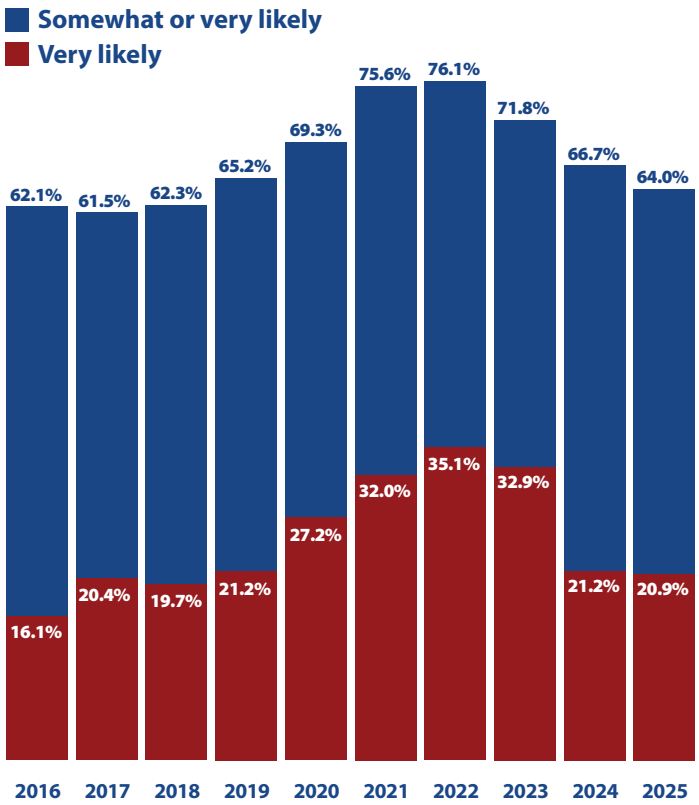

Figure 5: Percentage of organizations indicating that compromise by a successful cyberattack in 2025 is somewhat or very likely.

In fact, the percentage saying that a successful attack is "very likely" in the coming year has fallen to the lowest level since 2018 (see the red bars in Figure 5).

Clearly, the reduction in the rate of successful attacks in past years is leading our respondents to expect further reductions in the coming year. In fact, we might say that their optimism is growing even faster than their experience. Between the 2023 CDR and the current 2025 report, the percentage of organizations experiencing at least one successful cyberattack in the past year fell 3.1% (from 84.7% to 81.6%), while those saying that it's somewhat or very likely that they would be attacked successfully in the coming year fell 7.8% (from 71.8% to 64.0%).

You may also have noticed that our respondents are optimistic in another way. If 81.6% of organizations experienced at least one compromise last year (Figure 1), as a group they might be a tad overconfident in predicting that only 64.0% will be compromised this year (Figure 5). But that's okay; we wouldn't want to rain on their parade. (Oops, another metaphor. Sorry.)

"The percentage [of organizations] saying that a successful attack is "very likely" in the coming year has fallen to the lowest level since 2018."

Section 1: Current Security Posture

One interesting detail from the comparison by country (Figure 6) is that the six countries with the highest predictions for successful attacks include the four Asia-Pacific nations in our survey: Japan (85.5%), China (82.0%), Singapore (77.1%), and Australia (70.0%).

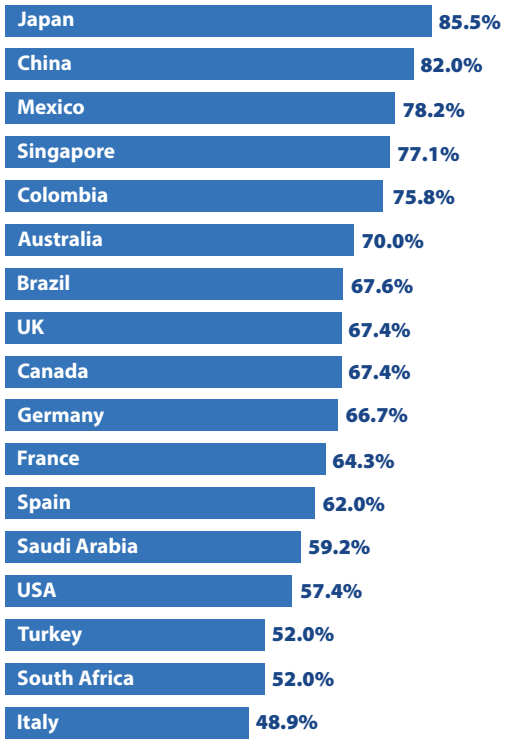

Figure 6: Percentage of organizations indicating that compromise by a successful cyberattack in 2025 is somewhat or very likely, by country.

When looking at the results by industry (Figure 7), it is interesting to note that finance and healthcare see the lowest likelihood of successful attacks (62.1% and 56.0%, respectively). We think that reflects the fact that those two sectors have made some of the largest investments in cybersecurity over the last few years.

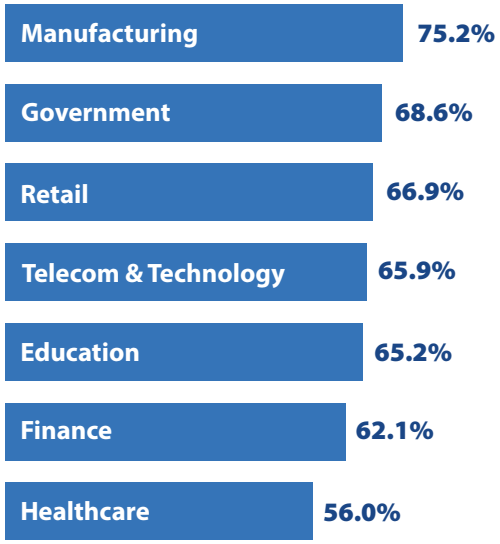

Figure 7: Percentage of organizations indicating that compromise by a successful cyberattack in 2025 is somewhat or very likely, by industry.

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:

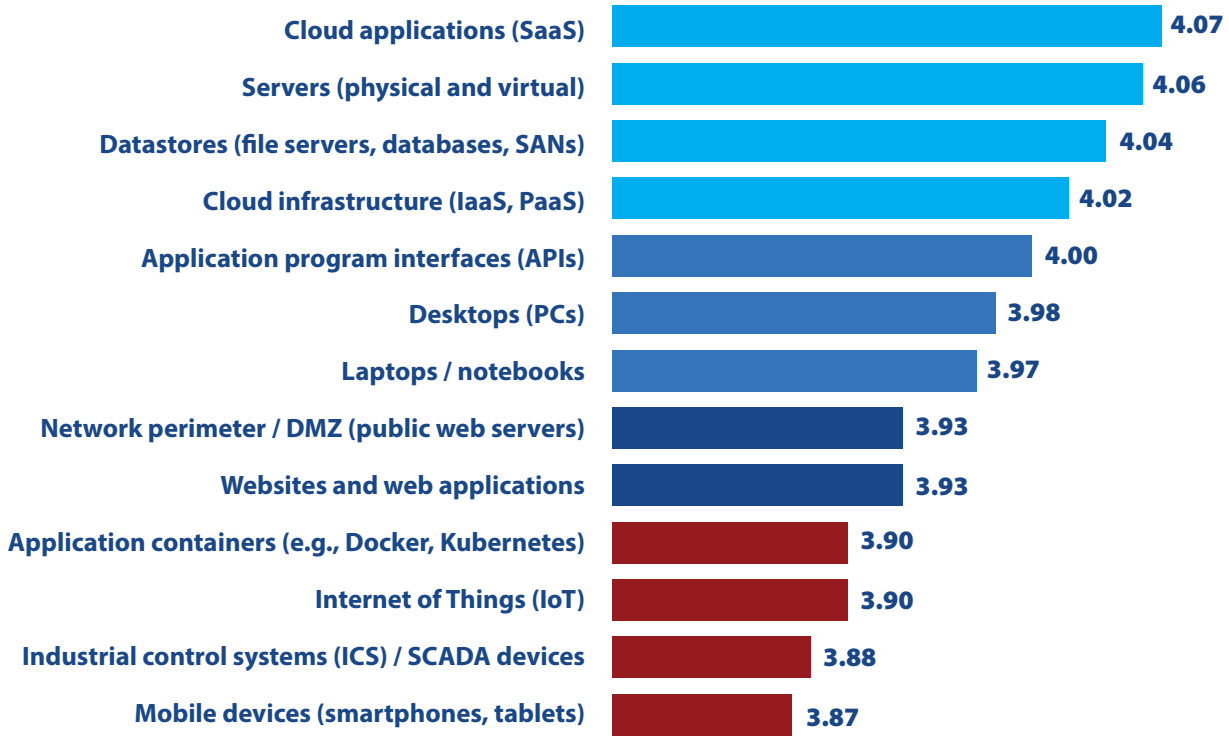

Figure 8: Perceived security posture by IT domain.

Cybersecurity teams need to protect many different types of devices, applications, and infrastructure components. Our survey asked respondents to rate their organization's security posture in 13 of those domains (see Figure 8).

Overall, respondents are fairly confident about their organization's ability to defend itself. Their ratings across the board averaged 3.97 on a scale of one to five, with five being the best possible security posture.

But they are a touch less confident than they were last year or the year before. From the 2023 report to last year's, the security posture rating fell in 10 of the 13 categories. The change this year was similar: declines in 11 of the 13. The average rating across all categories, which we call the "Security Posture Index," did not decrease much: by .05 and then .03 (see Figure 9). However, the trend points to nervousness among security teams that their defenses may not be keeping up with the advances made by threat actors.

Section 1: Current Security Posture

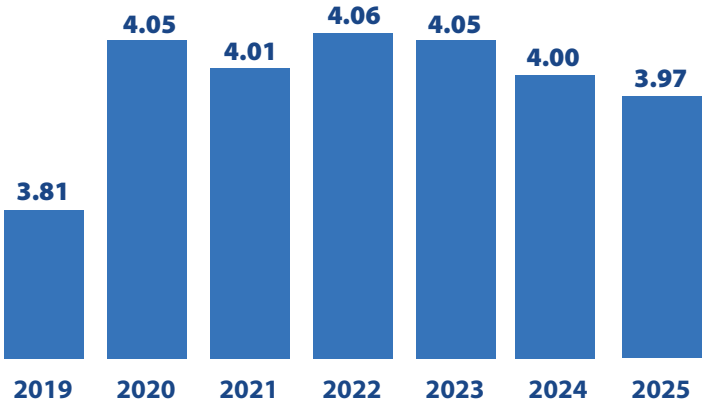

Figure 9: The Security Posture Index.

"Mobile devices such as smartphones and tablets...dropped…to the bottom. That is not because defenses for those devices got worse, but rather that phones have been storing more and more confidential business data and threat actors are developing new attacks against them."

Respondents were most comfortable about the security of "Cloud applications (SaaS)" and nearly as comfortable with "Cloud infrastructure (IaaS, PaaS)." This reflects the fact that cloud service providers have made great strides in improving the security of their environments, in many cases by creating their own native security tools.

Organizations are also relatively confident about their security posture for servers and datastores. Most of these are mature technologies, supported by proven security tools and a body of security best practices.

Speaking of mature technologies, "Desktops (PCs)" was the one domain where the security posture rating improved from the previous report.

One area of great concern continues to be industrial control systems, which has been in the bottom position for several years. Survey respondents also consider internet of things (IoT) security to be a weak spot, which fell two places on the list to tie with application containers for third from worst.

And the IT domain where security teams are least confident? "Mobile devices (smartphones, tablets)," which also dropped two places, from third from worst to the bottom. That's not because defenses for those devices got worse, but rather that:

- Phones have been storing more and more confidential business data.
- Threat actors have been developing new attacks against them.

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:

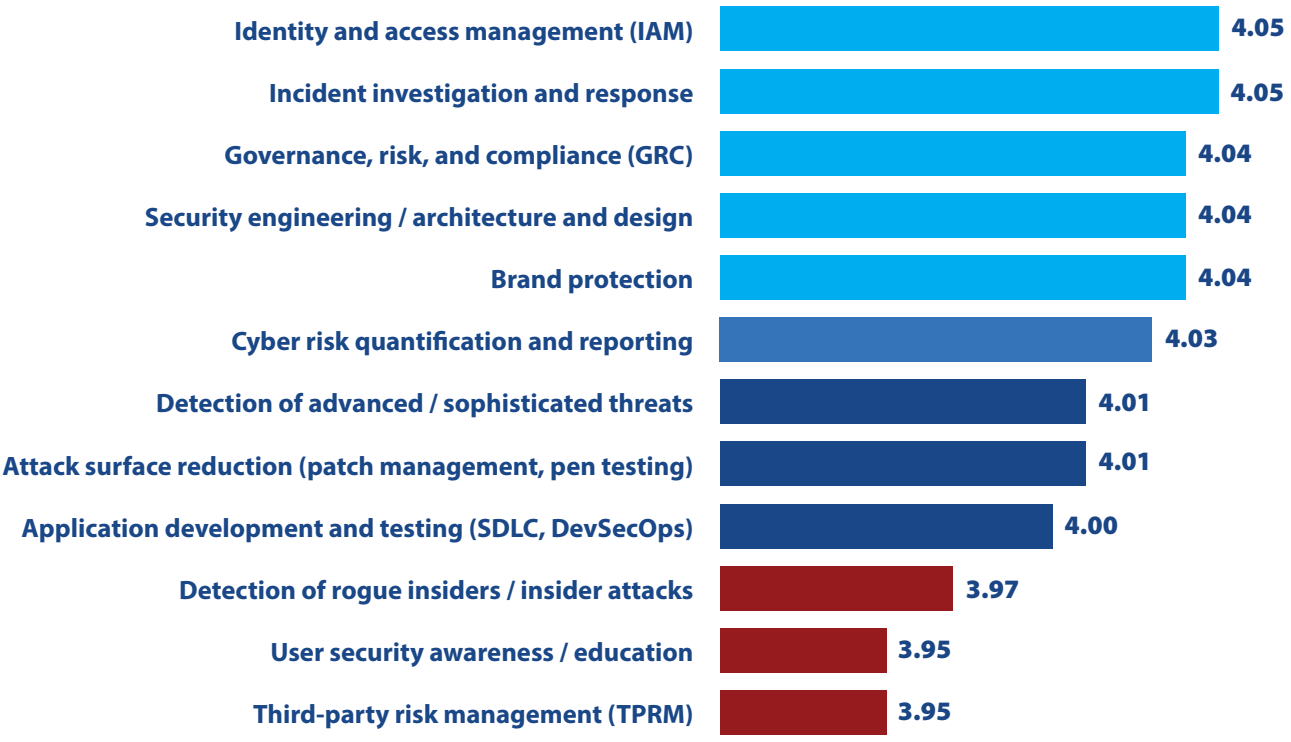

Figure 10: Perceived adequacy of security capabilities by functional area.

Confidence in the adequacy of defenses across functional areas of IT security fell significantly in this survey, for the second year in a row. In both years, ratings declined in 11 of the 12 categories tracked. In fact, this year confidence didn't go up in *any* of the areas. The one that didn't go down, "Brand protection," simply remained unchanged.

As with the previous question about security posture by IT domain, we don't think respondents are complaining that defenses got weaker. Rather, they sense that attack surfaces are getting larger and new attack techniques are developing faster.

The functional areas with the biggest declines in scores were "Cyber risk quantification and reporting (GRC)," "Detection of advanced/sophisticated threats," and "User security awareness/education."

Other major areas of concern are "Detection of rogue insiders/insider attacks" and "Third-party risk management (TPRM)," which were third from the bottom and tied for the bottom spot, respectively (see Figure 10).

Section 1: Current Security Posture

One of relatively bright spot was "Incident investigation and response," which moved from the fifth position from the top last year to the second position this year. "Brand protection" also moved up, from eighth place to fifth.

Organizations feel most comfortable about their capabilities for "Identity and access management (IAM)," "Incident investigation and response," "Cyber risk quantification and reporting (GRC)," "Security engineering, architecture, and design," and "Brand protection," all of which had average ratings of 4.04 or 4.05 on a five-point scale.

"Confidence in the adequacy of defenses across functional areas of IT security fell significantly in this survey, for the second year in a row. In both years, ratings declined in 11 of the 12 categories tracked…We don't think respondents are complaining that defenses got weaker. Rather, they sense that attack surfaces are getting larger and new attack techniques are developing faster."

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.

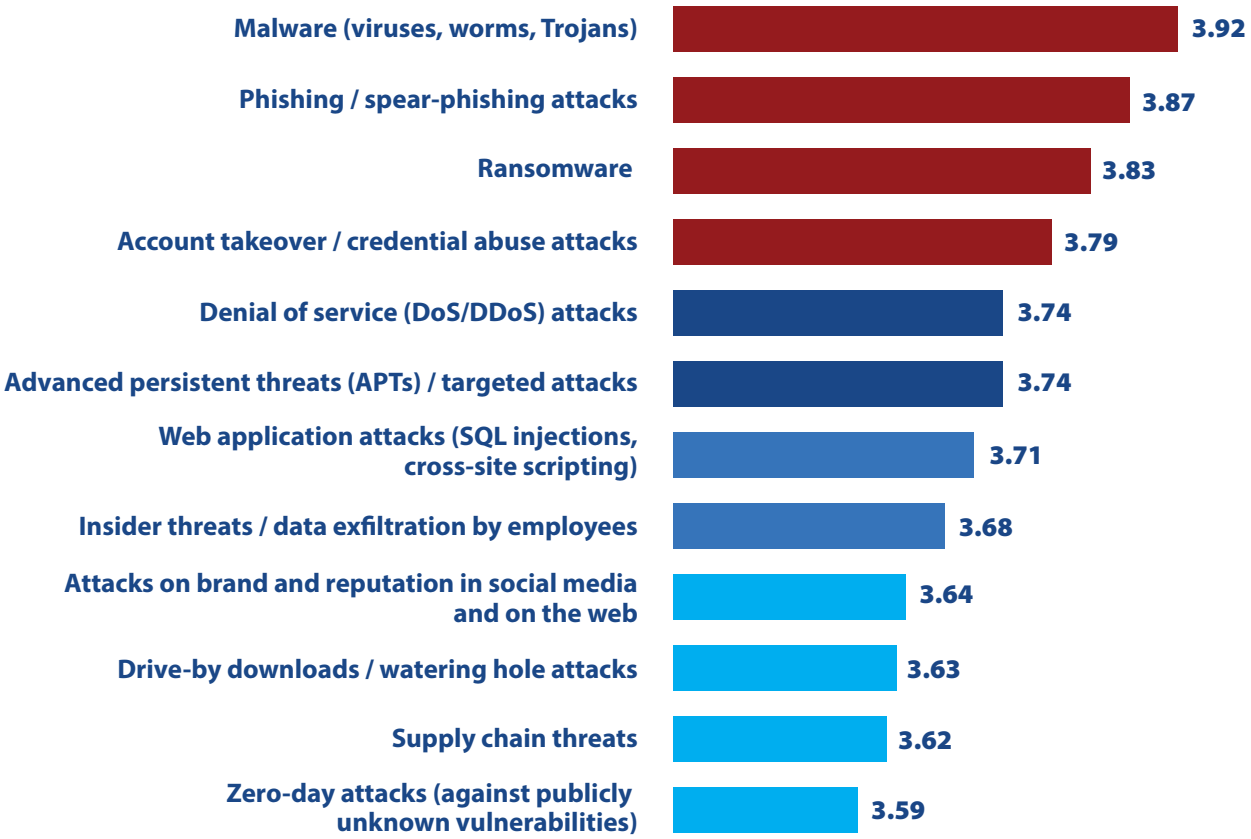

Figure 11: Relative concern for cyberthreats.

