CYBEREDGE GROUP

2022 Cyberthreat Defense Report

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

<< Research Sponsors >>

PLATINUM

(ISC)² Gigamon imperva MENLO SECURITY perimeterx THREATX

GOLD

aqua Attivo NETWORKS CONNECTWISE Delinea LOOKINGGLASS Netsurion Powering Secure and Agile Networks PHISHLABS by HelpSystems

SILVER

agari by HelpSystems BINARY DEFENSE DRAWBRIDGE eclypsium netwrix SailPoint Telos

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.

Now in its ninth year, the CDR has become a staple among IT security leaders and practitioners by helping them gauge their internal practices and security investments against 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 2022

As always, our latest CDR installment yields dozens of actionable insights. But the following are the top five takeaways from this year's report:

1. **There has been no let-up in pressure on security teams.** While the number of organizations that experienced a successful cyberattack dropped a touch from 86.2% in the previous survey to 85.3% in this one, the percentage victimized by six or more attacks increased to a new record of 40.7%. And the number of respondents who think it is somewhat or very likely that their organization will be successfully attacked in the coming year reached a new record of 76.1%.

2. **The biggest security issues for many organizations are a persistent shortfall of skilled IT security personnel and low security awareness among employees.** These continue to top the list of factors that inhibit organizations from adequately defending themselves against cyberthreats (see page 24). We also see a lack of security skills across a wide range of job roles (page 15) and find user security awareness to be an area where our survey respondents doubt their organization's capabilities (page 13).

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**

3. **Among cyberthreats, ransomware and account takeover (ATO) attacks are poised to overtake malware as the #1 concern.** Malware is still perceived as the most important threat, but ATO and credential abuse attacks moved up from fourth place last year to #2 this year, and ransomware is only a tad behind. We think one or the other will take over the top spot in the next year or two (see page 17).

4. **Pressure from ransomware rachets up once again.** The percentage of organizations victimized by a ransomware attack in the past 12 months rose 2.5% to reach a new high of 71.0%. Ransom demands continued to rise, and the percentage of organizations deciding to pay jumped from 57.0% to 62.9%, also a record. The data also points to a "sweet spot" for ransomware gangs: organizations with 5,000 to 25,000 employees. These are being targeted more often than their smaller and larger counterparts because they can afford to pay high ransoms, yet disabling them does not typically disrupt local economies or shut down essential infrastructure and draw the attention of national governments and law enforcement agencies (see page 21).

5. **Security teams are getting a handle on the new norm created by COVID-19.** After scrambling to adapt to the disruptions caused by the pandemic, they are now well along in deploying and managing technologies and processes to build security into web and mobile applications, make work from home (WFH) secure, and improve the security and economics of networking with cloud-based resources (see pages 50, 52, and 54, respectively).

Introduction

Cyberwar and the Russian Invasion of Ukraine

This report is being written during the early stages of Russia's invasion of Ukraine. Obviously, our survey results don't reflect the impact of that event. However, in "The Road Ahead" section that begins on page 56, we offer some predictions about how the invasion may affect information security and the cybersecurity industry.

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 faced 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
- The investments in security technologies already made 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 data, analyses, and findings to answer 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 also 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 from us 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 all the intrepid defenders out there.

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 you begin to assess:

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

Introduction

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 cloud application security. We also look at how IT security training and professional certification can help enterprises address the serious shortfall in skilled IT security staff. These appraisals will help you think about how your organization can best improve your cyberthreat defenses going forward.

Section 3: Current and Future Investments

Your organization can ill afford to stand still when it comes to maintaining effective cyberthreat defenses. Your IT security team 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, security management and operations, and identity and access management. You will be able to compare your organization's investment decisions against the broad sample and get a sense of what "hot" technologies your 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 for tasks such as strengthening application security and protecting employees working from home.

Navigating This Report

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

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

Contact Us

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

Research Highlights

Current Security Posture

- **Six+ cyberattacks becoming common.** Last year, 85.3% of organizations experienced a successful cyberattack, while those experiencing 6+ attacks rose to a new high of 40.7% (page 7).
- **No let-up seen.** The number of respondents saying a successful attack is likely in the coming year reached a new record of 76.1% (page 9).
- **SaaS apps well protected.** Respondents have confidence in the security posture of SaaS companies, but not so much in their own mobile devices or APIs (page 11).
- **Attack surface blues?** Respondents have doubts about their organization's ability to manage attack surfaces – and about user security awareness (page 13).
- **Ongoing talent drought.** 84.1% of organizations can't find enough skilled security people. If you are one, ask for a raise (page 15)!

Perceptions and Concerns

- **New threats rising.** ATO and ransomware attacks are closing in on malware as the cyberthreats of greatest concern (page 17).
- **PII and credentials at risk.** Among web and mobile application attacks, PII harvesting and ATO are the most prevalent and concerning (page 19).
- **Good and bad news on ransomware.** Damage from ransomware continues to grow, but governments and law enforcement agencies are finally striking back (page 21).
- **People problems persist.** Yet again, the two biggest barriers to effective security are a lack of skilled personnel and employees' low security awareness (page 24).
- **Integrated defenses are good for you.** Respondents cite multiple benefits of unified app and data security defenses (page 26).
- **Hybrid cloud security challenges.** Distributing apps across data centers and cloud platforms creates significant challenges for security teams (page 28).
- **Cloud and software security education requested.** Security professionals see certifications, especially in cloud and software security, as career boosters (page 30).

Current and Future Investments

- **Security spending solid.** The percentage of overall IT budgets allocated to security held steady at a near-record 12.7% (page 32).
- **More for most.** A strong 83.2% of organizations expect to see their IT security budget grow this year (page 34).
- **Network security warhorses.** Five security technologies are currently in use in at least 55% of organizations (page 36).
- **Endpoint security basics.** Basic anti-virus is ubiquitous on endpoints, and EDR, DLP, and EPP are popular. Deception technology is an intriguing newcomer (page 38).
- **Watch those APIs!** Solutions to protect APIs are the leading application and data security technology, adopted in almost two-thirds of organizations (page 40).
- **Must manage risk.** In the area of security management, cyber risk management and reporting products are becoming essential (page 42).
- **Identities at center stage.** Last year, organizations increased their use of nine of the 10 identity and access management technologies we follow (page 44).
- **MSSPs making friends.** Because of staffing shortages, organizations are outsourcing more tasks to managed security service providers (page 46).

Practices and Strategies

- **Cloud security edging ahead.** The percentage of security applications and services delivered via the cloud rose 0.5%, to 41.1% (page 48).
- **Baking security into the app.** Organizations are embracing a range of technologies to enhance application security (page 50).
- **Safe at home.** To protect work from home, organizations rely on old standbys like anti-virus solutions and VPNs and new approaches like SASE and ZTNA (page 52).
- **Security in packets and hardware.** Organizations are rapidly deploying SD-WAN technology and hardware-based security (page 54).

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?

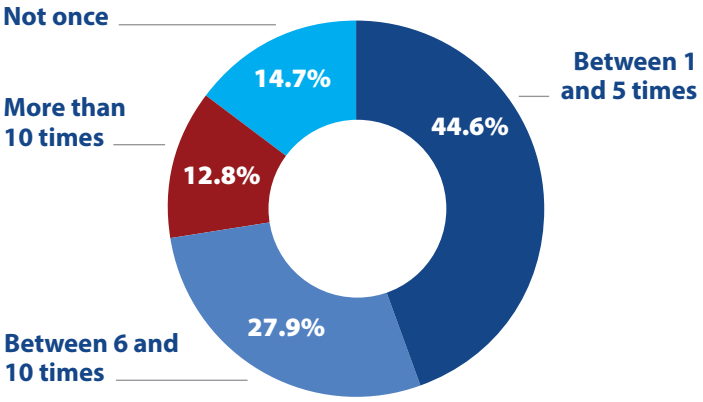

Figure 1: Frequency of successful cyberattacks in the last 12 months.

A short summary of the cybersecurity landscape over the past year: gale-force winds continue.

More than six out of seven organizations (85.3%) experienced a successful cyberattack within the last 12 months. That's down a touch from the previous year's record high of 86.2%, but still substantially larger than in any of the prior seven years of this survey. The number of organizations suffering six or more successful attacks set a new record of 40.7%. That contrasts with only 16.2% eight years ago (see Figures 1 and 2).

In the course of this report, we will explore many reasons why the pressure on IT security teams has remained so strong.

"A short summary of the cybersecurity landscape over the past year: gale-force winds continue."

It isn't a matter of money: IT security budgets have continued to grow in most places, albeit at a slightly slower rate than in previous years (page 24). In fact, lack of budget ranks near the bottom of the list of factors that inhibit security teams from adequately defending against cyberthreats (page 24).

However, the typical organization's attack surface continues to expand, driven primarily by the effects of the COVID-19 pandemic. Security teams must work hard to protect more employees working from home (page 52), protect more software in hybrid cloud environments (page 28), and build better security into web and mobile applications (page 19). At the same time, security teams are facing insidious new threats. Two of the

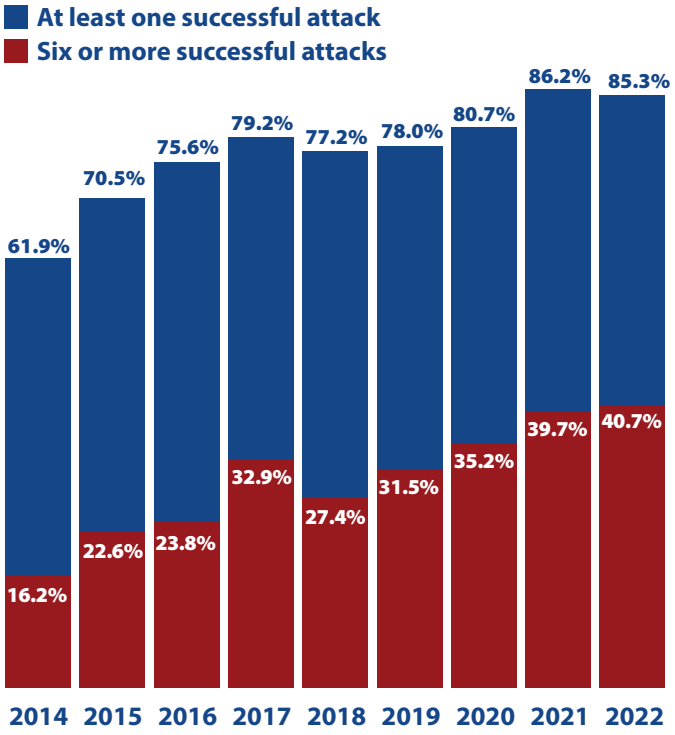

Figure 2: Percentages compromised by at least one successful attack and by six or more successful attacks.

Section 1: Current Security Posture

blockbuster issues of the past year have been the increasing popularity (for cybercriminals) of double extortion ransomware, which not only encrypts data but also exfiltrates it to the web (where it can be published), and vulnerabilities in the Log4j utility from Apache, which could potentially affect 3 billion devices and applications.

And the pressure can't be relieved by hiring, since the vast majority (84.1%) of organizations are already experiencing a shortfall in IT security personnel (page 15).

But don't give up hope. We will also review the technologies that organizations are planning to implement in areas such as network, endpoint, application, and identity security (pages 36-45) and how organizations can use security training and certifications to move junior security professionals into more-advanced roles (page 30).

Now, back to our data about successful cyberattacks in the past year.

Of the seven major industries surveyed for this report, education was the most often victimized for the second year in a row (90.5%), followed closely by telecom and technology (90.3%).

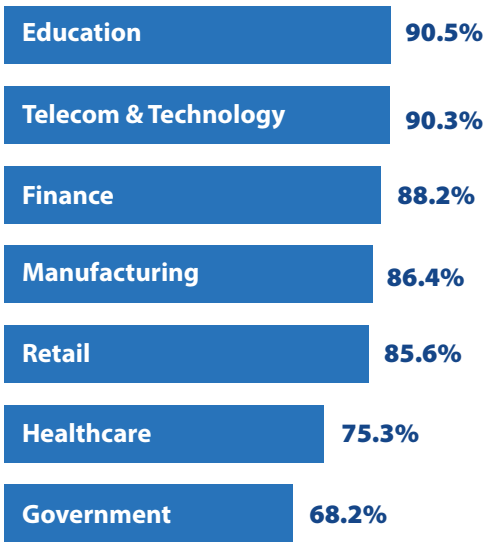

Figure 3: Percentage compromised by at least one successful attack in the past 12 months, by industry.

Not far behind were finance (88.2%), manufacturing (86.4%), and retail (85.6%). Healthcare (75.3%) and government (68.2%) were affected somewhat less often (see Figure 3).

Looking globally, the countries with the highest percentage of organizations successfully attacked were Colombia (93.9%), Turkey (93.7%), Spain (91.8%), Mexico (90.6%), Canada (89.8%), and France (89.3%). The UK, Germany, and Australia were at the other end of the spectrum, with 81.4%, 72.6%, and 62.5% of their organizations being compromised, respectively (see Figure 4). Maybe the Aussies know something. Not only was Australia the only country where less than 70% of organizations were breached at least once, but only 20.9% of the organizations there reported six or more successful attacks, about half of the international average.

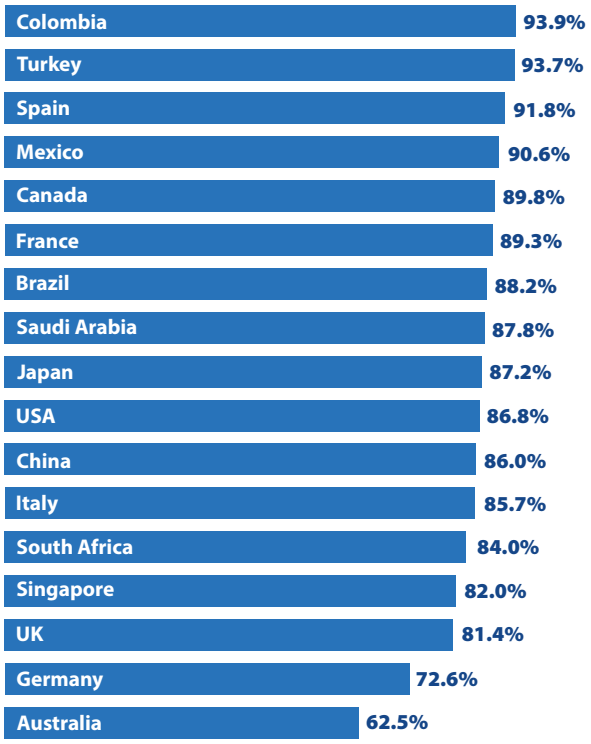

Figure 4: Percentage compromised by at least one successful attack in the past 12 months, by country.

Section 1: Current Security Posture

Future Likelihood of Successful Cyberattacks

What is the likelihood that your organization's network will become compromised by a successful cyberattack in 2022?

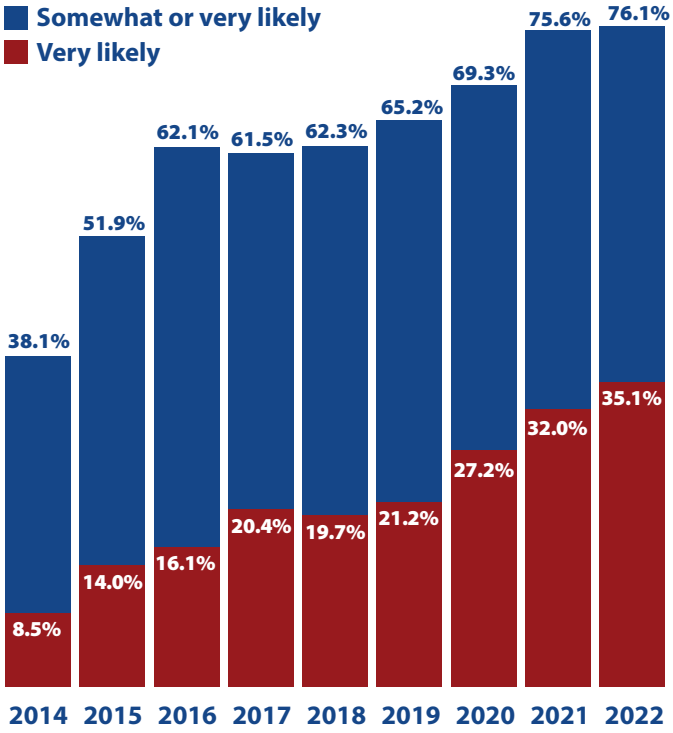

Figure 5: Percentage indicating compromise is "more likely to occur than not" in the next 12 months.