The threats doing the most to cause sleepless nights are not going to surprise you. Our leading nightmares are malware (with a score of 3.92 on a scale of 1 to 5), phishing (3.87), ransomware (3.83), "Account takeover and credential abuse attacks" (3.79), "Denial of service (DoS/DDoS) attacks" (3.74), and "Advanced persistent threats (APTs)/targeted attacks" (also 3.74). These are the same top six as last year, in exactly the same order, except for ransomware and ATO switching places in the third and fourth positions. These are the cyberthreats most directly connected with data breaches and extortion, i.e., the threats that produce the biggest monetary returns for adversaries.

The bottom (relatively least concerning) end of the list also changed very little over the past few years. The leaders there are "Attacks on brand and reputation in social media and on the web" (3.64), "Drive-by downloads/watering-hole attacks" (3.63), "Supply chain threats" (3.62), and "Zero-day attacks (against publicly unknown vulnerabilities" (3.59).

Section 2: Perceptions and Concerns

We are a little surprised to see respondents so sanguine about supply chain threats, since there were some very visible supply chain attacks in 2024, including a number associated with security and network security tools. Perhaps cybersecurity teams feel that enough controls are in place to blunt these attacks. Or perhaps there is a bit of a "that's not my problem" attitude, since the primary responsibility to prevent supply chain security issues may fall on the teams buying and managing infrastructure and on third-party risk management groups, rather than cybersecurity groups.

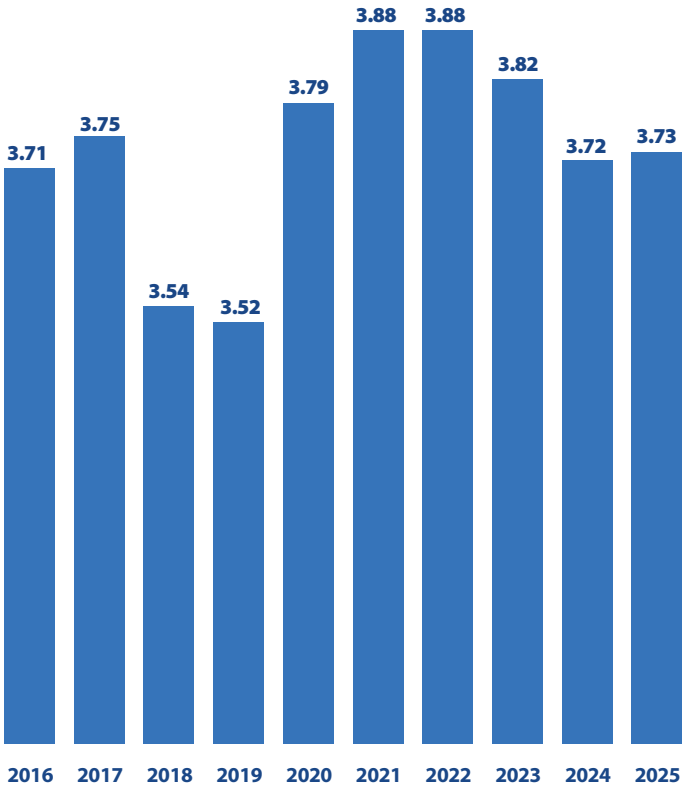

Figure 12: Threat Concern Index, depicting overall concern for cyberthreats.

What is the big picture? You can see it in Figure 12, which shows CyberEdge's Threat Concern Index. This is an average of the scores for the 12 cyberthreat types included in this section. The overall concern for cyberthreats fell significantly between the 2022 and 2024 surveys, but plateaued this year. We think the earlier improvement reflects the return of workers to offices, increased investment by organizations in AI and other advanced security technologies, and the widespread implementation of zero trust frameworks. However, it may be that organizations are seeing diminishing returns from investments in those areas and are perhaps becoming more worried about the dangers of threat actors doing more to capitalize on AI and deepfakes.

"We are a little surprised to see respondents so sanguine about supply chain threats...Perhaps cybersecurity teams feel that enough controls are in place to blunt these attacks. Or perhaps there is a bit of a 'that's not my problem' attitude."

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.)

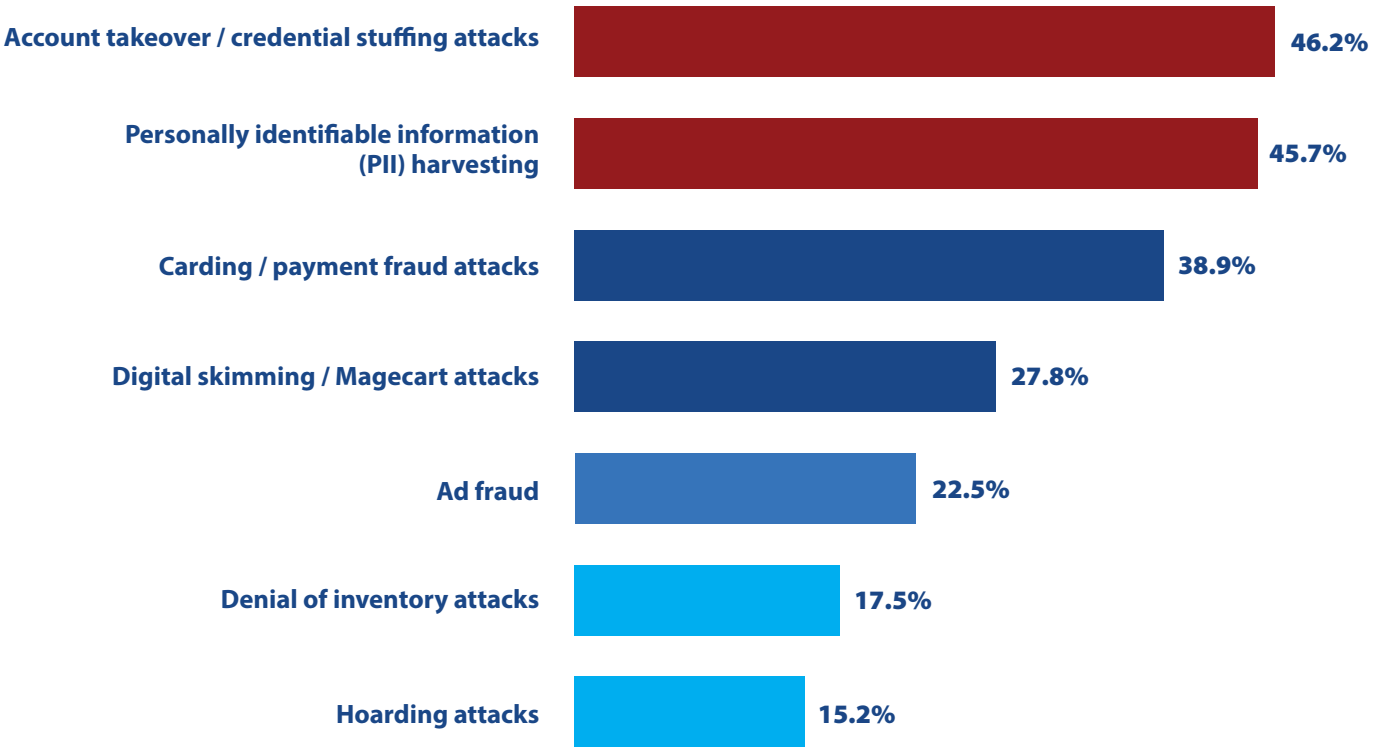

Figure 13: Most-concerning web and mobile application attacks.

Today, who *doesn't* conduct business on the web? What forward-looking enterprise that deals with customers, clients, or constituents *doesn't* offer a mobile app to make it easy? The answer to both questions: only a vanishingly few organizations don't perform transactions or share confidential information either on websites or through apps. And everyone knows that websites and phones can be crime scenes and staging grounds for fraud.

Web and mobile application attacks menace every enterprise that transacts business on the web and through mobile apps. Financial institutions and retailers can lose substantial sums to online fraud. But these attacks can affect every 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.

That's why our survey asks respondents to select the three web and mobile application attacks that most concern them (see Figure 13).

Section 2: Perceptions and Concerns

The most serious threats in this category, each highlighted by almost half of the respondents, were "Account takeover (ATO) and credential stuffing" attacks (46.2%) and "Personally identifiable information (PII) harvesting" (45.7%). They use stolen or leaked passwords and email addresses to impersonate customers and other legitimate users to drain money or valuable data out of web and mobile applications.

The other two leading banes of internet transactions are (a) "Carding/payment fraud attacks" (38.9%) and (b) "Digital skimming/Magecart attacks" (27.8%). These attacks use a variety of technical and social engineering techniques to capture and leverage numbers, names, and security codes from credit cards and other payment vehicles.

Cybersecurity and fraud prevention teams are working hard to foil web and mobile application attacks. They are widening the use of biometrics and multi-factor authentication (MFA) to more and more customer- and client-facing applications, and using behavioral analysis (now powered by AI) to detect impersonation and fraud. They are also educating consumers and customers on how to create (and never reuse) strong passwords, avoid falling for social engineering techniques, and take sensible precautions when using payment cards.

Sadly, these efforts are barely holding the line, if that. Concerns about all our "top four" web and mobile attacks increased over the past year.

Let's go back to the questions at the beginning of this section about who *isn't* affected by web and mobile application attacks. The answer is: 9.1% of organizations. The other 90.9% are affected by one or more (see Figure 14).

When we break down the data by industry, some might be surprised to find that technology and manufacturing companies are affected even more than finance and retail firms (see Figure 15). But that just testifies to the fact that today, the vast majority of organizations in almost every industry transact business and share sensitive information through websites and phones.

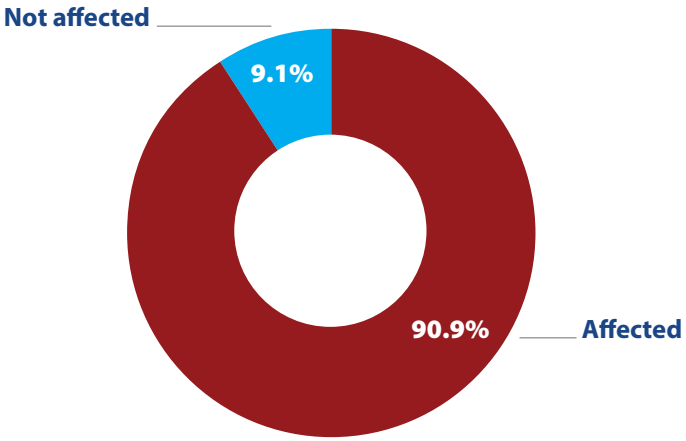

Figure 14: Organizations affected by a web or mobile application attack.

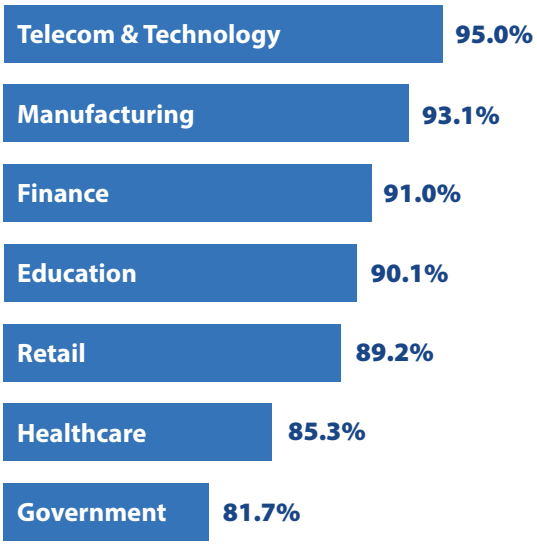

Figure 15: Organizations affected by a web or mobile application attack, by industry.

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?

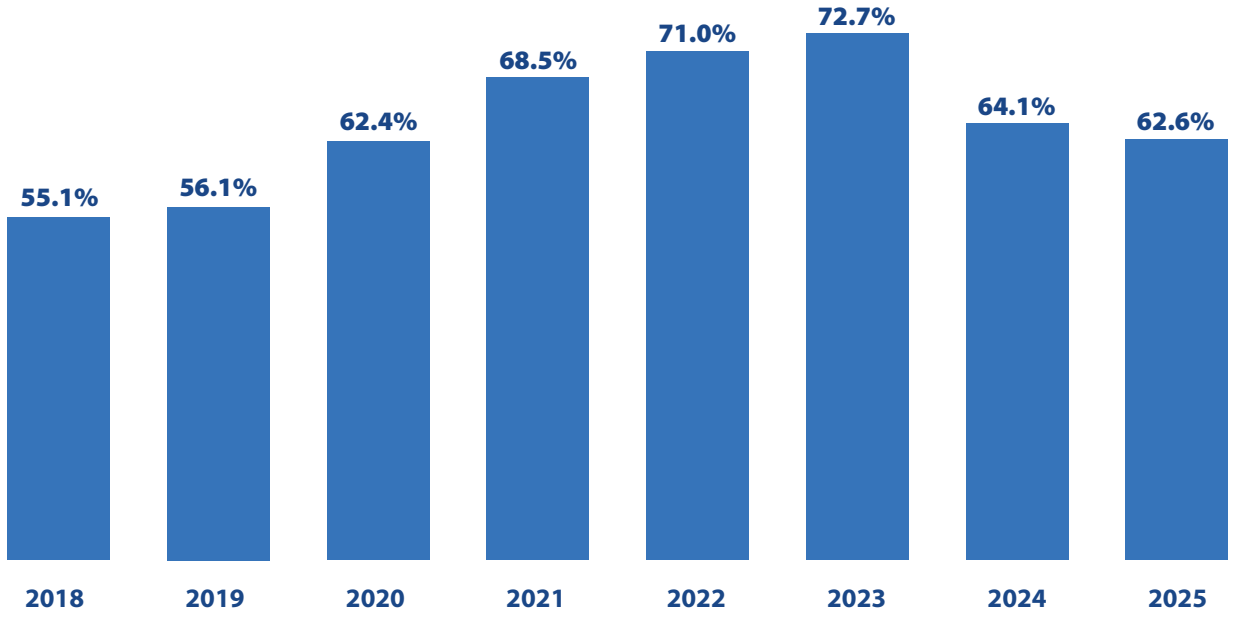

Figure 16: Percentage of organizations victimized by ransomware.

The percentage of organizations affected by ransomware fell for the second year in a row, reversing the trend of the previous decade. The decline of 10.1% over two years is quite significant (see Figure 16).

The factors behind this substantial decrease include:

- Aggressive actions by government and law enforcement agencies to pursue ransomware gangs around the globe and to take down the infrastructure they use (or rent to other criminals)
- Better defenses against some of the tools and techniques used to distribute and activate ransomware
- Fewer victimized organizations paying ransoms (discussed below), which reduces the financial returns and incentives for ransomware gangs

Government and law enforcement efforts are now truly global. Major actions against participants in ransomware activities in 2024 took place across Africa, Asia, Europe, North America, and South America (so far, ransomware has not been a major problem in Antarctica).

International coordination and cooperation have advanced significantly, as illustrated by the activities of the 68 nations participating in the International Counter Ransomware Initiative (CRI), now in its fifth year. That organization has declared a "joint

Section 2: Perceptions and Concerns

commitment to develop collective resilience to ransomware, support members if they are faced with a ransomware attack, pursue the actors responsible for ransomware attacks and not allow safe haven for these actors...and forge international partnerships so we are collectively better equipped to counter the scourge of ransomware." (Source of quotation: International Counter Ransomware Initiative 2024 Joint Statement.)

However, the reduction in the number of organizations victimized by ransomware has been partially offset by a trend toward targeting larger enterprises that can afford larger ransom payments. According to ransomware experts at Coveware, the average (mean) ransom payment has been trending upward for several years (see Figure 17).

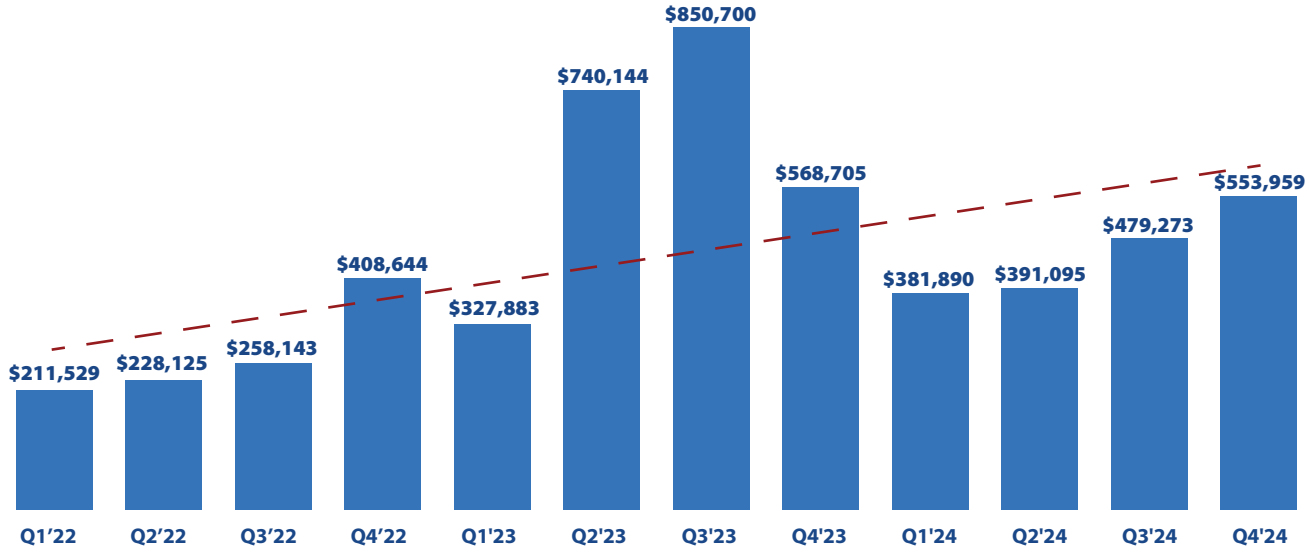

Figure 17: Average ransom payments by quarter (data source: Coveware Quarterly Ransomware Reports).

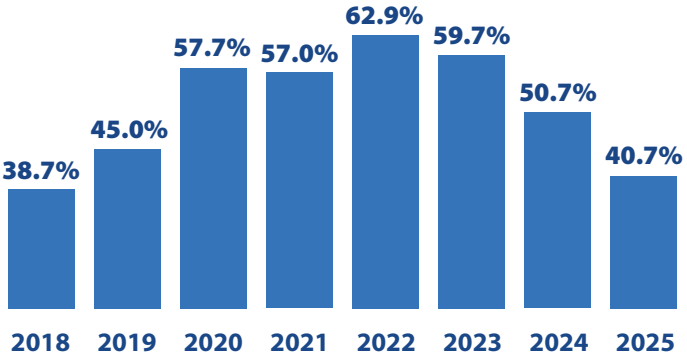

Figure 18: Percentage of victimized organizations paying ransoms.