Expectations about successful cyberattacks over the coming 12 months reached a new high in this year's survey. The number of respondents indicating that such an attack was either "somewhat likely" or "very likely" edged up from 75.6% to 76.1%. In addition, the mix between those two views shifted for the worse. The percentage saying a successful attack was "very likely" jumped by 3.1%, to 35.1%. That is four times the number (8.5%) who gave that response eight years ago when this survey started (see Figure 5).

The best we can say is that the rate of increase in the combined total has slowed to half a percentage point in this survey, after having jumped 2.9%, 4.1%, and 6.3% in the 2019, 2020, and 2021 CDRs, respectively. We think the curve has flattened because organizations have spent the last two years putting in place infrastructure and processes to protect remote operations, home-based workers, and personal devices (i.e., devices not managed by the IT department). Examples of such measures include bring-your-own-device (BYOD) policies and zero trust network access (ZTNA) approaches to network and application access (see pages 52 and 54). Those investments are giving security teams greater confidence in their ability to manage the challenges created by the COVID-19 pandemic.

It is interesting to note that the 76.1% of respondents indicating that a successful attack is somewhat or very likely in the coming 12 months is less than the 85.3% who experienced such an attack in the past year. In other words, at least some security professionals who were victimized last year think their organizations are better able to defend themselves this year. Or else they are just optimistic. A positive attitude is healthy, when not taken to extremes. Perhaps we should all follow the example of Benjamin Disraeli, the 19th century British prime minister, who said: "I am prepared for the worst, but hope for the best."

"Perhaps we should all follow the example of Benjamin Disraeli, the 19th century British prime minister, who said: 'I am prepared for the worst, but hope for the best.'"

Section 1: Current Security Posture

When we look at expectations by country, the highest number of respondents predicting successful cyberattacks were in Japan (87.9%), Canada (85.4%), and Singapore (84.0%). In the middle of the pack: the United States (79.7%), Spain (76.0%), and Germany (74.3%). The optimists were Colombia (60.7%), Brazil (55.9%), and Turkey (a mere 38.0%) (see Figure 6).

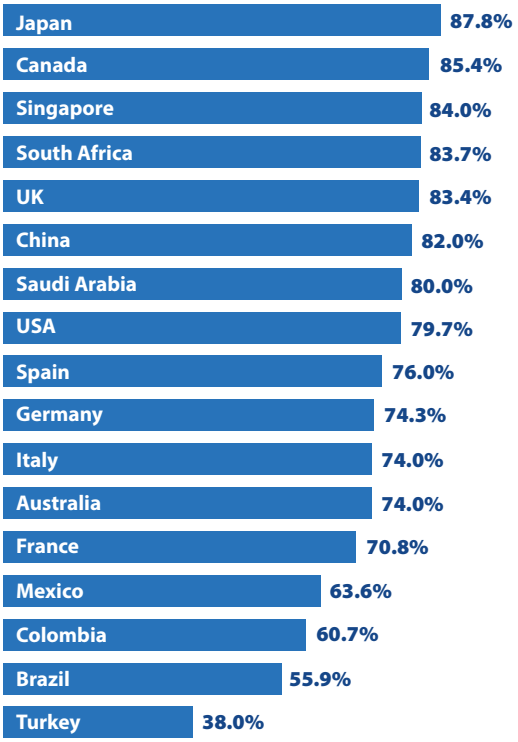

Figure 6: Percentage indicating compromise is "more likely to occur than not" in the next 12 months, by country.

By industry, respondents from finance are expecting the worst (86.7%), followed by those in education (84.1%), telecom and technology (79.1%), and healthcare (76.0%). Those in retail (70.4%) and manufacturing (68.9%) were more sanguine. And as on the previous question, security professionals in the government sector (54.3%) were least worried (see Figure 7).

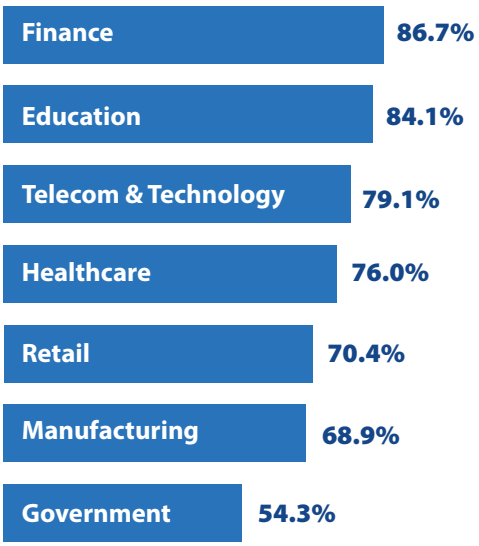

Figure 7: Percentage indicating compromise is "more likely to occur than not" in the next 12 months, by industry.

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:

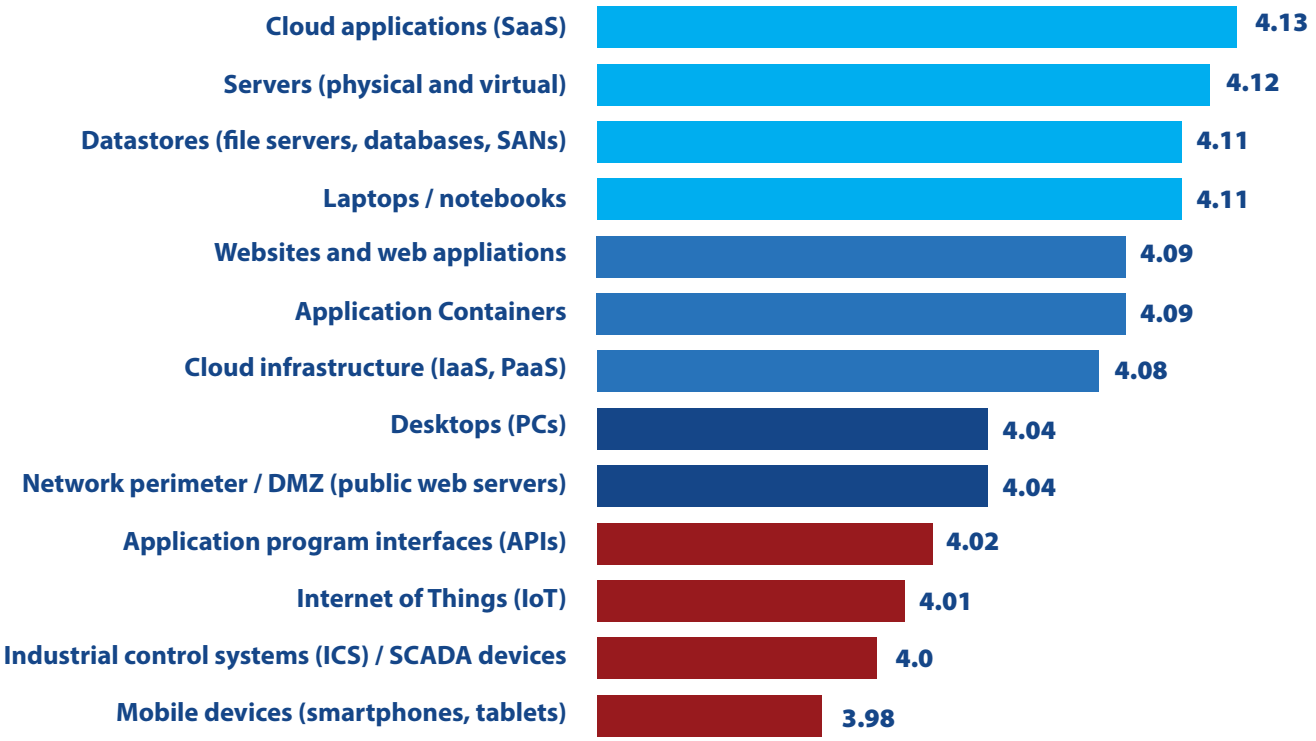

Figure 8: Perceived security posture by IT domain.

Each year we try to gauge how security professionals feel about their ability to defend against cyberthreats across different types of systems, technologies, and environments. This information gives us a picture of the IT domains where they are most confident, and those that are creating the most headaches (see Figure 8).