Another very striking finding from our data is that the percentage of organizations that were affected by ransomware and actually paid a ransom fell a full 10% over the last year, from 50.7% to 40.7%. It is now an astonishing 22.2% below the peak of 62.9% in our 2022 CDR (see Figure 18).

Section 2: Perceptions and Concerns

The reasons for this trend include:

- More reliable and attack-resistant backup and recovery methods
- Increasing doubts about the inclination and even the ability of ransomware gangs to provide effective decryption tools, and to honor their promises not to reveal exfiltrated data (in other words, doubts that paying a ransom will produce any results)
- The refusal of some cyber insurance companies to cover ransom payments (although the policies may still cover costs related to losses from ransomware attacks)
- A growing number of laws prohibiting ransom payments to some classes of cybercriminals and groups associated with terrorist organizations, and governments strongly discouraging ransom payments to anyone

Regarding this last bullet, the attitude of many governments and law enforcement agencies is moving steadily toward the famous declaration: "Millions for defense, but not one cent for tribute" (referring to resisting both demands for ransoms by Barbary pirates and requests for bribes by government officials).

The data in Figure 19 supports the idea mentioned above: that paying a ransom may not produce any results, either in terms of getting back encrypted data or dissuading criminals from disclosing stolen information. Only slightly more than half (54.3%) of the organizations that pay ransoms are successfully recovering their data. That's down from 72.7% two years ago.

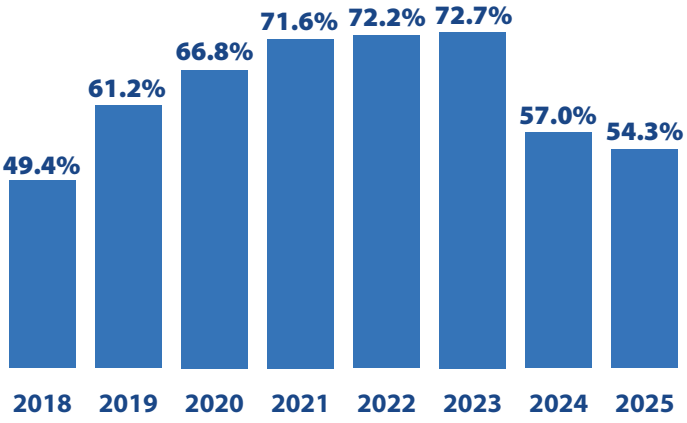

Figure 19: Percentage of ransom payers that recovered data.

"The attitude of many governments and law enforcement agencies is moving steadily toward the famous declaration: 'Millions for defense, but not one cent for tribute.'"

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.

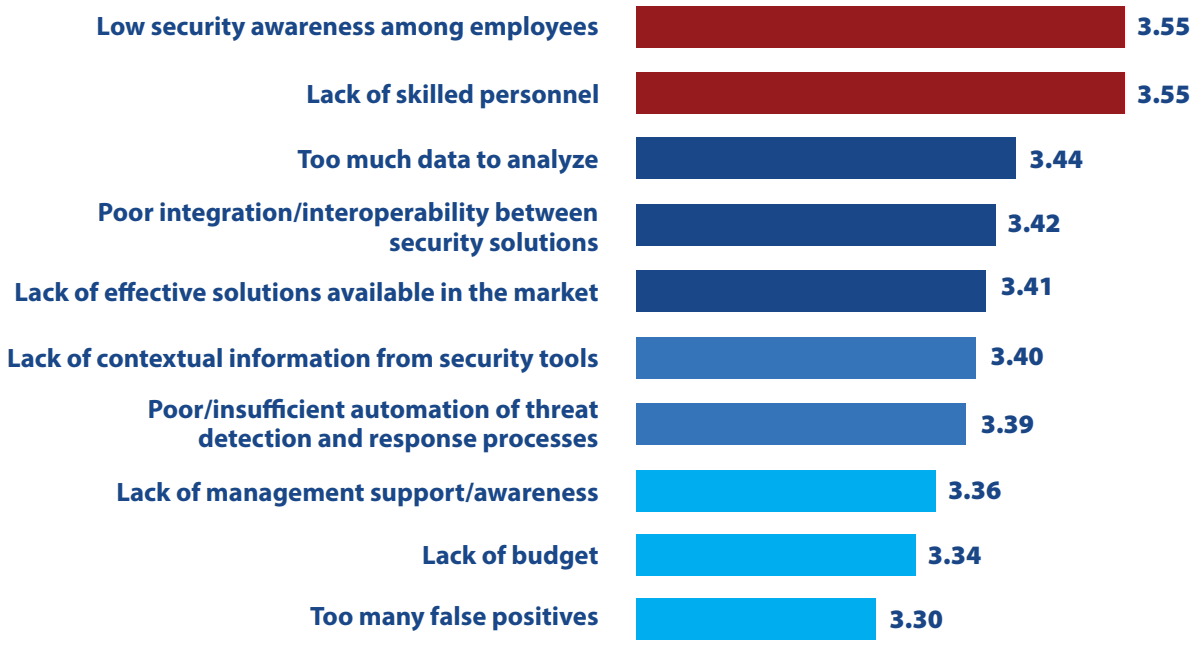

Figure 20: Inhibitors to establishing effective defenses against cyberthreats.

Why haven't we (the cybersecurity community) been able to crush cybercrime and frustrate hostile nation-state actors? With all our experience and technology, why are we having to work so hard just to stay in the same place relative to our adversaries? What's holding us back?

We ask every year, and this is what we learned from the latest feedback.

Two inhibiting factors have traded places at the top of the list for many years now, and in this survey they ended in a tie for first. "Low security awareness among employees" and "Lack of skilled personnel" both came in at 3.55 on our scale of 1 to 5, with 5 being the biggest barrier to success (see Figure 20).

This result reinforces the idea that in cybersecurity, as in so many other areas of business and life, people challenges trump technology issues every time. Without doubt, although computers speed up every year, people don't (and some days we suspect they are getting slower). But the data serves as a reminder that we should be investing more in educating end users and training our cybersecurity teams.

Section 2: Perceptions and Concerns

With significantly lower scores, but still high on our list of barriers to success, are "Too much data to analyze" (3.44), "Poor integration/interoperability between security solutions" (3.42), and "Lack of effective solutions available in the market" (3.41).

Looking toward the bottom of the list, it is somewhat reassuring to see that "Lack of management support/awareness" and "Lack of budget" are viewed as lesser issues. It implies that at least we have the backing of our bosses.

It is interesting that "Too many false positives" is now rated as the least serious inhibitor. This indicates progress in our ability to scan security data and filter out false positives. Undoubtedly, AI has played a role in this improvement.

Our Security Concern Index averages the ratings of all the inhibitors to provide a reading on the overall feeling of cybersecurity professionals toward factors that get in the way of success. As Figure 21 shows, there has been little change from last year. This finding aligns with some of the other data showing that right now, cybersecurity teams are pretty much keeping up with their challenges, neither pulling farther ahead or falling farther behind.

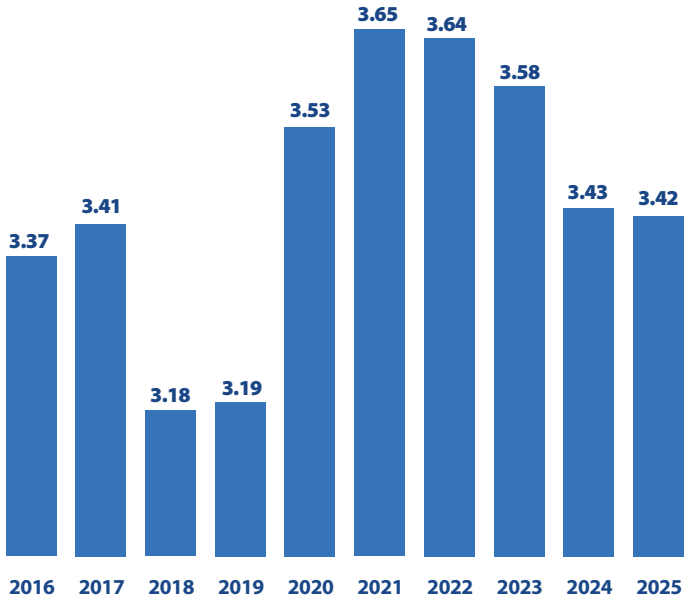

Figure 21: The Security Concern Index, representing the average rating of security inhibitors.

"Although computers speed up every year, people don't (and some days we suspect they are getting slower). But the data serves as a reminder that we should be investing more in educating end users and training our cybersecurity teams."

Section 2: Perceptions and Concerns

Attack Surface Management Challenges

What are the biggest challenges pertaining to attack surface management (ASM) within your organization? (Select up to five.)

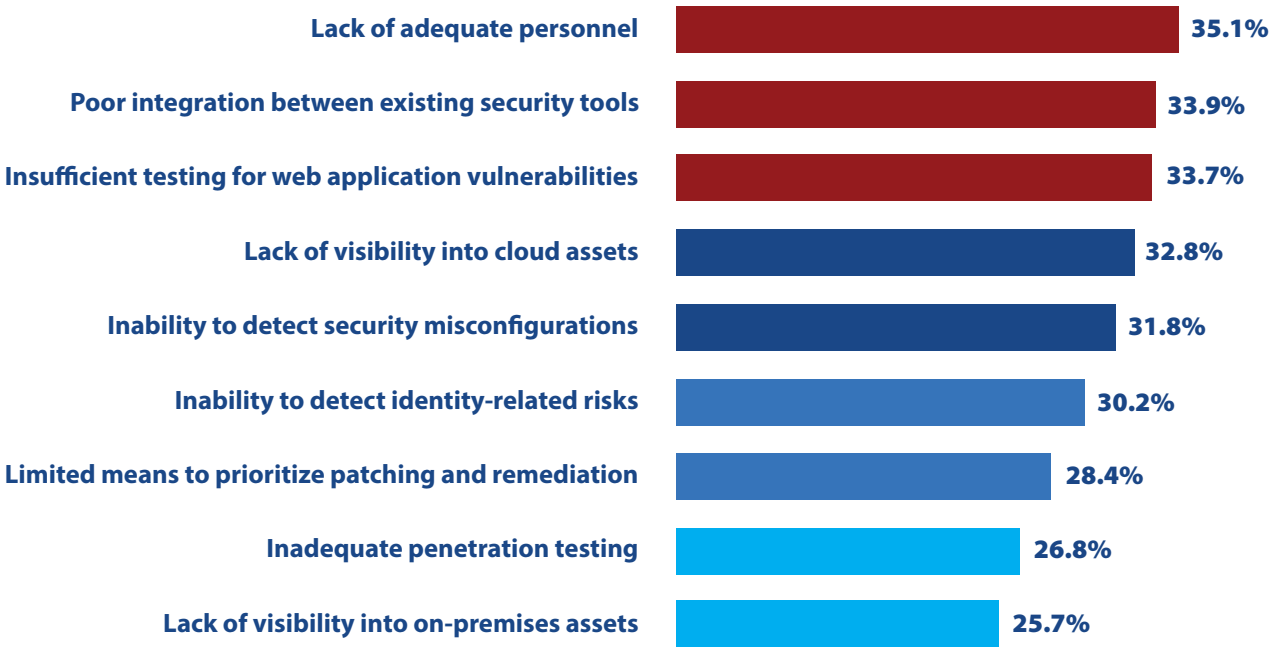

Figure 22: Biggest challenges pertaining to attack surface management.

The concept of an attack surface, the combination of all areas where adversaries can try to enter or cause an effect on a computing environment, has been around for some time. But we noticed recently that cybersecurity practitioners and vendors have been paying more attention to the idea that attack surfaces should be systematically studied and hardened. This has given rise to the discipline of "attack surface management" (ASM), which includes elements of vulnerability scanning, penetration testing, security hygiene, and risk management.

This topic is particularly important because:

- Attack surfaces are getting much larger, for example, because sensitive data that used to be stored in a few databases and file servers in corporate headquarters is now scattered across multiple SaaS applications, cloud platforms, hosted services, home offices, and remote devices.
- Some cybersecurity experts now suggest that organizations should think in terms of having multiple attack surfaces with different characteristics, versus one extremely large one.

Section 2: Perceptions and Concerns

Examples of attack surfaces that can be said to exist within the same organization are a software attack surface, a cloud attack surface, a network attack surface, a physical (or device) attack surface, a social media attack surface, an identity attack surface, and a human attack surface.

Given the importance of the topic, we added a question to this year's survey about the five biggest challenges each organization faces pertaining to attack surface management.

The challenge mentioned most often: "Lack of adequate personnel," cited by 35.1% of respondents. No surprise there: the cybersecurity skills shortage is a running theme throughout this survey.

Just behind lack of adequate personnel is "Poor integration between existing security tools" (33.9%). Because attack surfaces are so broad and have so many facets, organizations are forced to use multiple tools to track different areas. That makes it hard to see patterns and to determine priorities for remediation across functional silos. The idea of attack surface management platforms that integrate and combine tools is starting to emerge to help security teams address this challenge.

Third on the list is "Insufficient testing for web application vulnerabilities" (33.7%). Because web applications are now being distributed across multiple cloud and data center systems, detecting security issues can be especially tricky. If you want to drill down in this area, just turn to the next page and see what our respondents have to say about challenges caused by having hybrid multi-cloud environments.

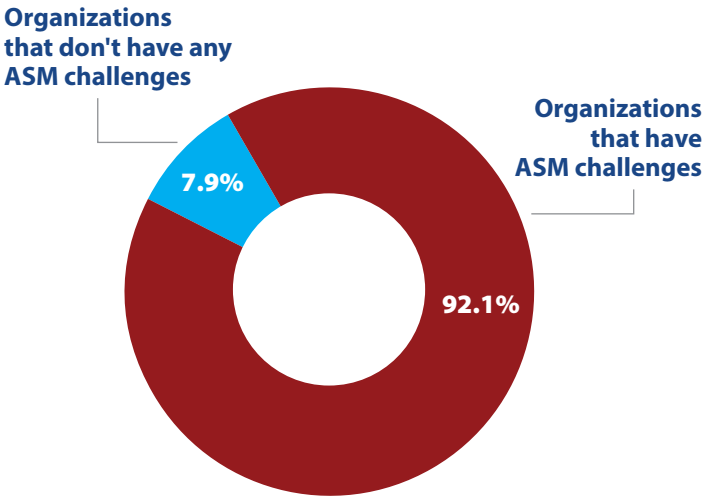

Figure 23: Organizations that have challenges related to attack surface management.

The next three challenges are "Lack of visibility into cloud assets" (32.8%), "Inability to detect security misconfigurations" (31.8%), and "Inability to detect identity-related risks" (30.2%).

Clearly this is an area with a very diverse set of security requirements, not all of which can be addressed at once. It will be interesting to see how the discipline of attack surface management evolves.

In the meantime, to validate that the need is real, we found that only 7.9% of respondents say their organization doesn't have any attack surface management challenges (see Figure 23).

"The challenge mentioned most often: 'Lack of adequate personnel,' cited by 35.1% of respondents. No surprise there: the cybersecurity skills shortage is a running theme throughout this survey."

Challenges Caused by Hybrid Multi-cloud Environments

What are the biggest challenges to your organization caused by having a hybrid multi-cloud environment (that is, an environment that includes on-premises systems and two or more cloud platforms)? (Select up to five.)

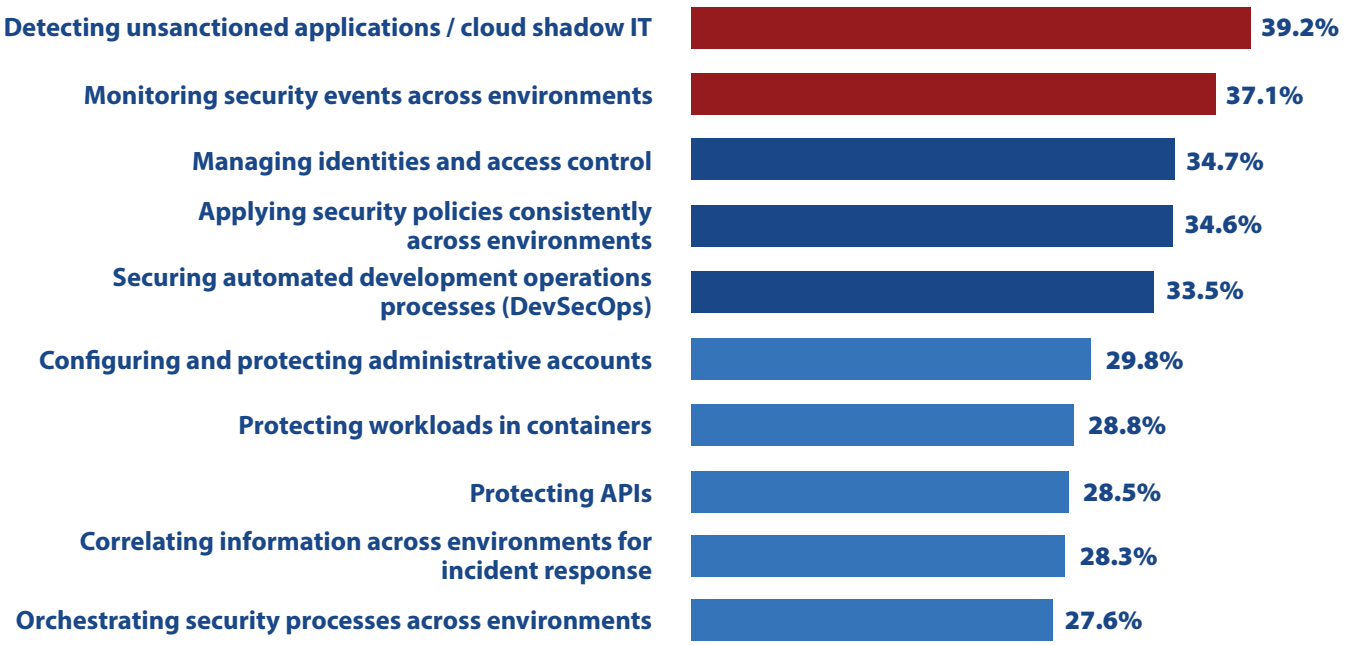

Figure 24: Biggest challenges caused by having a hybrid multi-cloud environment.

As we noted in the previous section and elsewhere in this report, enterprise attack surfaces are expanding and diversifying. One of the main reasons is that applications and data are now, to use a technical term, "all over the place."

Today, most organizations of any size are operating in hybrid multi-cloud environments. That means cybersecurity teams must monitor and protect applications and data residing on systems inside their own data centers, in the hosting facilities of SaaS application vendors, and on multiple cloud platforms hosted by cloud service providers such as Amazon (Amazon Web Services or AWS), Google (Google Cloud Platform or GCP). Microsoft (Microsoft Azure), and IBM (IBM Cloud).

In this year's survey, we decided to ask what aspects of working in a hybrid multi-cloud environment are most problematic for cybersecurity teams.

As it turns out, the issue cited most often is "Detecting unsanctioned applications/cloud shadow IT," selected as one of the top five challenges by 39.2% or the respondents (see Figure 24). It has been easy for individual employees and departments to subscribe to unauthorized online applications and services with below-standard security and to store sensitive data and confidential documents there. Cybersecurity teams are playing catch-up trying to discover and remediate these breaches of policy.