This year respondents chose software as a service (SaaS) cloud applications as the area where they are most comfortable about their organization's security posture. SaaS moved up from third position in the previous two surveys. Clearly, SaaS vendors have done a good job of staying on top of security issues (or at least are perceived that way by their customers).

Section 1: Current Security Posture

Respondents are also confident about physical and virtual servers, as well as datastores such as file servers, databases, and SANs. These are always at or near the top of the list because they are mostly located in data centers under the direct observation and control of operations and security staffs.

Laptops and notebooks joined the top tier, in fourth position, moving up from eighth in the previous survey. In fact, this area had the largest year-to-year increase in security posture ratings, from 4.01 last time (on a scale of 1 to 5) to 4.11 in this one. We believe this reflects all the attention and effort over the past two years that has gone into better protection for remote and home workers in response to COVID-19. On page 52 we discuss technologies and architectures that are enabling employees to securely work from home.

The IT domain that most concerns respondents is mobile devices such as smartphones and tablets. A big part of the problem is that COVID has increased the business use of mobile devices owned by employees. These cannot easily be updated, locked down, or even monitored by their employers, and are therefore less defended and more vulnerable to attacks. A multi-sponsor survey report published by CyberEdge in 2020, "The Impact of COVID-19 on Enterprise IT Security Teams Report," showed a nearly 60% leap in the number of organizations implementing BYOD policies in response to the new pandemic reality. Clearly, IT security teams continue to be nervous about securing employee-owned mobile devices.

The next two greatest areas of concern are "manufacturing and operational technology (OT)," which includes categories such as industrial control system (ICS) and supervisory control and data acquisition (SCADA) systems, and devices that make up the emerging internet of things (IoT). These are areas with large numbers of devices that were never designed with security in mind. They are also being targeted by state-sponsored and criminal hacking groups, with a few well-publicized incidents related to international conflicts and blackmail.

"Laptops and notebooks joined the top tier, in fourth position, moving up from eighth in the previous survey… We believe this reflects the attention and effort over the past two years that has gone into better protection for remote and home workers."

Application programming interfaces (APIs), which were in the middle of the pack last year, have now emerged as fourth-highest area of concern. As organizations move to modular services-based cloud applications, APIs become more tempting targets for threat actors. Protecting APIs is likely to become an even bigger issue over the next few years. We will have more to say about this later in this report (pages 40 and 59).

One final observation: the security posture ratings increased from last year in every single category. This fact shows that organizations are feeling a little bit better about the defenses they have in place to stop cyberthreats. Perhaps this is an early sign that security teams are finally catching up with threat actors in their ongoing arms race.

Section 1: Current Security Posture

Assessing IT Security Functions

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

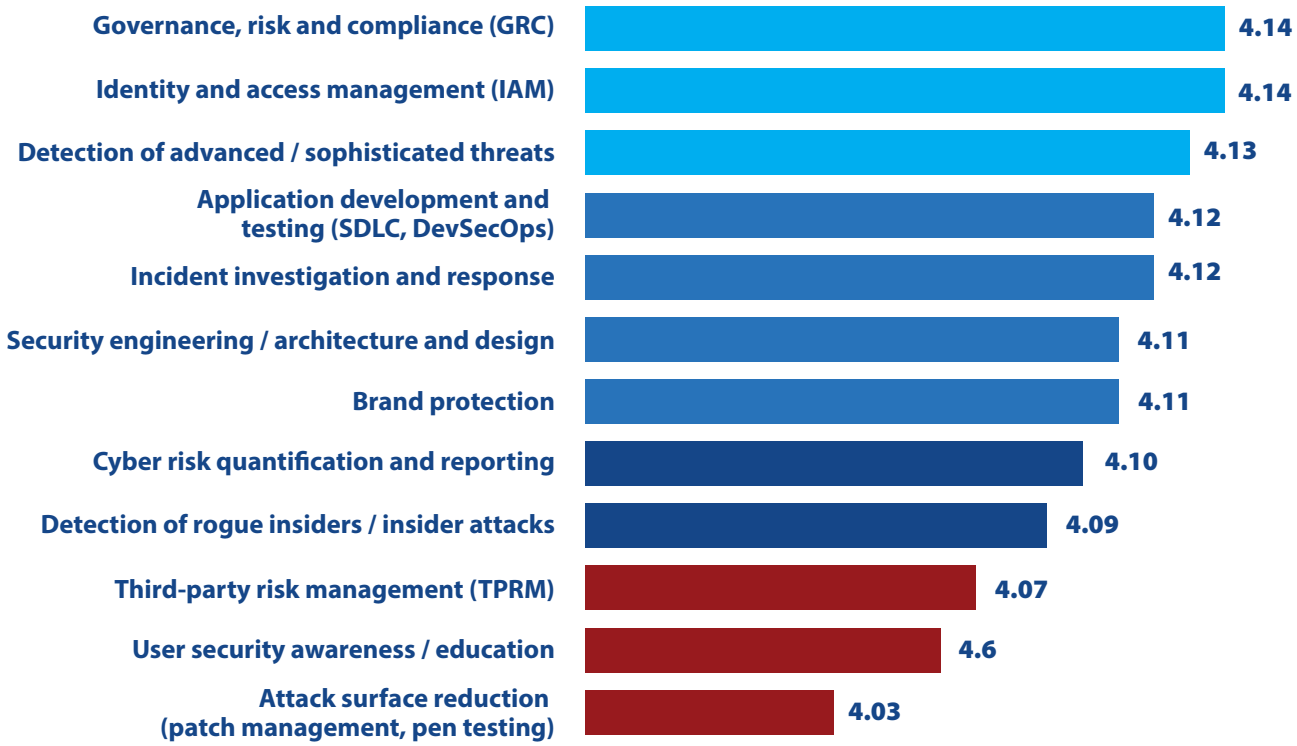

Figure 9: Perceived adequacy of functional security capabilities.

This question asks respondents to rate the adequacy of their organization's capabilities in different functional areas of IT security. The answers show us perceived strengths and weaknesses in security-related processes and programs (see Figure 9).

Organizations remain most positive about their capabilities for governance, risk and compliance (GRC) and identity and access management (IAM). These are followed closely by detection of advanced threats and application development and testing, two areas where many organizations have made considerable investments in the past couple of years.

Section 1: Current Security Posture

However, respondents were somewhat less upbeat about their organization's processes for security engineering, architecture, and design. That function was at the top of the list in the previous survey, but fell to sixth place in this one.

The area of greatest concern is attack surface reduction, which includes disciplines such as patch management, vulnerability management, penetration testing, and security configuration management. Attack surfaces have been expanding as workers use more mobile and personal devices in less-protected settings, and access applications hosted in a greater variety of cloud environments. Finding and fixing vulnerabilities across all these areas will be a growing challenge for the foreseeable future.

User security awareness and education is another significant challenge. Threat actors continue to develop ingenious phishing and social engineering campaigns to acquire valid credentials, plant malware, and otherwise leverage human weaknesses to further their malicious activities. As we will see on page 24, low security awareness among employees is now the second-most serious barrier to establishing effective defenses against cyberthreats (after a lack of skilled security personnel).

Another problematic functional area is third-party risk management (TPRM). It is very difficult to monitor, much less improve, the security practices of suppliers and other third parties that have access to an organization's applications and data. The press continues to report major data breaches that originate from credentials and PII captured from third parties and from vulnerabilities and misconfiguration in vendors' software and systems.

"The area of greatest concern is attack surface reduction... Attack surfaces have been expanding... Finding and fixing vulnerabilities across all these areas will continue to be a growing challenge for the foreseeable future."

We introduced a new functional area in this year's survey: cyber risk quantification and reporting. We see many organizations devoting more time and resources to these activities recently. This trend is driven in a large part by the need to justify security investments to top executives and boards of directors, and to show progress toward security program goals. The data shows this area falling in the middle range as far as adequacy of capabilities.

We should note that our survey was conducted in November 2021, just before the Log4j security vulnerabilities came to light. Undoubtedly, concerns about functions like attack surface reduction and application testing have intensified considerably since then.