Section 2: Perceptions and Concerns

Not surprisingly, another of the most serious challenges is "Monitoring security events across environments" (37.1%). Most computing environments and platforms have their own management, monitoring, and security tools that don't share information well with each other. As cross-platform tools are introduced and standards for sharing data and processes between environments are developed, these issues will become less important, but that will take time.

The challenge rated third biggest is "Managing identities and access control" (34.7%). Today, a typical individual using multiple platforms may have accounts with different usernames and credentials on each of them. Cybersecurity and identity teams may have no idea they all belong to one person. They may implement special monitoring and controls in some environments for a "privileged user" like an IT systems administrator or a top executive, but fail to take the same precautions in others. When people leave the organization, administrators may not disable all their accounts, leaving some available to be taken over and abused by attackers. Identity management issues are becoming increasingly serious with the proliferation of non-human identities (NHIs) for hardware devices and software workloads.

The fourth challenge on the list is "Applying security policies consistently across environments" (34.6%). Today, cybersecurity managers would like to ensure that zero trust policies such as continuous, adaptive authentication and the principle of least privilege (PoLP) are enforced consistently across environments. Users expect roughly similar processes for creating accounts, authenticating to applications, managing credentials, reporting phishing messages, and so forth. But the more platforms users touch, the harder it is to provide consistency in these areas.

We don't have the space here to review all the challenges listed in Figure 24, but it is worth noting how many domains they cross. Besides the ones discussed above, they include secure application development, security for containerized workloads and services, protection for APIs, and security orchestration, automation, and response (SOAR).

One other observation: today, almost everyone (94.6% of organizations with at least 500 employees, to be precise) has a hybrid multi-cloud environment (see Figure 25). Although you might expect smaller companies to be late adopters in this area, that hasn't been the case. Figure 26 shows that organizations with 500-999 employees are working in multi-cloud environments at almost exactly the same rate as larger entities.

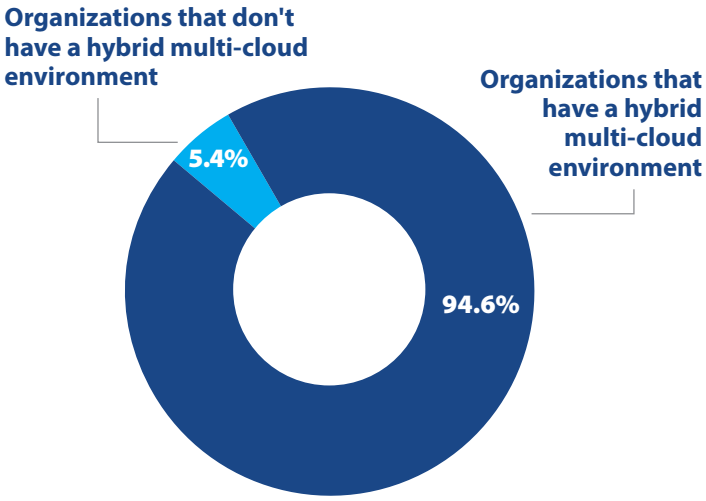

Figure 25: Organizations that have a hybrid multi-cloud environment.

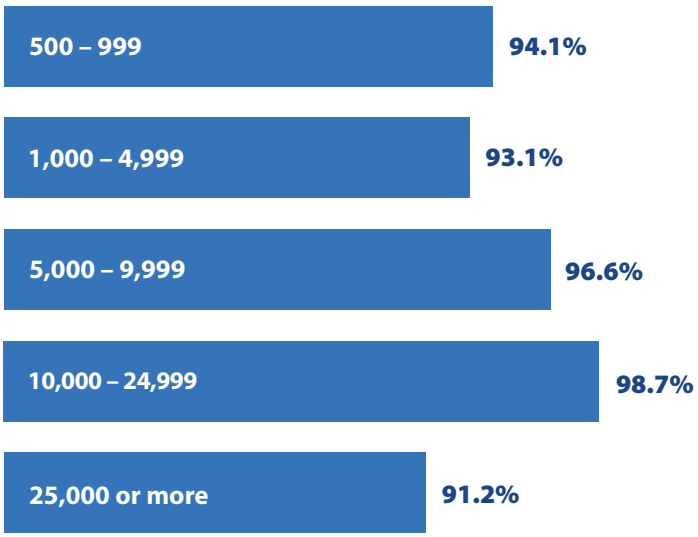

Figure 26: Organizations that have a hybrid multi-cloud environment, by number of employees.

Section 2: Perceptions and Concerns

Boosting Careers with Cybersecurity Certifications

Based on your organization's current climate, which of the following types of cybersecurity certifications do you believe would be most beneficial to your career path? (Select up to three.)

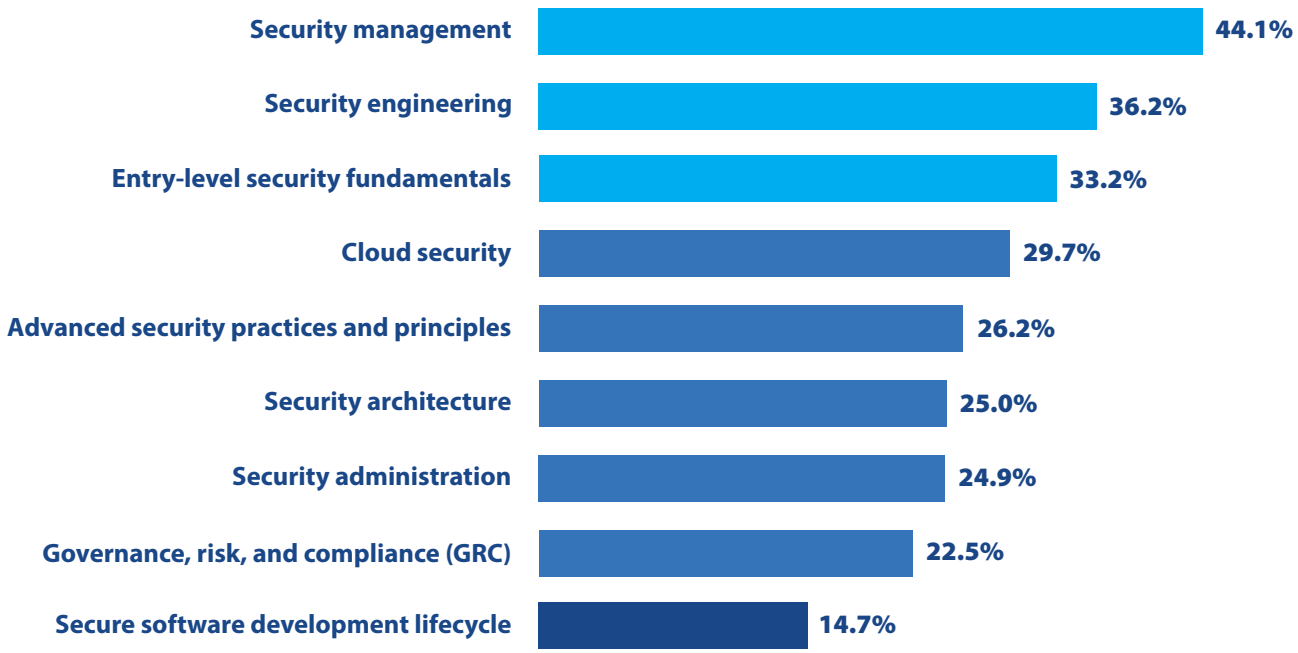

Figure 27: Types of cybersecurity certifications most beneficial to career paths.

Cybersecurity professionals only remain effective as long as they stay current on evolving threats and the latest defenses. Opportunities for interesting work, increased compensation, and advancement may depend on demonstrating knowledge and competence in "hot" domains. Moreover, most cybersecurity team members *enjoy* learning about the latest technologies and techniques used by both evildoers and good guys.

For these reasons, ongoing cybersecurity training education in general, and professional certifications in particular, make security professionals both more effective (minimizing risks and reducing costs) and happier on the job (decreasing staff turnover and retaining key skills).

But what types of cybersecurity certifications do cybersecurity team members perceive as most beneficial for their careers?

Section 2: Perceptions and Concerns

The top choice is "Security management" (selected by 44.1% of respondents), which covers management and leadership skills for cybersecurity team leaders up to CISOs. Courses typically enroll people with established technical skills and educate them in areas such as planning and cybersecurity program management, alignment of security with organizational priorities, and team leadership. These days, when cybersecurity groups regularly interact with top executives and boards of directors, security management curriculums often include discussions of communicating upward to executives and outward to peers in other business functions.

Coming next on the list is "Security engineering" (36.2%). Certification programs in that area focus on applying engineering principles and processes to areas like project planning and management, security systems design, technical procurement, and security operations management. Security engineering programs are particularly popular with people who are, or aspire to be, security or systems engineers or analysts.

"Many organizations seek to bring intelligent people into the field [of cybersecurity] though a combination of structured and on-the-job training. In fact, entry-level security fundamentals certifications were selected more often than any other certification type in nine of the 17 countries covered in our survey."

But not all certification programs are for established security professionals or specialists. The third most often cited certification type is "Entry-level security fundamentals." Because of the severe shortage of cybersecurity professionals (see page 23), many organizations seek to bring intelligent people into the field though a combination of structured and on-the-job training.

In fact, "Entry-level security fundamentals" certifications were selected more often than any other certification type in nine of the 17 countries covered in our survey:

- Brazil
- China
- Columbia
- France
- Germany
- Mexico
- Saudi Arabia
- Spain
- Turkey

Certifications in "Cloud security" are also in demand (29.7%). This reflects the continuing migration of application workloads and data to cloud platforms and services and the need to master new skills and cloud-native security tools.

The other types of certifications listed in Figure 27 are also in demand, although not quite as widely. That's because most of them provide knowledge in areas that draw fewer (although usually very dedicated) practitioners, such as security architecture, security administration, and secure software development.

Section 3: Current and Future Investments

IT Security Budget Allocation

What percentage of your employer's IT budget is allocated to information security (e.g., products, services, personnel)?

Do you (information technology department) still love us (cybersecurity)?

You proclaim that we are a top priority. But are you backing that up with hard currency – is the percentage of your funding allocated to us rising or falling?

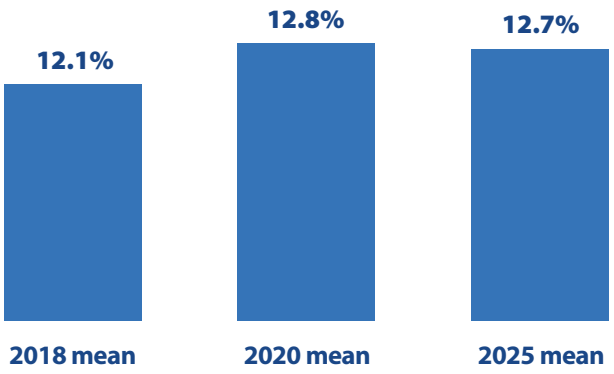

Figure 28: Percentage of IT budget allocated to security.

As we can see from Figure 28, the upward trend has flattened out.

But we're okay with that. IT budgets have been rising substantially, so just keeping the same allocation means our budgets have been rising nicely too (see the next section of this report). And we know that cybersecurity budgets jumped in the 2020-2021 timeframe to cope with increasing security needs related to the COVID pandemic and the work-at-home explosion. So we can't complain that our allocation has remained steady or dropped just a bit when those pressures abated.

But how does your specific organization compare with all the others out there? Let's look at Figure 29. If the percentage of the IT budget going to cybersecurity falls in the 6% - 15% range, then you are comfortably close to the average. If the allocation is greater than 16%, IT and cybersecurity have a great relationship. If it's 5% or less, somebody needs counseling.

Percentage of IT budget spent on security	1%–5%	6%–10%	11%–15%	16%–20%	>20%
Percentage of organizations	13.3%	30.0%	27.4%	20.6%	8.6%

Figure 29: Percentage of organizations at different levels of allocation.

Section 3: Current and Future Investments

We can also take into account the data shown in Figure 30. In a few countries (South Africa, Colombia, Brazil, China), the *average* allocation is more than 14%. In a few others (Japan, Singapore, Germany), the average is 11% or less.

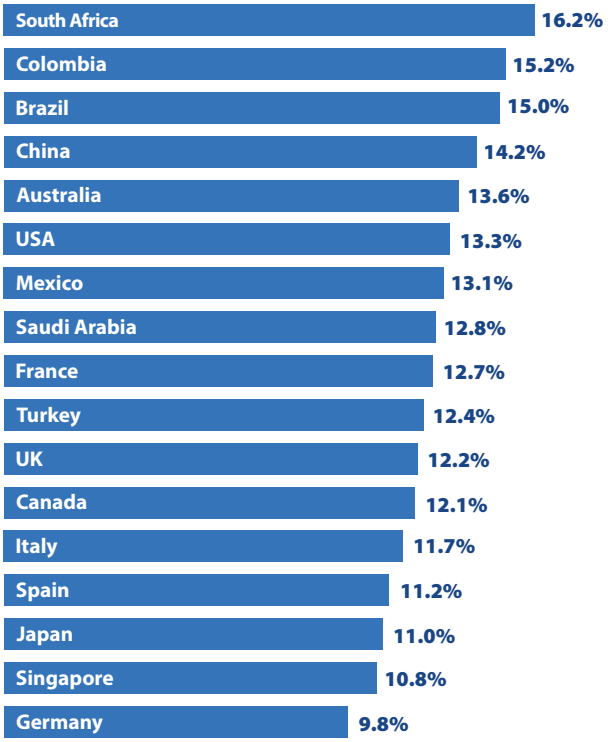

Figure 30: Percentage of IT budget allocated to security, by country.

Although variations across industries are much less, the numbers in Figure 31 are also interesting. The percentage of the IT budget allocated to cybersecurity is highest in telecom and technology (14.0%) and finance (13.9%), and lowest in government (12.0%) and manufacturing (11.4%).

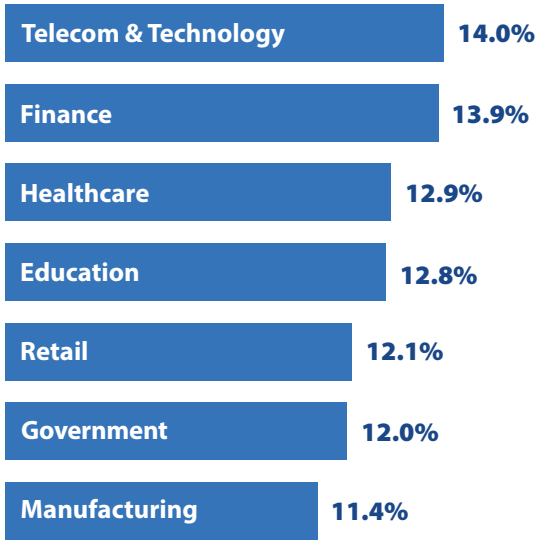

Figure 31: Percentage of IT budget allocated to security, by industry.

"Do you (information technology department) still love us (cybersecurity)? You proclaim that we are a top priority. But are you backing that up with hard currency – is the percentage of your funding allocated to us rising or falling?"

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 2025?

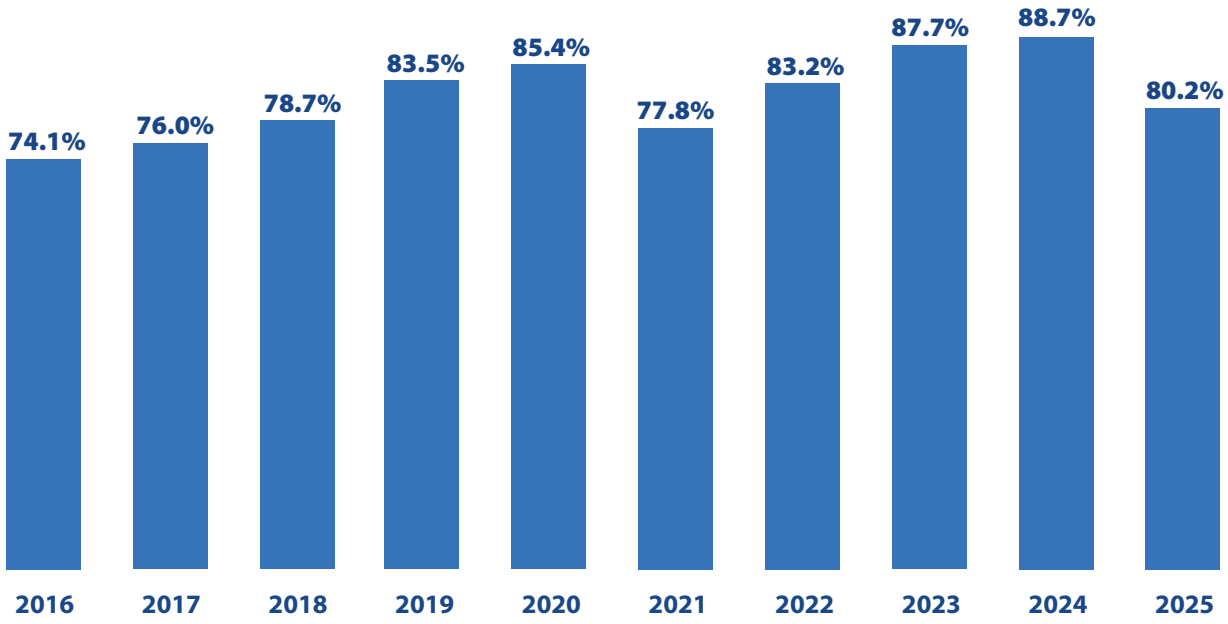

Figure 32: Percentage of organizations with rising IT security budgets.

Although economic growth and corporate profits across the world have been uneven, IT security budgets have continued to grow. As shown in Figure 32, four out of five organizations expect their security budgets to increase this year. That's down slightly from last year, when almost nine out of 10 respondents predicted an increase, but it still demonstrates that organizations are continuing to invest in improving their security postures.

Another way of looking at the data is that only 6.5% of organizations expect their budgets to go down this year, while 13.4% predict they will stay about equal.

"On average, IT security budgets are expected to increase 4.3% this year. That is a bit off from last year's record-high 5.7%, but still quite healthy, thank you very much."

Section 3: Current and Future Investments

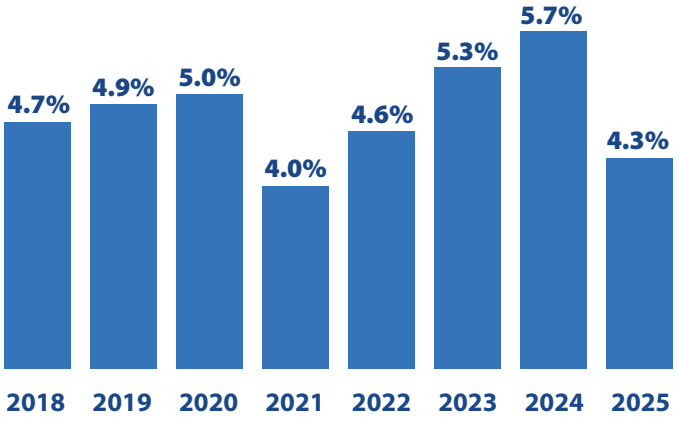

Figure 33: Mean annual increase in IT security budgets.