Section 1: Current Security Posture

The IT Security Skills Shortage

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

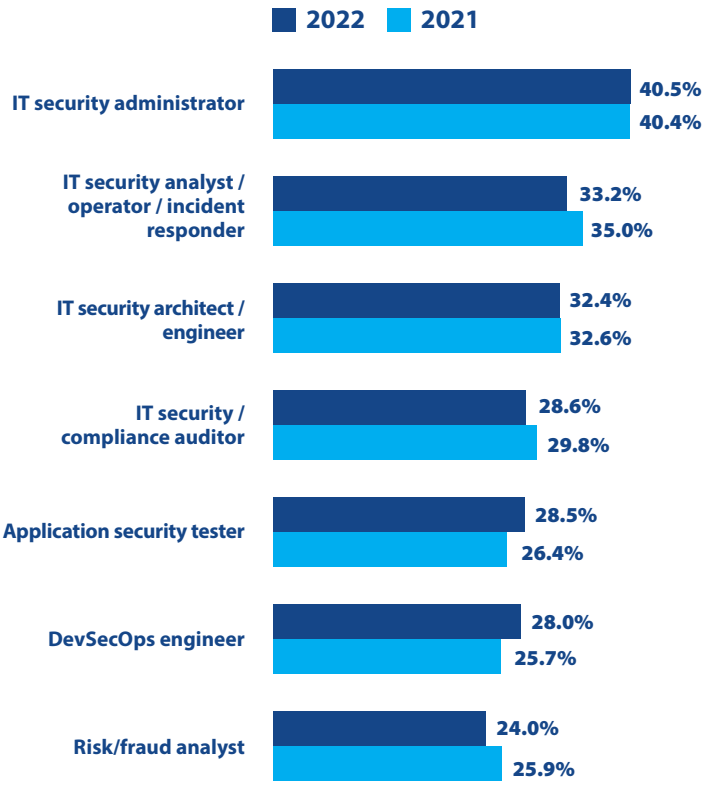

Figure 10: Cybersecurity skills shortage, by role.

A shortage of experienced IT security personnel has been a serious problem for the great majority of organizations for at least the past five years. As shown on page 24, it is the single most serious barrier to establishing effective defenses against cyberthreats.

Just like last year, the greatest unfilled demand is for security administrators, who have the critical job of installing, configuring, and maintaining security tools and infrastructure. Four out of 10 organizations (40.1%) can't find enough (see Figure 10).

One in three organizations can't find enough IT security analysts, operators, or incident responders (33.2%). The shortfall was slightly less than in the previous survey, when it was 35.0%. Almost one-third of organizations are short of IT security architects and engineers (32.4%), essentially the same as a year ago.

Rounding out the roles were application security testers (28.5%), DevSecOps engineers (28.0%), and risk and fraud analysts (24.0%). The deficit of application security testers and DevSecOps engineers worsened from the previous survey, probably the result of a turn toward building security into applications rather than relying entirely on perimeter defenses.

Section 1: Current Security Posture

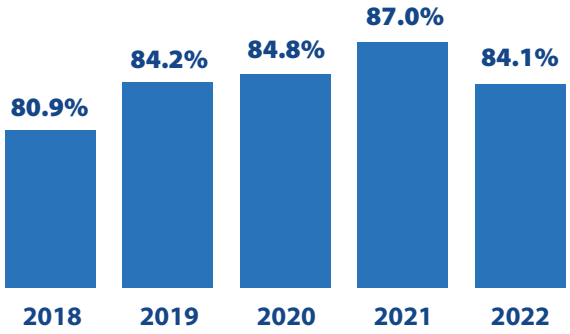

Figure 11: Percent of organizations experiencing a shortfall of skilled IT security personnel.

Figure 11 shows the percentage of organizations suffering from a shortfall of skilled IT security personnel in at least one role over the last five years. The trend is clearly upward, although surprisingly, the percentage fell somewhat in this survey, from 87.0% to 84.1%. However, that lower number is comparable to the percentages in the two previous years, and still represents more than five out of six organizations. Also, in some countries 90% or more of organizations couldn't fill jobs in at least one category: South Africa (90%), Colombia (90.9%), China (93.9%), Singapore (94.0%), and Japan (100% !!!).

One explanation for this year's leveling off is that more organizations are turning to managed security services providers (MSSPs) to outsource one or more security tasks. Statistics about the usage of MSSPs are shown on page 46.

Of the major industries, the highest percentage of organizations with staffing issues were in education (91.1%), healthcare (88.0%), retail (86.7%), finance (86.7%), and telecom and technology (85.4%). Government (81.6%) and manufacturing (78.7%) are in slightly less dire straits (see Figure 12).

"Surprisingly, the percentage [experiencing a shortfall] fell somewhat... However, that lower number still represents more than five out of six organizations."

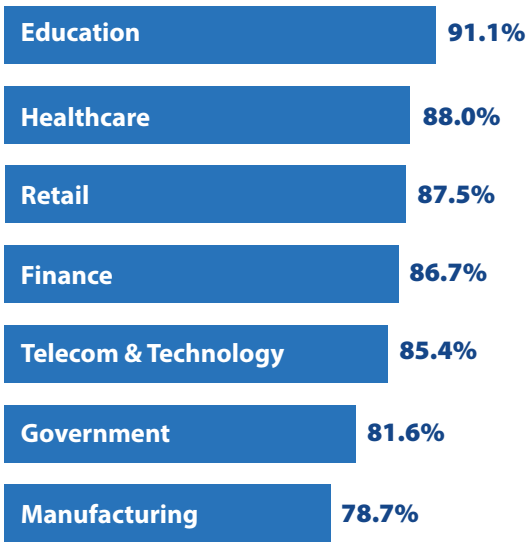

Figure 12: Percentage of organizations experiencing a shortfall of skilled IT security personnel, by industry.

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.

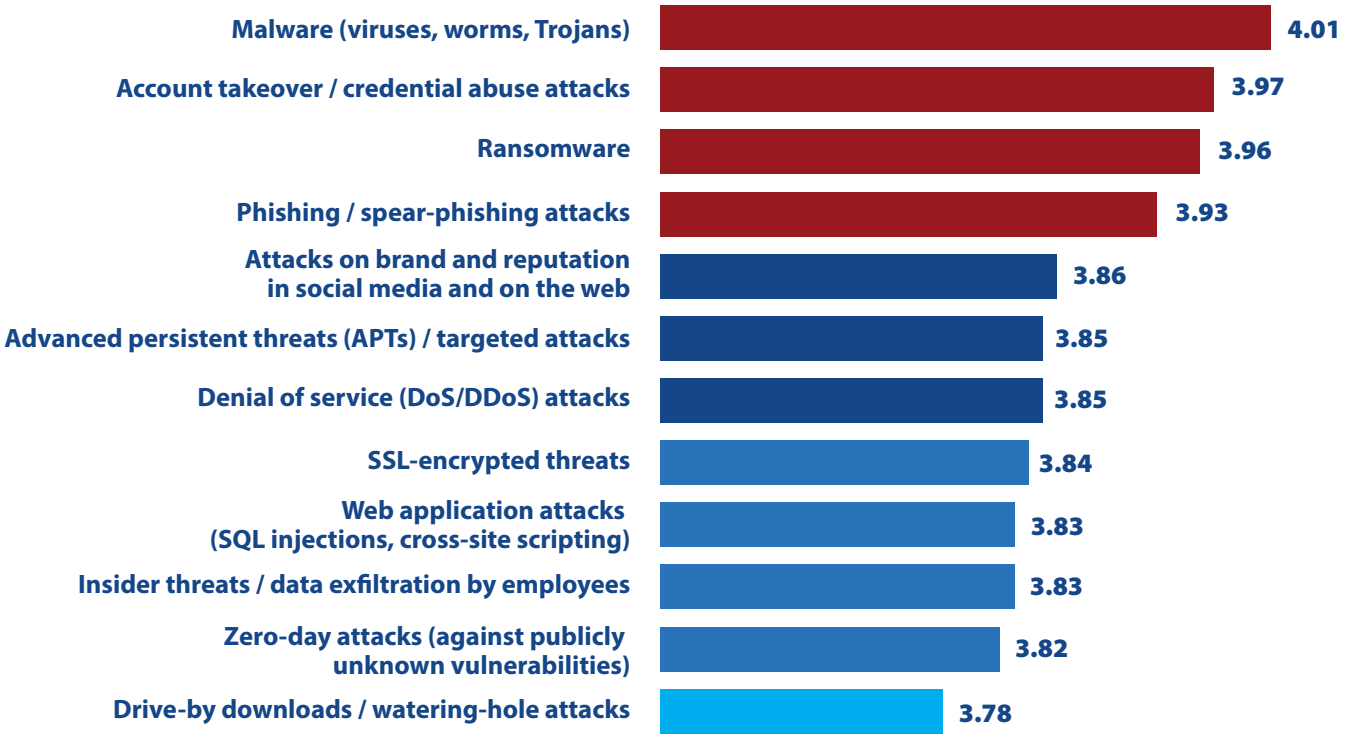

Figure 13: Relative concern for cyberthreats, by type.