On average, IT security budgets are expected to increase 4.3% this year (see Figure 33). That is a bit off from last year's record high of 5.7%, but still quite healthy, thank you very much.

Figure 34 shows a breakdown of the size of budget increases for IT security groups that expect one. (This chart excludes groups that anticipate equal or lower budgets.) As in past years, the sweet spot among organizations expecting budget growth is an increase of between 5% and 9%.

There are significant differences in expected budget changes across industries (see Figure 35). Manufacturing, retail, and healthcare organizations anticipate gains of 4.9%, 4.7%, and 4.5%, respectively, while finance, government, and education have more modest expectations of 3.6%, 3.4%, and 3.1%.

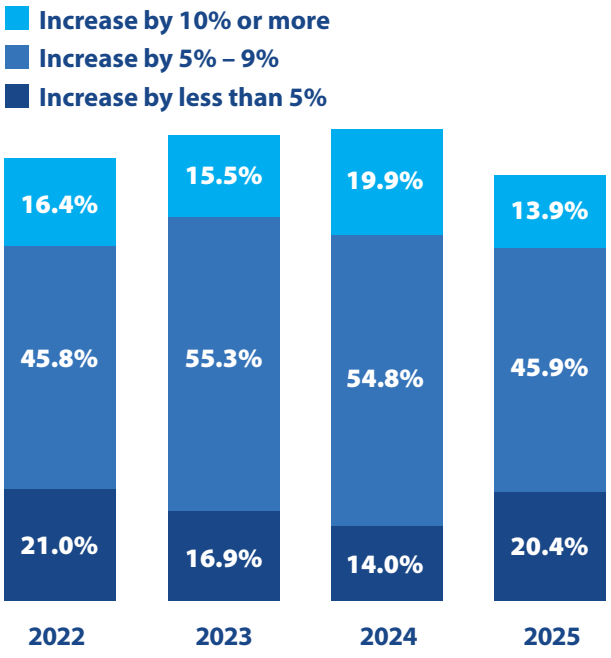

Figure 34: Breakdown of annual increase of IT security budgets (excludes organizations expecting declining or flat budgets).

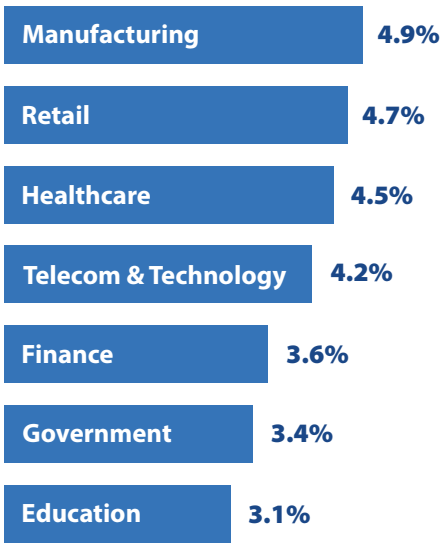

Figure 35: Mean IT security budget increase, by industry.

Section 3: Current and Future Investments

Top Priorities for Improving Identity Security

What are your organization's top priorities in the next 12 months for improving identity security? (Select up to five.)

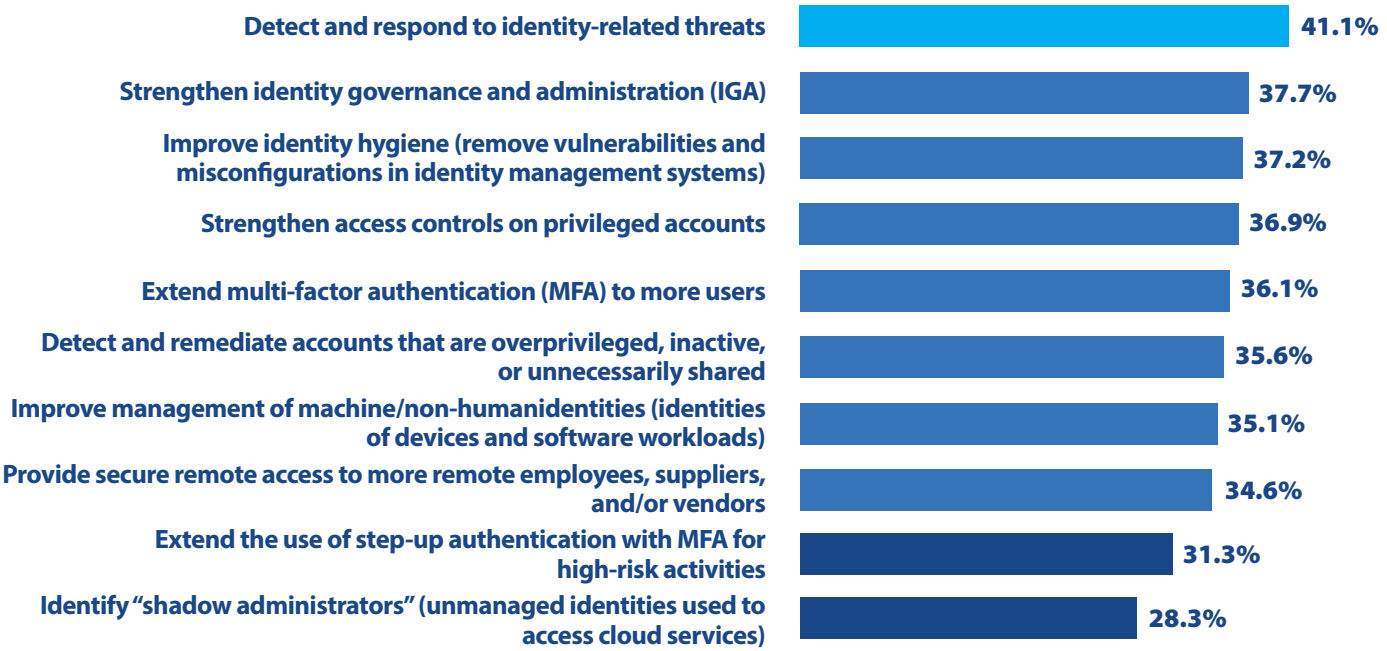

Figure 36: Top priorities for improving identity security.

Identity security has long been a cornerstone of cybersecurity, ensuring that the right people have the right access to the right assets. It focuses on protecting accounts, sensitive data, and mission-critical assets by leveraging policies, processes, and tools that govern identity authentication and authorization.

However, in the last few years, identity security has become more difficult and more important.

More difficult because:

- User accounts, credentials, and critical assets are now scattered across more applications, devices, and computing environments.
- The number of user accounts and non-human identities (NHIs) has exploded.
- Identities and credentials continue to be targeted, stolen, and used by a growing number of threat actors.

Section 3: Current and Future Investments

More important because:

- Secure identities are central to zero trust security, which relies on identities for all access decisions and must ensure that users can only reach the assets they need to do their jobs and only at the moment they need them (i.e., enforcing the principle of least privilege).
- Industry frameworks and compliance standards increasingly require identity security controls such as MFA and dynamic risk assessments based in part on identity information.
- Many organizations depend on identity-specific information to deliver "frictionless" services to some customers but limit access to others.

To examine some of the impact of these factors, we asked respondents to select up to five of their organization's top priorities for improving identity security over the next 12 months (see Figure 36).

The priority selected most often, by 41.4% of the respondents, is "Detect and respond to identity-related threats." This certainly makes sense, since threat actors are increasingly relying on stolen identities and credentials to launch a wide variety of attacks.

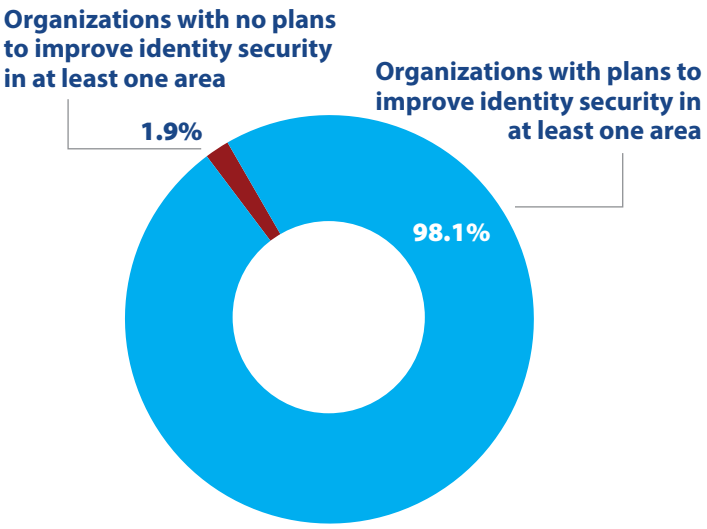

Figure 37: Organizations planning to improve identity security in at least one area.

The second item on the list is "Strengthen identity governance and administration (IGA)" (37.7%). IGA is mostly concerned with managing identity lifecycles efficiently and in complete alignment with corporate and security policies. Strengthening and automating IGA processes such as identity provisioning and de-provisioning improve security and compliance. They also allow adminisrators to spend more time on strategic projects and less on routine tasks.

Just behind strengthening IGA comes the goal of improving identity hygiene (37.2%). Identity hygiene involves eliminating vulnerabilities and misconfigurations in identity management systems. This is critical because threat actors have recognized that if they can compromise user directories and other elements of the identity infrastructure, they can impersonate users, compromise their accounts, grant themselves additional permissions (privilege escalation), and freely traverse applications and systems (lateral movement) without being observed.

Strengthening access controls on privileged accounts (36.9%) involves putting better monitoring and more defenses around the activities of users who have the most privileges (and if compromised, could do the most damage). These users include top executives who work with business-critical assets like financial accounts and confidential information and IT system administrators who manage (and can potential modify or disable) key business and technical processes.

Other key priorities include extending the enforcement of MFA to more users (often to comply with regulations), identifying and remediating risky accounts that could be leveraged by attackers, and creating identities for software workloads and devices so their access to other systems can be managed (e.g., you don't want that new security tool or device to suddenly start reaching into your customer database).

Is this growing interest in identity security widespread? The answer is clearly "yes!" As illustrated in Figure 37, more that 98% of organizations plan to improve identity security in at least one area during the coming year.

Section 3: Current and Future Investments

Preferences for AI in Security Products

Select the option that best describes your organization's overall preference for purchasing security products that feature artificial intelligence (AI) technologies.

Unless you've been living in a cave without internet connectivity (and why would you, since today you can live in a cave *with* internet connectivity), you know that AI will soon be everywhere.

But do cybersecurity professionals believe that AI is ready to deliver value in the context of security? Are they looking for AI-based capabilities when they evaluate security tools?

Well, more than four out of five (82.1%) have a moderate or strong preference for security products that feature AI technologies. Only 5.6% say they have no preference (see Figure 38).

However, the strength of preferences do vary by country and industry (see Figures 39 and 40). Mexican respondents were unanimous in having at least at moderate preference, while residents of the United States, Italy, Germany, and Canada are more skeptical about AI. Cybersecurity professionals at telecom and technology companies and finance firms are signicantly more enthusiastic than those at educational institutions and healthcare companies.

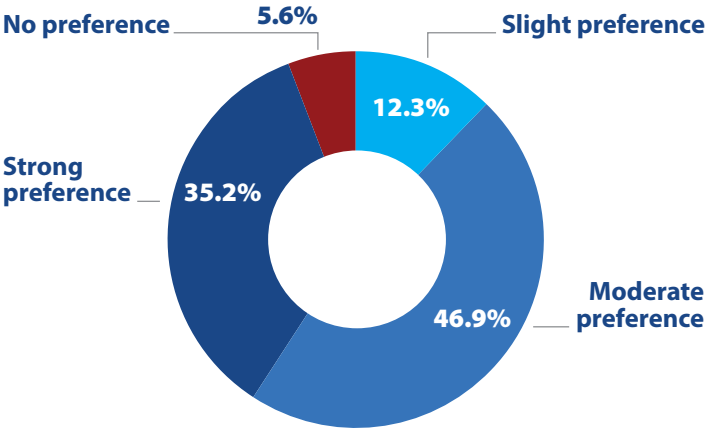

Figure 38: Preference for AI in security products.

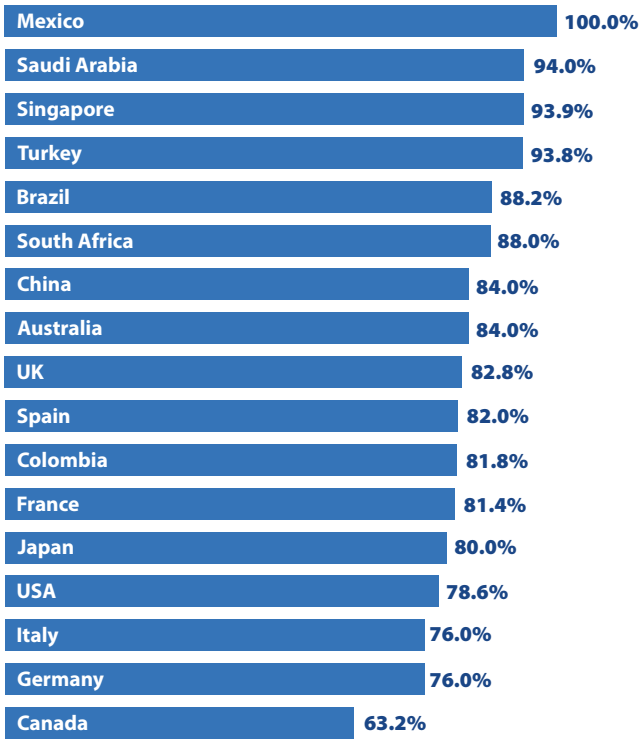

Figure 39: Moderate or strong preference for AI in security tools, by country.

Section 3: Current and Future Investments

The last time we asked this question was in the 2021 CDR, and it's interesting to note that preferences haven't changed much since then (see Figure 41). In fact, 5.3% *fewer* respondents in the latest survey say they have a strong preference, although that decline is partially offset by a 2.1% increase in those who say they have a moderate preference.

Isn't that counterintuitive, given that AI features in security products are much more common now than they were four years ago? We think these results reflect the fact that AI is now expected to be utilized in security tools, rather than just hoped for. You can afford to have a moderate preference if you are pretty sure you are going to get what you want as a matter of course, rather than having to seek it out.

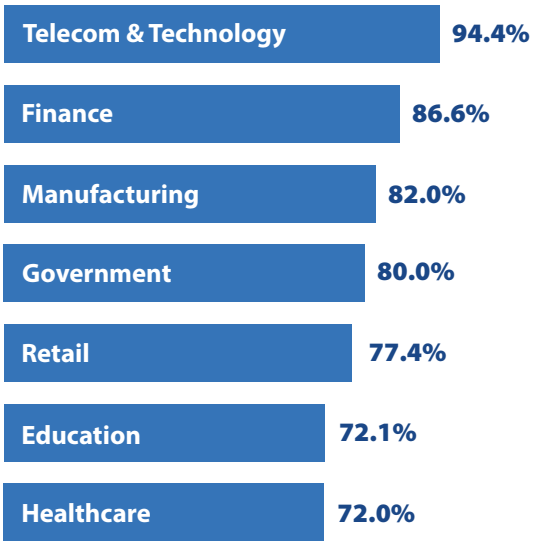

Figure 40: Moderate or strong preference for AI in security tools, by industry.

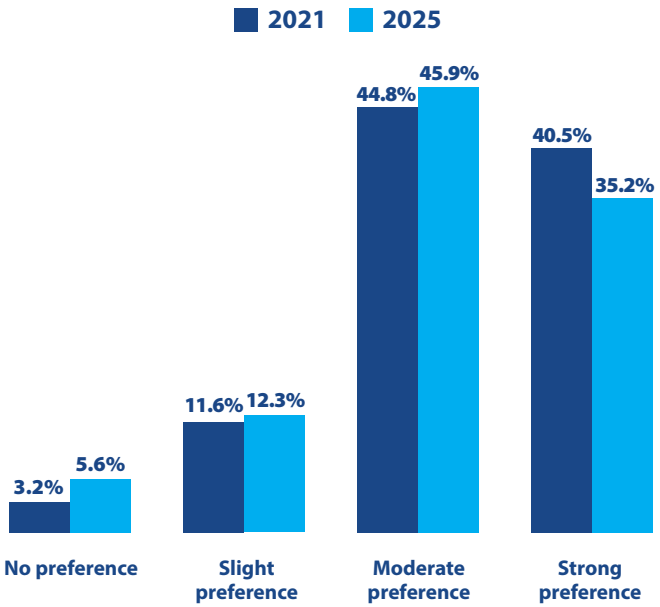

Figure 41: Preferences for AI in security products, 2025 compared to 2021.

"You can afford to have a moderate preference if you are pretty sure you are going to get what you want as a matter of course, rather than having to seek it out."

Section 3: Current and Future Investments

Outsourcing to Managed Security Service Providers (MSSPs)

Which of the following IT security functions does your organization outsource to a managed security service provider (MSSP)? (Select all that apply)

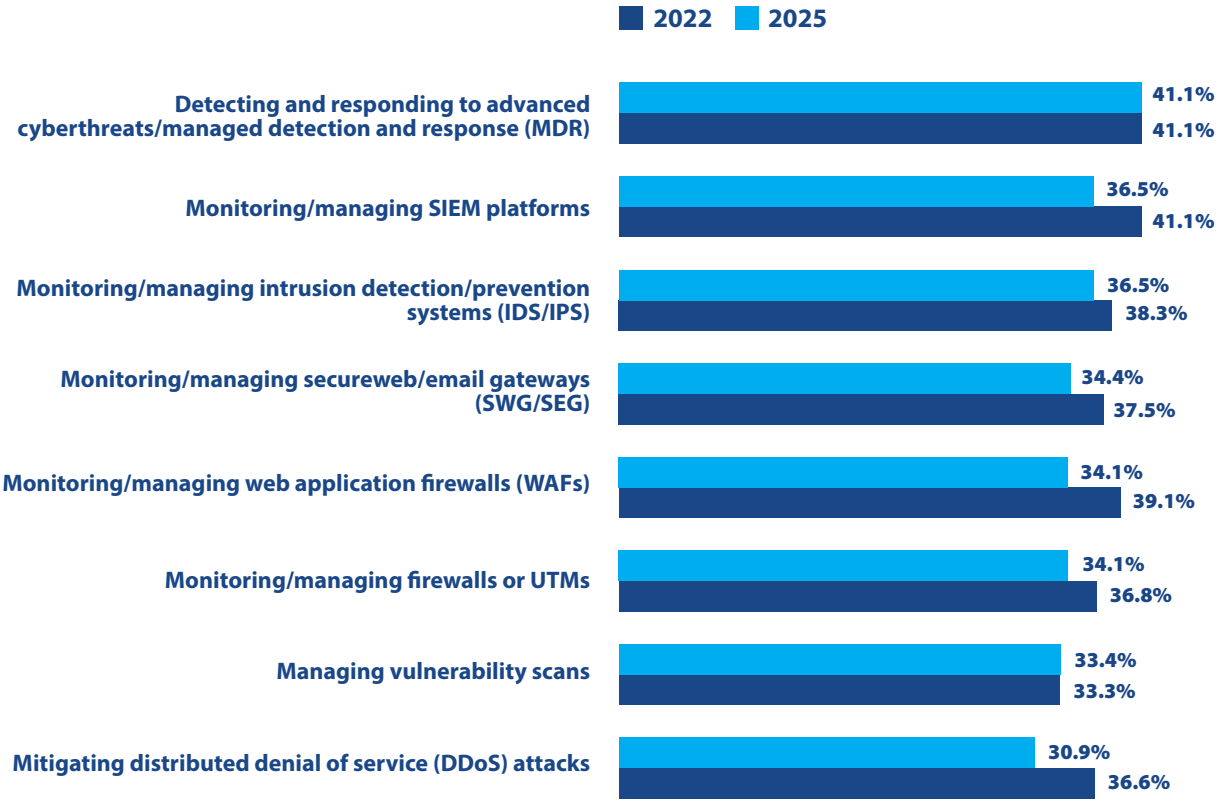

Figure 42: IT security functions outsourced to an MSSP in 2022 and 2025.