What types of threats are keeping security professionals up at night? For the seventh year in a row, malware tops the list (see Figure 13). That's not remarkable, since malware is a key component of most digital skimming, ransomware, phishing, and targeted attacks, among others, and threat actors continue to come up with new techniques that allow malware to evade detection.

The surprise in this data is that account takeover (ATO) and credential abuse attacks (which include credential stuffing) moved up from fourth place last year to second place in this survey, slightly ahead of ransomware (!) and just behind malware. In fact, the average concern rating for this type of attack increased the most of any of the 12 categories on this list, rising .08 from 3.89 to 3.97 (on a scale of 1 to 5). The increase was driven by an upsurge in concern among finance and financial services companies, and to a lesser extent among manufacturing and telecom and technology companies.

Section 2: Perceptions and Concerns

Of course, ransomware is also near the top of the list, in third position and just a tad behind ATO attacks. The average concern rating for ransomware increased .04 from last year, also a pretty big one-year jump. Clearly this was fueled by increased coverage of ransomware attacks in the press (e.g., Colonial Pipeline), demands for larger ransom payments, and the emergence of "double extortion ransomware attacks" (see page 21).

In fact, based on current trends, we expect the level of concern about account takeover and ransomware attacks to pull even with or pass malware on this list in the next year or two.

We also want to note the rising anxiety about attacks on brand and reputation in social media and on the web. The concern rating for that category rose .07, the second-largest increase this year, lifting it from 11th to 5th position on the list. We believe the increase is due both to more activity by threat actors (such as typosquatting and hijacking social media accounts) and the recognition that this issue belongs to IT security teams as well as marketing and social media groups within the enterprise.

"Based on current trends, we expect the level of concern about account takeover and ransomware attacks to pull even or pass malware on this list in the next year or two."

Respondents were least concerned about zero-day attacks, drive-by downloads, and watering hole attacks. However, as we mentioned earlier, the survey was conducted before the Log4j story broke. As a result of that vulnerability, zero-day attacks may move up a bit in next year's report.

Every year we average the ratings across all categories to create a "Threat Concern Index" (see Figure 14). That index remains at a record high of 3.88. As we mentioned earlier, gale-force winds continue to blow in the world of cybersecurity.

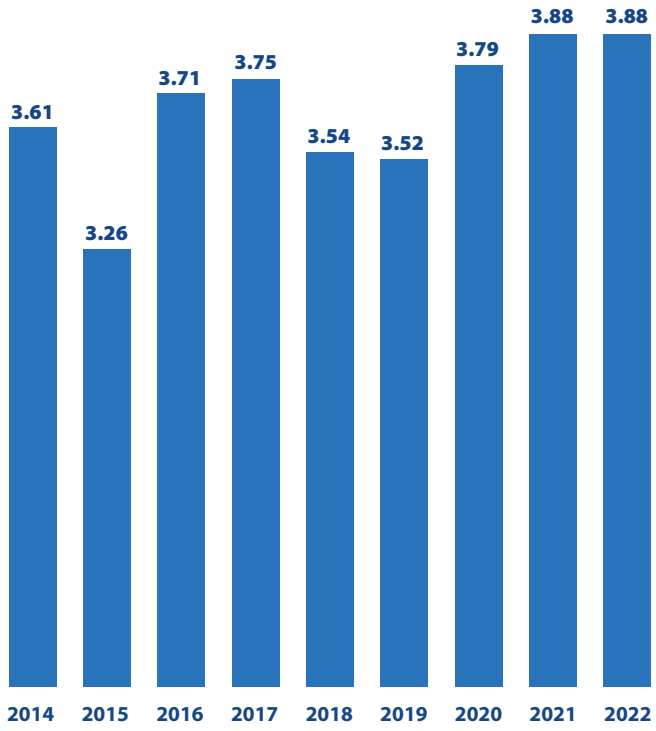

Figure 14: Threat Concern Index, depicting overall concern for cyberthreats.

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.)

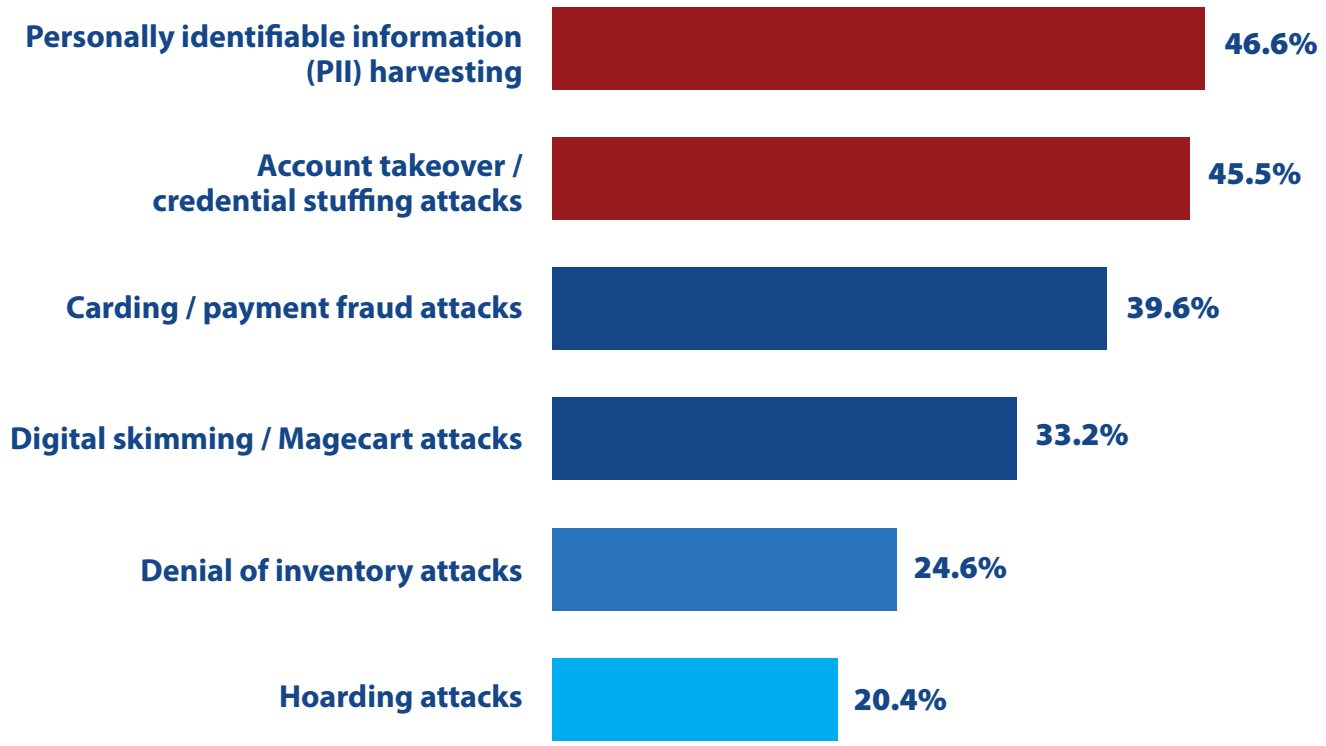

Figure 15: Most-concerning web and mobile application attacks.

In this question we drill down into worries about threats to web and mobile applications. From a list of six types of web and mobile application attacks, we asked respondents to select up to three that concern them the most (see Figure 15).

The percentage of concerned respondents increased in all four of the categories that were repeated from last year (the top four shown in Figure 15). Why? The number of work-from-home employees continues to rise, as well as the number of study-at-home students, creating more targets for cybercriminals and more incentives to perfect their tactics, techniques, and procedures.

"The number of work-from-home employees continues to rise... creating more targets for cybercriminals and more incentives to perfect their tactics, techniques, and procedures."

Section 2: Perceptions and Concerns

This year, harvesting of personally identifiable information (PII) rose to the top of the list, edging out ATO and credential stuffing attacks. The number of respondents concerned about these attacks jumped almost 7% percent from last year, from 39.7% to 46.6%. PII harvesting often involves hiding code in JavaScript that captures financial and personal data, including credentials from forms on users' browsers. The data and credentials are sent to a server controlled by threat actors, who can use them to access user accounts, strengthen phishing attacks, steal identities, and perform other malicious activities. In our survey, more than half of all respondents in education, aerospace and defense, finance, entertainment, and healthcare were particularly worried about PII harvesting.

The share of organizations concerned about ATO and credential stuffing attacks also increased from the previous survey, from 43.7% to 45.5%. Next in line are carding and payment fraud attacks (39.6%) and digital skimming and Magecart attacks (33.2%). Less common, but still affecting a significant number of organizations, are denial of inventory attacks (24.6%) and hoarding attacks (20.4%).

The vast majority of organizations in this survey are concerned about attacks on web and mobile applications. Nine out of 10 respondents (90.3%) indicated concerns about one or more of the attacks on the list (see Figure 16).

The numbers were particularly high in Spain (98.0%), China (also 98.0%), and Japan (95.6%) (see Figure 17). The lowest levels of concern (that is, relatively lowest, although still very high) were reported in the United States (87.6%), Germany (86.3%), and Australia (84.8%).

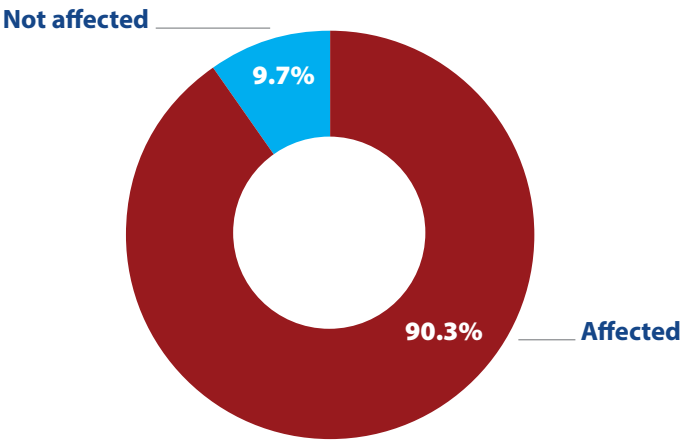

Figure 16: Organizations affected by a web or mobile application attack.

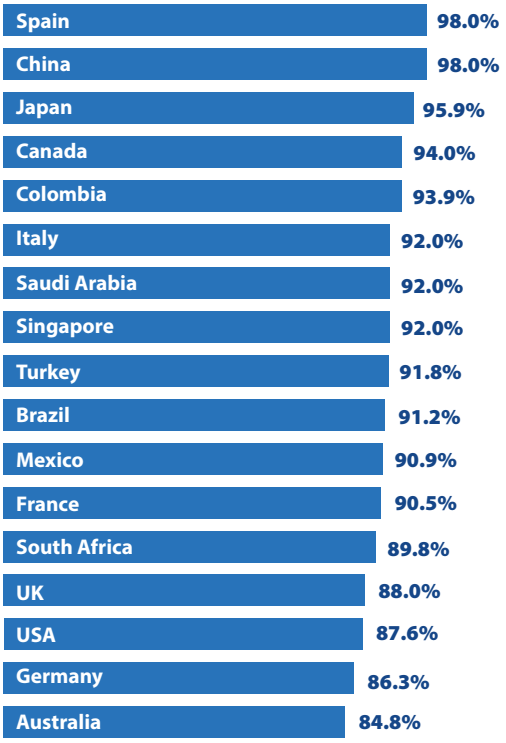

Figure 17: Organizations affected by a web or mobile application attack, by country.

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?

2021 saw a lot of big developments in the ransomware industry (and yes, today ransomware is an industry, with hundreds of millions of dollars in revenue and large, highly structured organizations). Some of the more noteworthy:

- Very high-visibility attacks affected hundreds or thousands of people, including attacks on the Colonial Pipeline (which cut off fuel delivery to 10,000 gas stations in the eastern United States), the giant meatpacker JBS (which created shortages of meat products in several US states), and Ireland's Health Service Executive (which disrupted healthcare services across Ireland).
- "Double extortion" ransomware attacks emerged as a major threat type; now ransomware gangs exfiltrate a copy of data before encrypting it, then threaten victims with exposure of sensitive information as well as data loss.
- The average size of ransomware payments increased significantly.
- National governments and international agencies finally started to crack down on major ransomware gangs (notably Russia's takedown of the REvil organization) and to push government and commercial organizations to harden their environments, disclose more information about attacks, and work closely with law enforcement groups.

What data do we have about ransomware attacks?

The percentage of companies victimized by a ransomware attack in the past 12 months set a new record (see Figure 18). That figure rose from 55.1% in our 2018 report, to 62.4% two years ago, to 68.5% last year, to 71.0% now. Threat actors continue to expand their activities, and no wonder: for most of them ransomware campaigns represent "easy money," with rising revenue from each attack (see Figure 19) and little chance of punishment. In addition, more bad actors can participate by leveraging the growing number of "ransomware-as-a-service" businesses that provide infrastructure to launch and manage ransomware attacks.

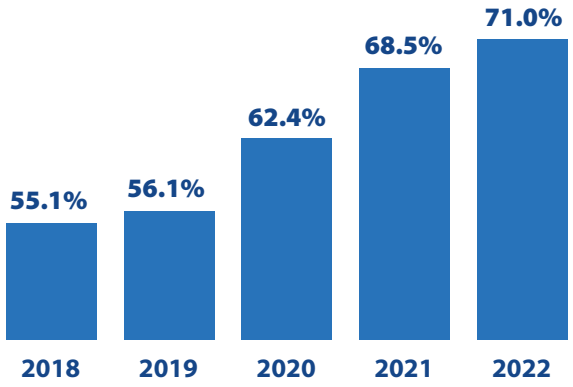

Figure 18: Percentage of organizations affected by ransomware.

The percentage of organizations that paid ransoms also increased substantially, from 57.0% in our last survey to 62.9% now (see the middle section of Figure 20). This rise reflects several trends, including added pressure from data exfiltration and the threat of data exposure.

Another factor is a cycle we have described in previous reports: ransomware gangs have noted that when they are conscientious about helping victims recover their data, other victims are more likely to pay ransoms, which increases the profits of the gangs and creates a greater incentive to launch more campaigns. Our data shows this cycle in action (see Figure 20). Over the past two years the percentage of ransom payers who recovered their data rose 3.4% from 68.8% to 72.2%, creating a tendency for more victimized companies to pay ransoms, up 5.4% over two years, and leading to more attacks, up 8.6% during the same period.

Section 2: Perceptions and Concerns

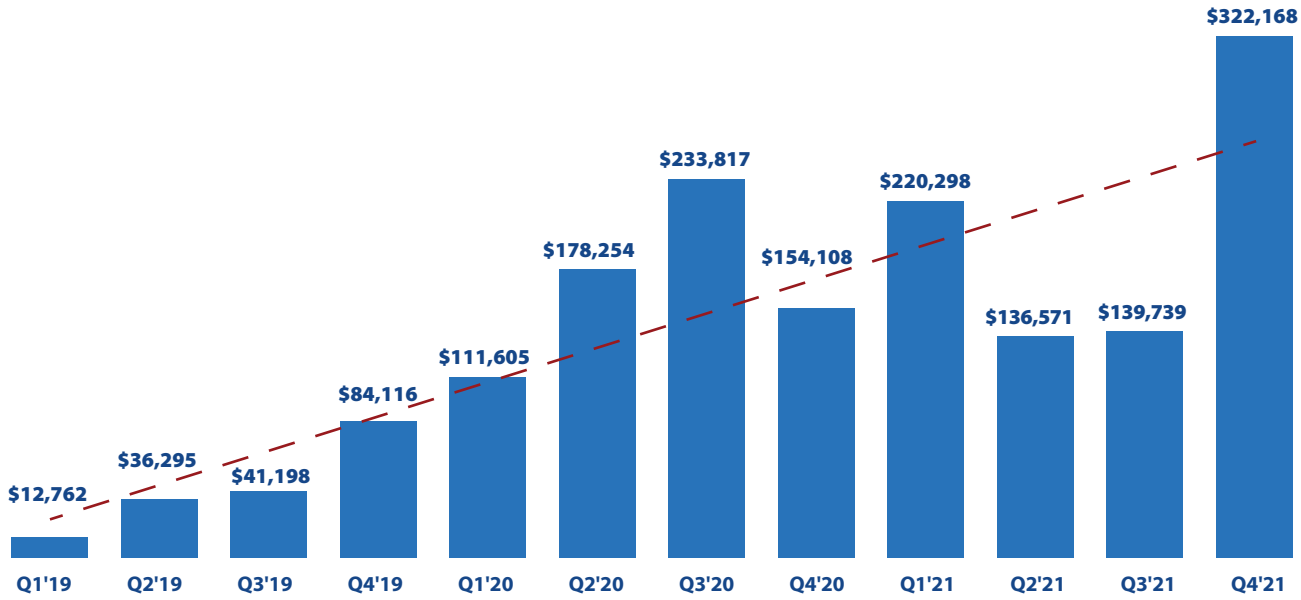

Figure 19: Average ransom payments, by quarter (data source: Coveware Quarterly Ransomware Reports).