As you have probably noticed, the shortage of experienced cybersecurity professionals is a running theme in this report (see pages 23, 25, and 29). One obvious solution is to outsource security activities to managed security service providers (MSSPs). But MSSPs aren't ideal in all situations. In fact, they are most widely used for tasks that:

- Are labor intensive
- Can be automated and performed remotely
- Are generic across industries and do not require a detailed knowledge of an organization's unique business processes or technology

So, what IT security functions do organizations outsource to MSSPs most often? Figure 42 compares respondents' answers in 2022 and 2025.

Section 3: Current and Future Investments

The leading response in both years was "Detecting and responding to advanced cyberthreats/managed detection and response." This is a classic example of a service that is very labor intensive, but includes tasks that can be automated and performed remotely, such as triaging alerts, notifying affected parties, and initiating containment actions.

The next five functions all involve monitoring and managing security tools: SIEM platforms, intrusion protection systems, web and email gateways, and various types of firewalls. Since the tools are generic across industries (although they may require some industry knowledge for tuning), it often makes sense to hire an MSSP that already knows the product inside and out rather than training an internal specialist. This dynamic seems to have held steady over time: the ordering of the different outsourced functions didn't change much between 2022 and 2025.

However, the number of organizations subscribing declined by several percentage points for six of the eight services included in the survey. At first glance, this might imply that there has been a significant pullback in outsourcing to MSSPs. However, as shown in Figure 43, the percentage of organizations not working at all with MSSPs declined slightly from 6.8% in 2022 to 10.3% in 2025. So it seems that rather than rejecting the use of MSSPs, some organizations are just using them more selectively.

At one time it was thought that outsourcing to MSSPs would be most attractive to smaller organizations that could not afford specialists in every area of security. However, the data in Figure 44 shows that is not the case now. The percentage of organizations working with MSSPs is essentially the same for those with 500-999 employees, those with 10,000-24,999 employees, and everyone in between. The usage of MSSPs only drops off for the largest organizations: those with at least 25,000 employees.

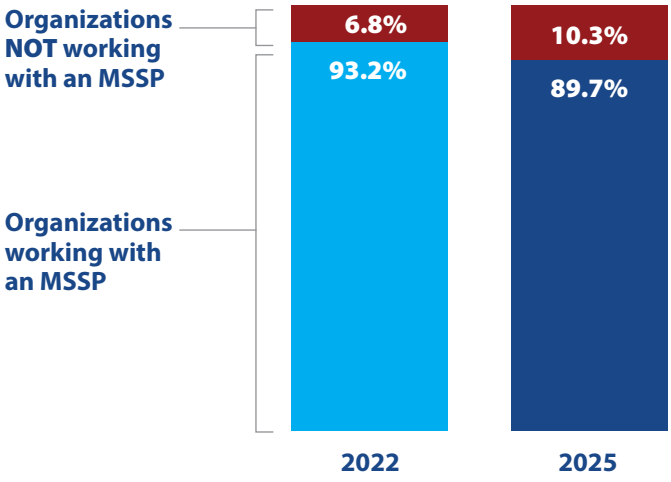

Figure 43: Organizations not working with an MSSP in 2022 and 2025.

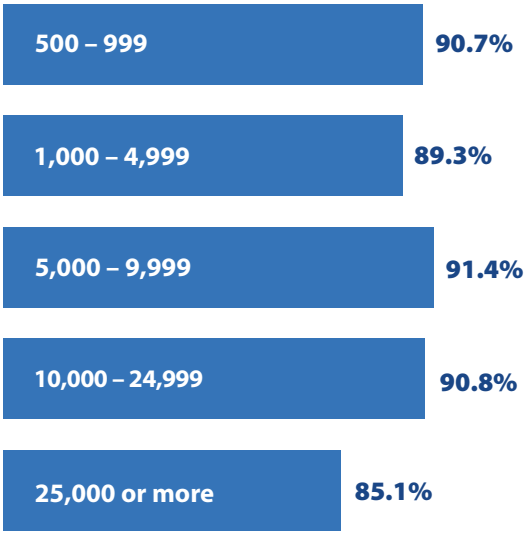

Figure 44: Organizations working with MSSPs, by employees.

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 email gateway (SEG)	58.4%	27.8%	13.7%
Intrusion detection / prevention system (IDS/IPS)	57.2%	32.0%	10.8%
Network access control (NAC)	56.7%	33.2%	10.2%
Secure web gateway (SWG)	56.4%	31.0%	12.5%
Data loss / leak prevention (DLP)	55.4%	33.7%	10.9%
Advanced threat prevention (sandboxing, ML/AI)	50.9%	37.3%	11.8%
Denial of service (DoS/DDoS) prevention	49.9%	34.4%	15.7%
SSL/TLS decryption appliances / platform	49.6%	36.3%	14.1%
Next-generation firewall (NGFW)	44.0%	41.8%	14.2%
Network behavior analysis (NBA) / NetFlow analysis	42.8%	37.3%	19.9%
Deception technology / distributed honeypots	36.6%	39.6%	23.9%

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

You might have heard that "data is the new perimeter," or "applications are the new perimeter," or "identities are the new perimeter," or "there is no more perimeter." Well, our almost-blind reliance on the old (network) perimeter may be gone, but that doesn't mean the network perimeter doesn't still exist or isn't an excellent place to position defenses.

In reality, a huge number of attacks are blocked every day at entry points to networks. So are attempts to exfiltrate data and intellectual property. Also, monitoring activity on the network is crucial to detecting nascent and ongoing attacks.

For these reasons, cybersecurity teams can benefit from knowing the network security technologies their peers are relying on today and the ones they plan to implement in the future.

Table 1 shows what percentage of organizations currently use each of 11 core network security technologies and how many plan to acquire solutions of that kind.

The first five rows in Table 1 are what we might call the "war horses" of network security: secure email gateways (SEGs), intrusion detection and prevention systems (IDS/IPS), network access control (NAC) products, secure web gateways (SWGs), and data loss (or leak) prevention (DLP) solutions. All of these are in production in at least 55% of organizations.

Section 3: Current and Future Investments

These five were the leading five in the last CDR, too, but the order has changed. SEGs moved to the top spot for installations from third place. NAC moved from fifth to third place. SWGs dropped from first place to fourth.

Why are these five so widely used?

SEGs scan incoming (and sometimes outgoing) email traffic to identify and block emails with suspicious links, malicious content, or dangerous attachments. The technology keeps evolving and now typically incorporates AI and threat intelligence capabilities to help it recognize suspicious deviations from norms and content associated with attacks on other organizations, among other enhancements. It is in use in 58.4% of enterprises, an increase of 1.7% from last year's survey.

IDS/IPS products continue to be core defenses. They are used to detect a wide range of activities associated with intrusions. Installations rose slightly last year, reaching 57.2%.

NAC ensures users can't log onto the corporate network unless they meet certain conditions, for example, such as using a known device running up-to-date endpoint protection products.

SWGs monitor web traffic to screen out malicious content and dangerous attachments. They also help incident response and forensic teams identify where web-based attacks originated and how they entered the network.

DLP focuses on preventing sensitive information from leaving the network. That is critical for two security use cases:

- Preventing threat actors from exfiltrating compromised data and files
- Blocking employees and other insiders from sending confidential information to outside locations where it might be vulnerable

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 39.6%. Deception solutions create fake computing environments, including simulated user accounts, servers, applications, databases, and file stores. They also track the actions of threat actors in the simulated environment, revealing their tactics, techniques, and procedures (TTPs).

Next: endpoint security technologies in use and planned for acquisition (page 43).

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)	73.9%	21.0%	5.1%
Data loss / leak prevention (DLP)	56.8%	32.2%	11.0%
Disk encryption	56.5%	32.3%	11.2%
Endpoint detection and response (EDR)	54.5%	32.8%	12.7%
EPP / Advanced anti-virus / anti-malware (machine learning, behavior monitoring, sandboxing)	54.3%	35.0%	10.7%
Browser or Internet isolation / micro-virtualization	53.4%	33.0%	13.5%
Digital forensics / incident resolution	46.5%	36.6%	16.9%
Deception technology / honeypot	38.6%	40.7%	20.7%

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

Signature-based anti-malware technology is not dead! It might be taking a different form, though.

Not dead, because installations rose 3.6% over the past year, from 70.3% to 73.9%, making it by far the most widely installed endpoint technology in our survey (see Table 2).

But perhaps not in the same form: we suspect that the reported growth comes from signature-based anti-malware capabilities in endpoint security packages, rather than from standalone anti-virus and anti-malware products. Still, it's worth noting that there doesn't seem to be a mass movement to leave signatures behind and rely entirely on behavioral analysis and AI pattern recognition.

The second most frequently installed endpoint security technology remains the same as last year: endpoint DLP. Products in this field examine outgoing files and flag, or simply block, items that contain words, phrases, and numbers that suggest sensitive information, including intellectual property and financial account numbers. They can take actions such blocking outgoing files or encrypting them before transmission. Endpoint DLP is currently installed at 56.8% of organizations, down 2.3% from the previous survey.

Another entry in the "it's definitely not dead" category is disk encryption, which jumped from sixth place in last year's survey to third place in this one. Its installation rate is 56.5%, only slightly behind DLP.

Section 3: Current and Future Investments

Endpoint detection and response (EDR) and endpoint protection platform (EPP) technologies each dropped one spot in the list, but remain popular, being installed in 54.5% and 54.3% of organizations, respectively. EDR solutions monitor endpoints to detect malware and events associated with attacks. EPP solutions usually include EDR features plus additional capabilities to help incident responders and threat hunters analyze what threat actors have been doing.

The last technology installed in more than half of organizations (53.4%) is "Browser or internet isolation/micro-virtualization." This technology involves running browser or application sessions in an isolated space so users can work as usual but attackers have no way of accessing their computers or mobile devices.

In the "planned for acquisition" column, the leaders are deception technology/ honeypot and digital forensics. Respondents at 40.7% and 36.6% of organizations say these are planned for the coming year.

Next: application and data security (page 45).

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	66.4%	23.2%	10.4%
Web application firewall (WAF)	63.1%	28.0%	8.9%
API gateway / protection	62.6%	29.5%	7.9%
Database activity monitoring (DAM)	56.6%	30.1%	13.3%
Application container security tools / platform	55.5%	34.8%	9.7%
Cloud access security broker (CASB)	52.6%	32.4%	15.0%
File integrity / activity monitoring (FIM/FAM)	50.0%	35.6%	14.4%
Runtime application self-protection (RASP)	47.7%	35.0%	17.3%
Application delivery controller (ADC)	47.5%	36.0%	16.5%
Static /dynamic / interactive application security testing (SAST/DAST/IAST)	45.5%	37.4%	17.1%
Third party code analysis	42.3%	35.0%	22.7%
Bot Management	37.4%	40.5%	22.1%

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

The same six application and data security technologies headed up our list of must-haves in both the last survey and this one. What stands out is that the "currently in use" percentage increased for every one of them over the year. In fact, it increased for 11 of the 12 technologies in this category. The only exception was application delivery controller (ADC) technology, which declined slightly.

Database firewall and web application firewall (WAF) technologies reached installation rates of 66.4% and 63.1%, respectively. Those numbers are up 6.3% and 7.7% from two surveys ago, indicating a major surge of interest in monitoring and protecting individual databases and web applications. Besides being good security, this trend may also reflect the emergence of the data security posture (DSP) and application security posture (ASP) concepts, which involve ongoing measurement and systematic improvement in security capabilities in those two spheres (see page 57 in "The Road Ahead" section).

Section 3: Current and Future Investments

API protection continues to be a hot topic. As organizations develop and deploy additional modular, cloud-based applications that communicate with other applications and cloud services through APIs, threat actors are targeting those interfaces more often. API gateway and protection technologies are now installed in 62.6% of organizations.

The next three application and data security technologies, in terms of installations, are database activity monitoring (DAM), application container security tools and platforms, and cloud access security brokers (CASBs). These are currently in use in 56.6%, 55.5%, and 52.6% of organizations.

Bot management lags in installations (37.4%) but rates the highest in this technology category for planned acquisitions (40.5%). Organizations want to be able to control traffic from bots because they are often used to launch ransomware, spam, and DDoS attacks, among others.

Application security testing technology, in its static, dynamic, and interactive flavors (SAST, DAST, and IAST), is similarly at near the bottom of Table 3 for "currently in use" (45.5%), but strong in the "planned for acquisition" column (37.4%).

We now turn to our final table in this survey, which covers current use and planned acquisition of security management and operations technologies (page 47).

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	57.5%	29.9%	12.6%
Patch management	55.8%	30.8%	13.4%
Security configuration management (SCM)	55.5%	31.8%	12.7%
Cyber risk quantification / scorecard	55.4%	32.7%	11.9%
Vulnerability assessment / management (VA/VM)	53.8%	33.9%	12.3%
Security information and event management (SIEM)	53.7%	35.5%	10.8%
Penetration testing / attack simulation software	50.0%	35.3%	14.7%
Threat intelligence platform (TIP) or service	46.8%	37.7%	15.5%
Advanced security analytics (e.g., with machine learning, AI)	46.6%	42.0%	11.4%
Full-packet capture and analysis	45.1%	37.9%	17.0%
Security orchestration, automation and response (SOAR)	44.5%	39.1%	16.4%
User and entity behavior analytics (UEBA)	44.5%	37.6%	17.9%

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

For the fourth year in a row, Active Directory protection is at the top of our security management and operations technology table. It is currently in use in 57.5% of organizations (see Table 4). Active Directory is the enterprise directory in the center of the identity security infrastructure for many enterprises. Many threat actors are targeting it because compromising Active Directory would give them access to identity information and credentials of all kinds, and potentially the ability to impersonate privileged users, escalate privileges at will, and move laterally throughout corporate networks. Directory services are also critical for managing non-human identities. These include identities assigned to software and hardware entities such as application workloads, IoT devices, and industrial control systems. Directories also provide role and permission information to support zero trust security.

Section 3: Current and Future Investments

Patch management will probably never go out of style. It is a bedrock function of IT operations and security teams. Unfortunately, it usually involves painfully time-consuming and generally unrewarding tasks, which is why many organizations would like to automate patch management processes. It's also the reason that 55.8% have installed one or more patch management products.

In third place is security configuration management (SCM) technology. Installed in 55.5% of organizations, SCM helps security teams manage security applications and devices and document that they are enforcing regulatory requirements and company policies. It not only helps organizations keep security configurations straight, but it also gives them the power to deploy configuration changes quickly across the enterprise.

Other security management and operations technologies in use in more than half of organizations are cyber risk quantification/scorecard (55.4%), vulnerability assessment/management (VA/VM) (53.8%), security information and event management (SIEM) (53.7%), and penetration testing/attack simulation software (50.0%).

What is on the security management and operations shopping list for 2025? The top items planned for acquisition are advanced security analytics (42.0%), security orchestration, automation and response (SOAR) solutions (39.1%), full packet capture and analysis (37.9%), and threat intelligence platforms (TIPs) or services (37.7%).

Section 4: Practices and Strategies

Frameworks and Standards Used to Assess Cybersecurity

Which frameworks and standards does your organization use to assess the effectiveness and compliance of your cybersecurity program? (Select all that apply.)

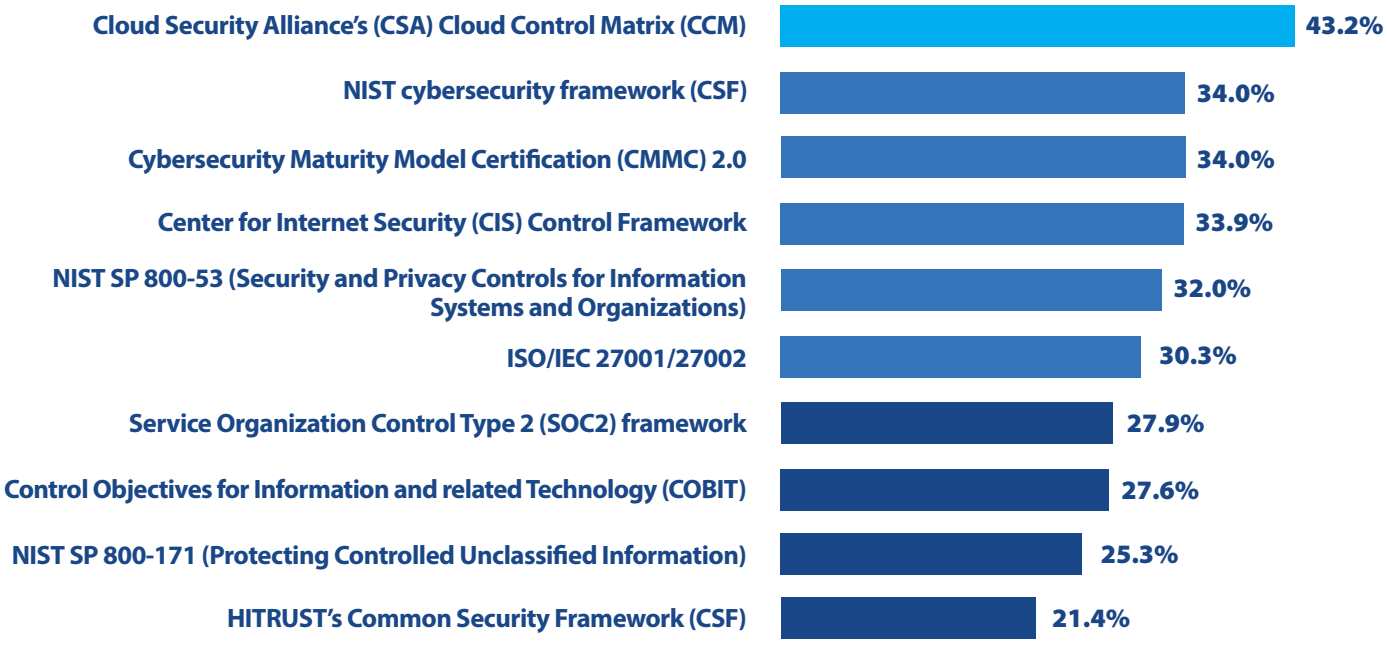

Figure 45: Frameworks and standards organizations use to assess cybersecurity programs.

A few years ago, it was not uncommon for cybersecurity professionals to be unenthusiastic or even hostile regarding frameworks and standards promulgated by government agencies and industry standards bodies. They were dismissed as incomplete, lagging behind the latest threats and solutions, and victims of lowest common denominator groupthink. They reminded some experts of the old saying that "a camel is a horse that was designed by a committee."

How the tide (and the camel) have turned! Today, the great majority of cybersecurity groups are using one or more frameworks or standards to define best practices, set priorities, guide investments in staff and technologies, and assess the effectiveness and compliance of their organizations.

Why the about-face? Partly because what were formerly recommended controls and suggested best practices have become mandatory, as governments and standards bodies respond to demands that organizations do more to protect the public from cybercrime, espionage, and other forms of aggression. Partly because governments and businesses have invested time and resources improving the completeness, quality, and timeliness of the standards documents so they represent genuine best practices drawn from the experiences of cybersecurity practitioners and experts. And partly for practical considerations, such as qualifying for cyber insurance policies and providing cover in the event of breaches and lawsuits ("It's not our fault, your honor, we complied with the standards.")

Section 4: Practices and Strategies

"A few years ago, it was not uncommon for cybersecurity professionals to be unenthusiastic about frameworks and standards...They were dismissed as incomplete, lagging behind the latest threats and solutions, and victims of lowest common denominator groupthink. They reminded some experts of the old saying that "a camel is a horse that was designed by a committee...

How the tide (and the camel) have turned!"

But which standards and frameworks are being used most by cybersecurity programs? We added a new question to this year's CDR to find out (see Figure 45).

One caution about the data. Our sample is somewhat weighted toward North American and European organizations. That may slightly exaggerate interest in frameworks endorsed by U.S. government agencies, such as those related to NIST and HIPAA/HITRUST. But we think the results are still broadly valid.

The framework most often cited by our respondents (43.2% of them) is the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM), which articulates 197 control objectives across 17 security domains related to cloud platforms and services. One of the strategies of the CSA is to map its controls to other prominent standards, such as those published by NIST, ISO, and PCI. This allows organizations to use a "secure once, comply many" approach where, by satisfying one set of requirements, they can document compliance (or near-compliance) with several others.

NIST (the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce) is extremely influential. It has three different frameworks on our list, including the NIST cybersecurity framework (CSF), cited by 34.0% of respondents, and SP 800-53, with security and privacy controls required for U.S. federal agencies (32.0%). Although most NIST frameworks and standards are only mandatory for U.S. government agencies and defense companies, they are perceived as quite comprehensive and very valuable by enterprises in many industries.

The Cybersecurity Maturity Model Certification (CMMC) (also 34.0%) is a framework specifically designed to assess compliance with a variety of NIST frameworks. Although it is intended for defense contractors in the United States, organizations in other sectors have also found CMMC to be a good tool for assessing the maturity and effectiveness of their cybersecurity programs.

The other framework near the top of our list is the Center for Internet Security (CIS) Control Framework (33.9%). It provides a prioritized set of best practices to defend against common attack vehicles such as malware, ransomware, web application hacking, insider attacks, and targeted Intrusions.

We said earlier that "the great majority" of cybersecurity groups are using frameworks and standards like these. How much is that? As shown in Figure 46, 97.1% are using at least one framework or standard in some fashion.

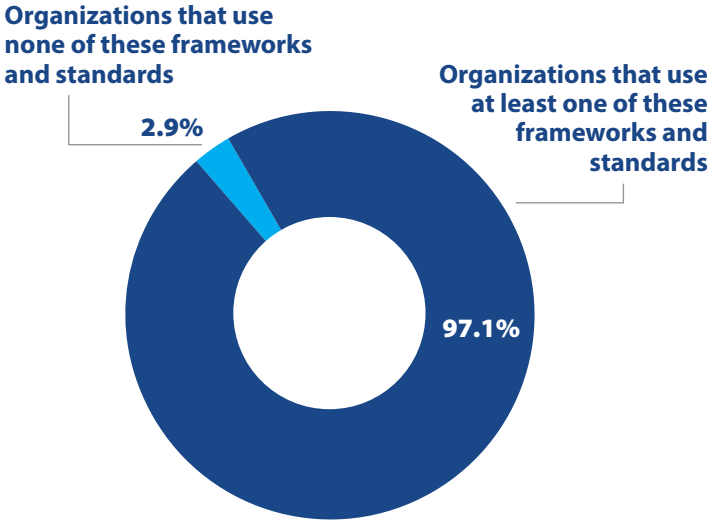

Figure 46: Organizations that use at least one framework or standard to assess their cybersecurity program.

Section 4: Practices and Strategies

Impact of Implementing Zero Trust Network Access (ZTNA)

Describe your agreement with the following statement: "Implementing zero trust network access (ZTNA) in our organization has significantly improved our security posture and our ability to defend against sophisticated threats."

"Zero trust" may be the most popular two words in cybersecurity today. Cybersecurity websites, newsletters, and blogs, not to mention courses and conferences, are full of "zero trust network access," "zero trust principles," "zero trust frameworks," "zero trust models," "zero trust architectures," "zero trust strategies," "zero trust solutions," "zero trust platforms," "zero trust this," "zero trust that," and "zero trust the other."

But are cybersecurity organizations just giving lip service to the latest fad, or is this zero trust thing producing results?

We asked our respondents to describe their agreement with the statement: "Implementing zero trust network access (ZTNA) in our organization has significantly improved our security posture and our ability to defend against sophisticated threats."

And what do you know: zero trust is real! Over half of the respondents (50.8%) somewhat agree with that statement, and another third or so (34.9%) strongly agree. Only 3.0% somewhat or strongly disagree, and 11.4% won't commit themselves to a position.

These figures are consistent with the fact that zero trust principles have been absorbed into many frameworks and standards. They have also helped turn security concepts like MFA, continuous adaptive authentication, privileged access management (PAM), and micro-segmentation from nice-to-haves to must-haves.

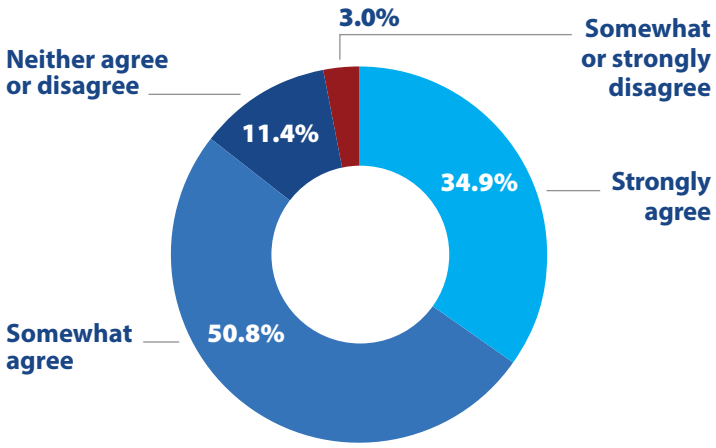

Figure 47: Agreement that implementing ZTNA has significantly improved the organization's ability to defend against sophisticated threats.

"'Zero trust' may be the most popular two words in cybersecurity today."

Section 4: Practices and Strategies

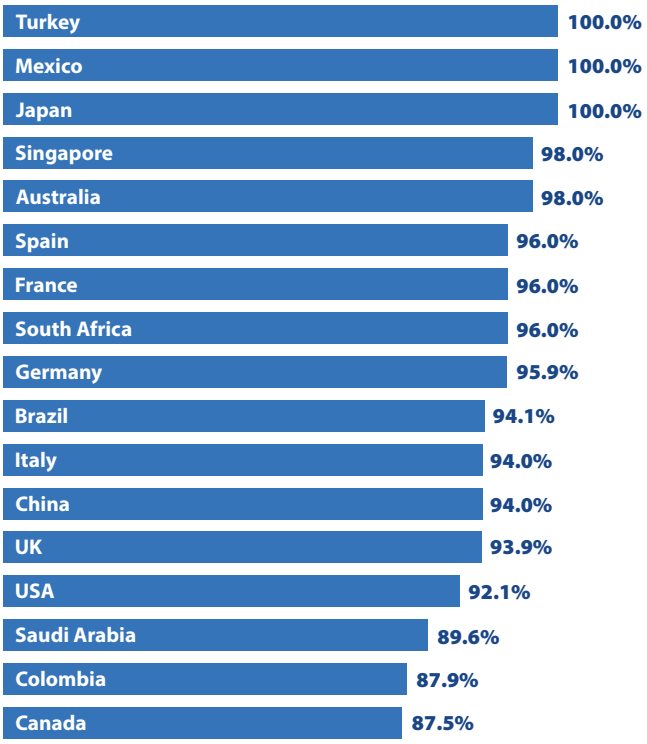

Figure 48: Organizations implementing ZTNA, by country.

We also gave respondents an option to select "We do not embrace ZTNA in our organization" (which they could only answer if they did not agree, disagree, or say that they neither agreed nor disagreed with our statement. As Figure 48 shows, there is a whole lot of embracing of zero trust (98% or more) in some countries (Turkey, Mexico, Japan, Singapore, and Australia), but not quite such universal enthusiasm (less than 90%) in a few other countries (Saudi Arabia, Colombia, and Canada).

Section 4: Practices and Strategies

Information Regularly Reported to the Board of Directors

What types of information are most important to present to your organization's board of directors on a regular basis? (Select up to five.)

Figure 49: Information most important to present regularly to the board of directors.

In previous surveys, we found that IT security leaders are interacting with members of their board of directors more often and in more ways than in the past (2023 CDR) and that more than half of boards (62.2%) have at least one member with a cybersecurity background that helps them understand security issues and educate non-technical members (2024 CDR).

This year we decided to dig deeper into what kinds of information IT security leaders are presenting to their board of directors (see Figure 49).

The type of information presented most often (selected by 42.9%) is "Overall assessment of the cybersecurity program maturity or effectiveness." This is a very business-savvy approach to communicating with boards. Not all board members can understand technical metrics or appreciate ingenious methods of discovering and remediating the latest malware. But any good manager can grasp the importance of getting better at what you're doing, and why it is important to fund cybersecurity so your program doesn't slip backward. A variety of available frameworks, maturity models, and tools for assessing the effectiveness of security programs provide scales or numerical scores to quantify current levels of effectiveness and track progress over time.

Section 4: Practices and Strategies

The second type of information on the list is "Quantified estimates of the costs of attacks (ransomware, data breaches, DDoS attacks, etc.)" (40.9%). Again, this reflects IT security leaders' recognition that they need to talk the language of business: dollars (or euros, yuan, yen, pounds, etc.). If you are going to ask for more money to fight, say, phishing attacks, you need to say what they are costing you or potentially could.

The next three types of information presented to boards are: "Assessments of the threat landscape and specific threats" (37.6%), "Progress complying with specific security and privacy standards or regulations" (35.9%), and "Measurements of employee cybersecurity training and awareness" (35.8%). These topics show that boards are receptive to information about some of the key details that cybersecurity teams deal with every day.

We were a little surprised to see "Benchmarks against peer organizations" in last place on this list (22.5%). Peer benchmarks, like program assessments, are easy to understand: "We are ahead of our peers in A, B, and C, and although still behind in D and E, we are catching up." Perhaps we will see greater use of them over time.

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.

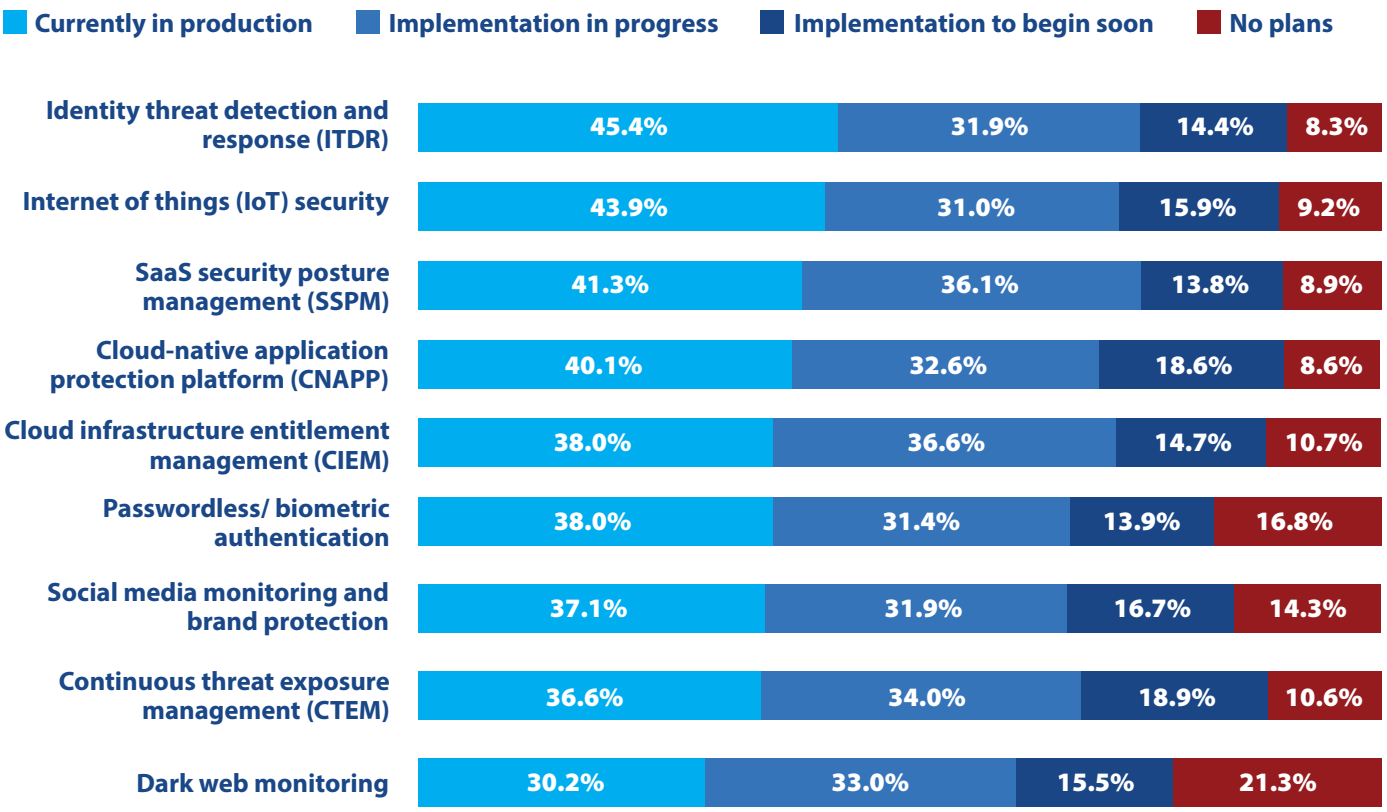

Figure 50: Plans for implementing emerging IT security technologies and architectures.

For the last several years, the final question in our survey has asked participants about plans for implementing a set of emerging technologies and architectures. Periodically we remove some entries because either (a) they are so well established that they can't be considered "emerging" anymore, or (b) they have lost momentum in the marketplace and are no longer rising stars.

Just so you know, in this report we dropped four that appeared in last year's CDR:

- Secure access service edge (SASE)
- Zero trust network access (ZTNA)
- Extended detection and response (XDR)
- Risk-based vulnerability management (RBVM)

Section 4: Practices and Strategies

And substituted these four:

- IoT security
- Social media monitoring and brand protection
- Continuous threat exposure management (CTEM)
- Dark web monitoring

Do you agree with these choices?

At the top of our list is identity threat detection and response (ITDR). Products in this area detect and help contain attacks on identity information everywhere it resides, including in enterprise directories, cloud identity stores, and applications, and on devices. It is an essential element of identity security (see page 35) and zero trust security (see page 51). ITDR is currently in production in 45.4% of organizations, and implementation is in progress in 31.9% more.

The technology in second place for deployment is Internet of Things (IoT) security. An interesting aspect of this area is that IoT security is not only about protecting IoT devices from attacks, vital as that is. It's also about protecting everything else in the computing infrastructure from attacks by IoT devices. That is, some IoT devices have lots of intelligence but weak defenses. That makes them tempting targets for threat actors who can compromise them and use them as platforms to capture data on the network or launch denial of service attacks. IoT security is active in 43.9% of organizations and being implemented in an additional 31.0%.

Our third technology is SaaS security posture management (SSPM). These solutions monitor and manage security issues in SaaS applications. They are in production in 41.3% of organizations and being deployed in an additional 36.1%.

Fourth and fifth come technologies that enhance security in cloud environments. A cloud-native application protection platform (CNAPP) monitors and protects cloud-based applications. Some also facilitate DevSecOps practices, which help organizations develop and deploy secure cloud applications. Cloud infrastructure entitlement management (CIEM) products manage identities and entitlements for cloud-based applications. CNAPP and CIEM solutions are in production in 40.1% and 38.0% of organizations and are being implemented in an additional 32.6% and 36.6%, respectively.

Passwordless authentication improves the experiences of both users and administrators and improves security by securing authentication without passwords. After all, too often passwords are captured in data breaches, guessed in brute force attacks, or stolen via phishing and social engineering. Passwordless authentication is in use in 38.0% of organizations and is being deployed in 31.4% more. Look up the FIDO Alliance if you are interested in how it works.

Social media monitoring and brand protection and dark web monitoring are ways of detecting threats outside of an organization's computing environment. They can alert cybersecurity teams to takeovers of an organization's social media accounts, look-alike websites and social media accounts used for phishing attacks and fraud, threat actors planning attacks on certain companies or industries, compromised data and credentials for sale on dark web marketplaces, and other threats that might never be detected by conventional security tools. These activities to obtain threat intelligence are in production in 37.1% and 30.2% of organizations and are being deployed in an additional 31.9% and 33.0%.

Finally, continuous threat exposure management (CTEM) is in production in 36.6% of organizations and is being implemented in an additional 34.0%. Solutions in this area provide continuous automated monitoring of attack surfaces, identify vulnerabilities and security issues, and provide data to prioritize remediation.

The Road Ahead

The AI Arms Races

There are many AI arms races going on right now. One is between technology firms striving to build and market the best AI models and platforms. Others pit companies in many industries against each other in struggles to gain advantages over competitors. Some involve scientists and other researchers employing AI so they can be the first to cure diseases and solve problems that plague humanity. There is also a literal AI arms race by governments and defense contractors to design and deploy lethal autonomous weapons systems (LAWS) – scary! And of course, we are in the midst of an arms race between cybersecurity professionals and threat actors.

Who is winning that last one? Right now, based in part on findings in our 2024 CDR, we have a sense that the good guys have been getting a little more mileage out of AI technologies than the bad guys. AI capabilities are being embedded rapidly into a wide range of security solutions. Although threat actors are also using AI technologies, so far none of the popular disaster scenarios—a deluge of undetectable, wholly persuasive phishing emails, proliferating polymorphic malware that effortlessly evades conventional defenses, hundreds of undetectable deepfake videos persuading hapless finance workers to wire money to mysterious bank accounts, thousands of deceptive social media accounts that successfully turn voters against political candidates—have materialized on a large scale.

But we are only in the first few miles of a marathon. The best we can do now is stay alert and respond quickly to new developments as they occur.

[Fill In the Blank] Security Posture Management

Have you noticed industry analysts and security product vendors promoting data security posture management (DSPM)? Application security posture management (ASPM)? Cloud security posture management (CSPM), network security posture management (NSPM), and identity security posture management (ISPM)?

Fortunately, this proliferation of terms has limits. In English we can only have 26 four-letter acronyms that end in "SPM." Speakers of Hindi and Khmer aren't so lucky: their alphabets have 50 and 74 characters, respectively.

But there is a good reason why "_____ security posture management" acronyms are popping up. They reflect the idea that each security domain has its own attack surface, and that each attack surface can be assessed, tested, hardened, and managed better. That can include:

- Scanning and testing for vulnerabilities and other security issues
- Improving administration and management processes to keep configurations, permissions, security controls, etc., up to date and functioning correctly
- Assessing and scoring risks across the domain and using the assessments and risk scores to prioritize remediation activities
- Tracking and reporting progress toward a better security posture for the domain.

You can get a flavor of this in our discussion of attack surface management challenges on pages 25 and 26.

By the way, "_____ security posture management" is not synonymous with "_____ security." The latter includes a whole bunch of detection and response activities that lie outside of posture management. You might think of the various forms of security posture management as focusing on reducing and hardening a domain's attack surface prior to attacks, while not including the parts of security that are about detecting, analyzing, and containing attacks in progress.

We don't know if the raft of __SPM acronyms will catch on, but even if the names change, we think the approach they represent will play an increasingly large part in cybersecurity programs.

The Road Ahead

Cold and Hot Cyberwars

You might have heard the expression: "Hope for the best but prepare for the worst." It sounds both practical and inspirational. But it's not easy or painless to put into practice. Preparing for the worst requires large investments in defenses to cope with extreme conditions that may never occur. That doesn't leave many resources to work toward whatever "best" conditions you hope to enjoy. In fact, most of us operate on a spectrum where we take some precautions against the worst possible conditions, but allocate most resources based on the assumptions that things will stay the same, or maybe even get better.

Very unfortunately, events related to the Russian invasion of Ukraine, global conflicts occurring now, and the potential for additional hot or cold wars between major powers, are pushing us toward the "preparing for the worst" end of the spectrum. Commercial enterprises and government agencies with no connections to the military or to defense industries could be targeted in these conflicts if they are perceived as supporting one of the belligerents, or simply to damage the productivity or morale of a nation or an interest group.

We're not saying everyone must become a doomsayer. But we think cybersecurity professionals, even those in industries that have traditionally focused on cybercrime, should be ready to analyze and prepare for some worst-case scenarios involving political or military adversaries.

The Quantum Computing Arms Race

What, another arms race? Didn't we already cover that?

Well, when quantum computing becomes commercially viable, it is going to upend everything we said earlier about the AI arms race between cybersecurity teams and threat actors. For example, quantum computers will be able to break the encryption algorithms we have relied on until now to keep communications and data secure. That includes bad guys going back and reading encrypted data obtained in earlier breaches that has been beyond their reach.

The experts predict that quantum computers will be widely available sometime between, oh, five and 50 years from now. (Really helpful, right?) You don't need to drop everything to come up with a detailed plan. But there are steps you can take now to start preparing. For example, you can investigate quantum-safe encryption algorithms that are starting to become available.

At a minimum, keep quantum computing on your radar. You'll be hearing a lot more about it over the next few years.

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 51) 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 52). This year, 39.2% of our respondents held CIO, CISO, or other IT security executive positions.

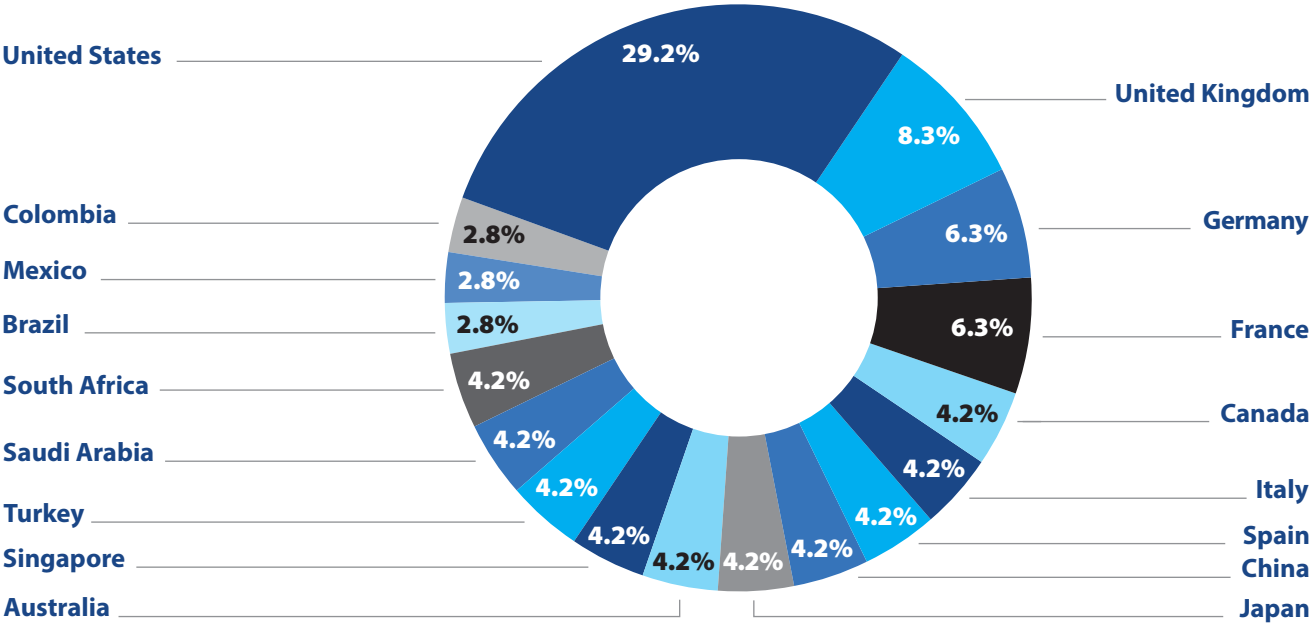

Figure 51: Survey participants by country.

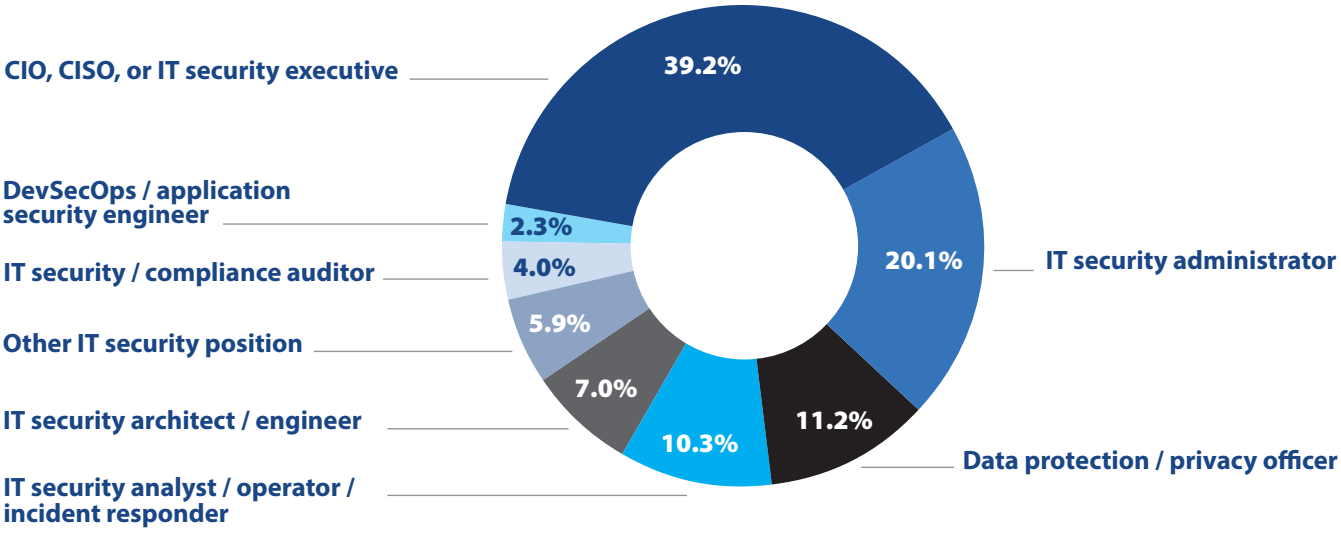

Figure 52: Survey participants by IT security role.

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 53). A total of 19 industries (plus "Other") are represented in this year's study (see Figure 54). 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 15.1% of participants.

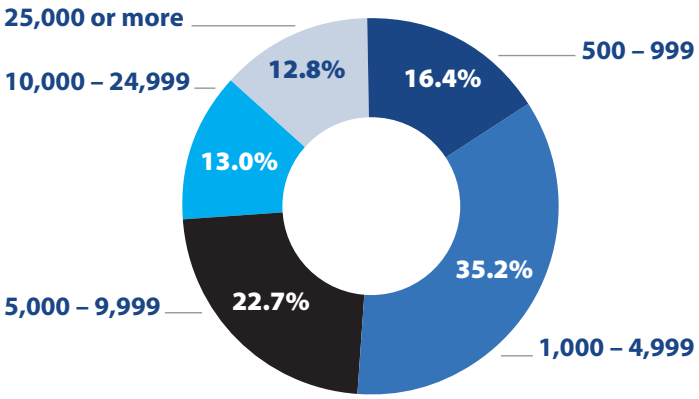

Figure 53: Survey participants by organization employee count.

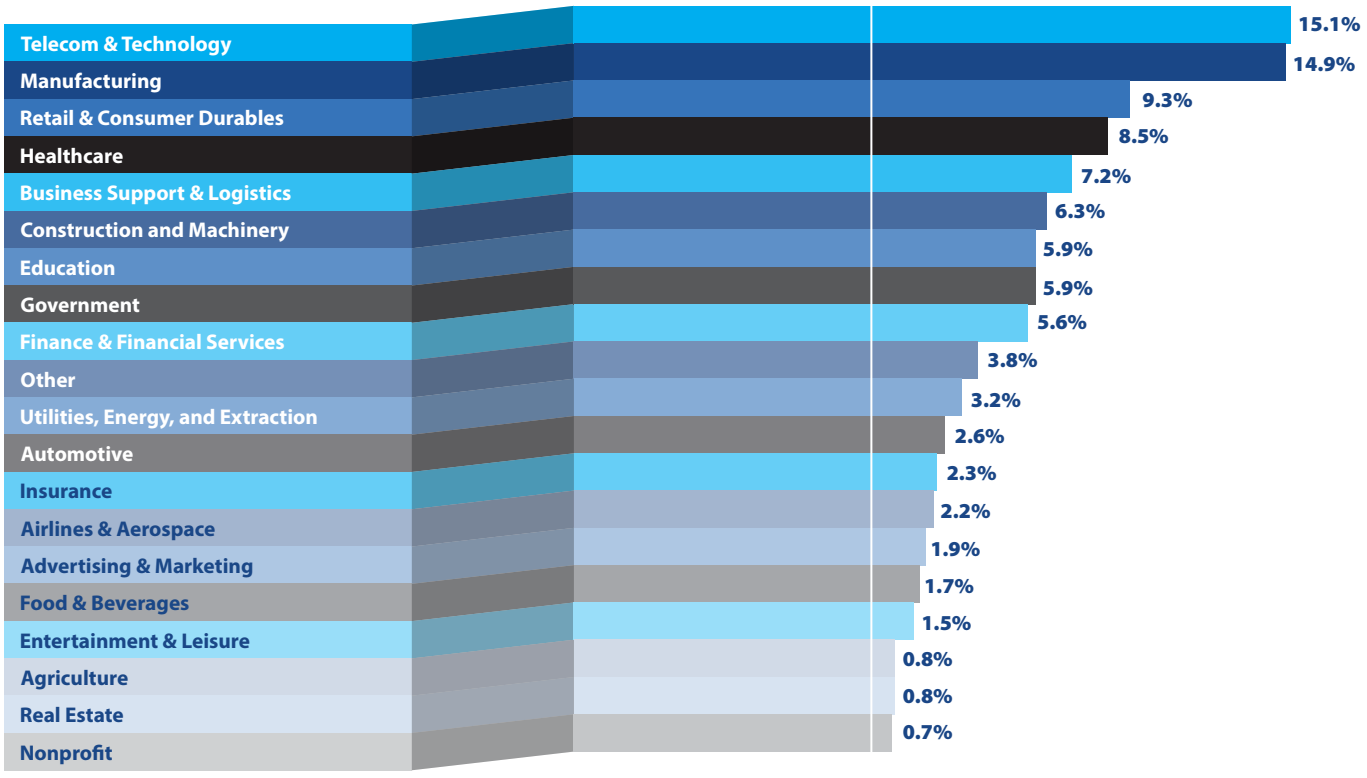

Figure 54: Survey participants by industry.

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 2024. 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, Inc. (NYSE: NET) is the leading connectivity cloud company on a mission to help build a better Internet. 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. Learn more about Cloudflare's connectivity cloud at cloudflare.com/connectivity-cloud. Learn more about the latest Internet trends and insights at radar.cloudflare.com.

Delinea | www.delinea.com

Delinea is a pioneer in securing human and machine identities through intelligent, centralized authorization, empowering organizations to seamlessly govern their interactions across the modern enterprise. Leveraging AI-powered intelligence, Delinea's leading cloud-native Identity Security Platform applies context throughout the entire identity lifecycle – across cloud and traditional infrastructure, data, SaaS applications, and AI. It is the only platform that enables you to discover all identities – including workforce, IT administrator, developers, and machines – assign appropriate access levels, detect irregularities, and respond to threats in real-time. With deployment in weeks, not months, 90% fewer resources to manage than the nearest competitor, and a guaranteed 99.99% uptime, Delinea delivers robust security and operational efficiency without compromise.

Google Cloud | cloud.google.com

Make Google part of your security team with Mandiant frontline experts, intel-driven security operations, multi-cloud risk management and secure-by-design and default platforms — supercharged by AI. Organizations can reduce digital risk and secure their AI transformation with the same cybersecurity specialists, capabilities, and secure enterprise platforms Google uses to keep more people and organizations safe online than anyone else in the world, powered by our industry-leading threat intelligence. AI enhances all of these components, enabling security teams to detect more threats, minimize toil, and take productivity to new levels.

ISC | www.isc2.org

ISC2 is the world's leading member organization for cybersecurity professionals, driven by our vision of a safe and secure cyber world. Our more than 265,000 certified members, and associates, are a force for good, safeguarding the way we live. Our award-winning certifications – including cybersecurity's premier certification, the CISSP® – enable professionals to demonstrate their knowledge, skills and abilities at every stage of their careers. Our charitable foundation, The Center for Cyber Safety and Education, helps create more access to cyber careers and educates those most vulnerable. Learn more, get involved or become an ISC2 Candidate to build your cyber career at ISC2.org.

Appendix 3: Research Sponsors

Gold Sponsors

Absolute Security | www.absolute.com

Absolute Security is partnered with more than 28 of the world's leading endpoint device manufacturers, embedded in the firmware of 600 million devices, trusted by thousands of global enterprise customers, and licensed across 16 million PC users. With the Absolute Security Cyber Resilience Platform integrated into their digital enterprise, customers ensure their mobile and hybrid workforces connect securely and seamlessly from anywhere in the world and that business operations recover quickly following cyber disruptions and attacks. Our award-winning capabilities have earned recognition and leadership status across multiple technology categories, including Zero Trust Network Access (ZTNA), Endpoint Security, Security Services Edge (SSE), Firmware-Embedded Persistence, Automated Security Control Assessment (ASCA), and Zero Trust Platforms.

HackerOne | www.hackerone.com

HackerOne is a global leader in offensive security solutions. Our HackerOne Platform combines AI with the ingenuity of the largest community of security researchers to find and fix security, privacy, and AI vulnerabilities across the software development lifecycle. The platform offers bug bounty, vulnerability disclosure, pentesting, AI red teaming, and code security. We are trusted by industry leaders like Amazon, Anthropic, Crypto.com, General Motors, GitHub, Goldman Sachs, Uber, and the U.S. Department of Defense. HackerOne was named a Best Workplace for Innovators by Fast Company in 2023 and a Most Loved Workplace for Young Professionals in 2024.

Illumio | www.illumio.com

Illumio is the world leader in ransomware and breach containment, protecting organizations from cyberattacks and enabling operational resilience without complexity. Powered by the Illumio AI Security Graph, our breach containment platform identifies and contains threats in modern hybrid multi-cloud environments before they become disasters. Named a Forrester Wave leader in microsegmentation, Illumio helps secure the operations that keep the world running — from critical infrastructure and financial systems to healthcare and beyond.

Secureworks | www.secureworks.com

Secureworks, a Sophos company, is a global cybersecurity leader that protects customer progress with Taegis, an AI-native security analytics platform built on more than 20 years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Appendix 3: Research Sponsors

Silver Sponsors

AgileBlue | www.agileblue.com

AgileBlue combines AI-powered cybersecurity with the 24/7 human touch you trust. Our SecOps platform autonomously detects, investigates, and responds to endpoints, network, and cloud cyber-attacks faster and more accurately than legacy technologies. Our platform is both intelligent and automated, but we take a custom approach for every client we work with, analyzing and detecting exactly what matters most. AgileBlue products are entirely cloud-based with advanced machine learning and user behavior analytics, all supported by our U.S.-based team of cyber experts.

Dataminr | www.dataminr.com

Adversaries strike fast—you have to be faster. Dataminr Pulse for Cyber Risk detects external cyber threats the moment they first surface. Powered by 50+ Domain-specific language models (DSLM) and a massive knowledge graph with over 1 million unique public data sources, Dataminr delivers real-time, actionable cyber insights to security teams at unprecedented speed and scale. Automate threat detection, reduce response time, and stay ahead of attacks before they escalate. Proactive security starts now—are you ready?

Intel 471 | www.intel471.com

Intel 471 empowers enterprises, government agencies, and other organizations to win the cybersecurity war using the real-time insights about adversaries, their relationships, threat patterns, and imminent attacks relevant to their businesses. The company's platform collects, interprets, structures, and validates human-led, automation-enhanced intelligence, which fuels our external attack surface and advanced behavioral threat hunting solutions. Customers utilize this operationalized intelligence to drive a proactive response to neutralize threats and mitigate risk. Organizations across the globe leverage Intel 471's world-class intelligence, our trusted practitioner engagement and enablement, and globally dispersed ground expertise as their frontline guardian against the ever-evolving landscape of cyber threats to fight the adversary — and win.

Keeper Security | www.keepersecurity.com

Keeper Security is transforming cybersecurity for millions of individuals and thousands of organizations globally. Built with end-to-end encryption, Keeper's intuitive cybersecurity platform is trusted by Fortune 100 companies to protect every user, on every device, in every location. Our patented zero-trust and zero-knowledge privileged access management solution unifies enterprise password, secrets and connections management with zero-trust network access and remote browser isolation. By combining these critical identity and access management components into a single cloud-based solution, Keeper delivers unparalleled visibility, security and control while ensuring compliance and audit requirements are met.

Media Sponsor

Security Buzz | https://securitybuzz.com/

Security Buzz is a leading cybersecurity news website. A subsidiary of CyberEdge Group, our mission is to deliver accurate, timely, and actionable information to help IT professionals and the general public navigate the complex world of cybersecurity. By offering a mix of breaking news, expert insights, and practical resources, we aim to empower our readers to make informed decisions and enhance their cyber defense strategies.

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@cyberedgegroup.com, or connect to our website at www.cyberedgegroup.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: 2025 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 www.cyberedgegroup.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@cyberedgegroup.com.