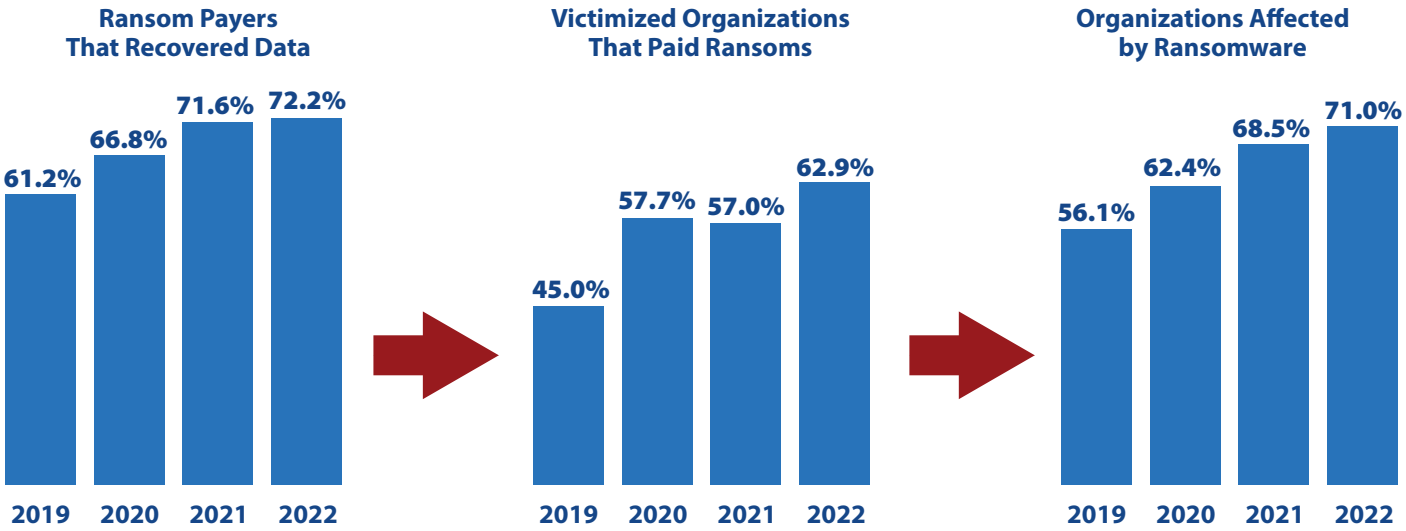

Figure 20: The ransomware vicious cycle: increased odds of recovering data … entice more victims to pay ransoms … which motivates more ransomware attacks.

Figure 21 provides more evidence that ransomware gangs operate like profit-maximizing businesspeople who rationally assess opportunities and risks. Our data shows that medium-large and large organizations, with 5,000-9,999 and 10,000-24,999 employees, respectively, are most likely to be victimized by ransomware (73.5% and 74.7%, respectively).

Section 2: Perceptions and Concerns

Why would these entities be targeted more often than organizations with 500-999 employees, victimized at a rate of 70.4%, and those with 1,000-4,999 workers, of which 69.6% were hit? Because the medium and large organizations can afford to pay higher ransoms. But then why would enterprises with more than 25,000 employees, which presumably could afford the largest payments, be victimized at the (relatively) low rate of 67.0%? As the ransomware gangs acknowledged publicly, taking out a big piece of someone's economy or shutting down essential infrastructure is bad for business because it attracts too much attention from national governments and law enforcement agencies.

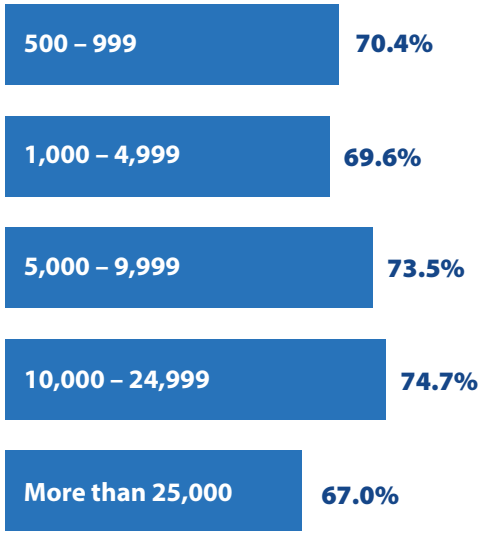

Figure 21: Percentage of organizations affected by ransomware in the last 12 months, by employee count.

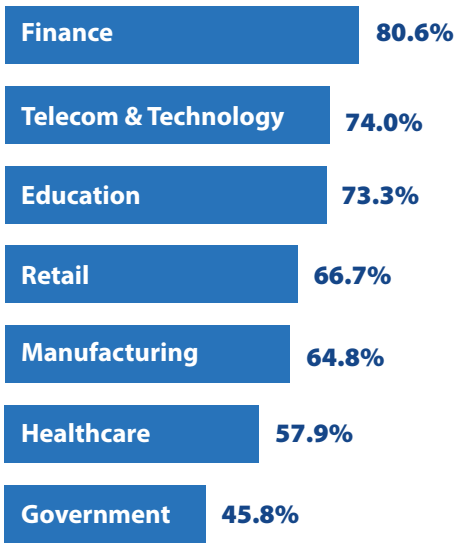

Figure 22: Percentage of organizations affected by ransomware in the last 12 months, by industry.

Finance (80.6%), telecom and technology (74.0%), and education (73.3%) were the worst-hit industries (see Figure 22). The least affected were healthcare (57.9%) and government (45.8%).

As shown in Figure 23, a shocking nine out of 10 organizations (89.6%) in China suffered ransomware attacks, followed by South Africa (89.6%) and the United States (81.6%). At the light end of the scale were Japan (60.4%), Germany (60.0%), Colombia (53.1%), Mexico (45.5%), and Turkey (44.9%).

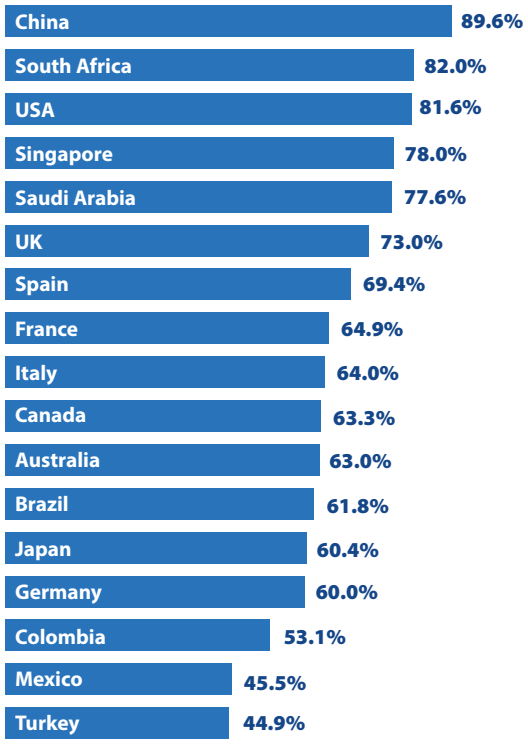

Figure 23: Percentage of organizations affected by ransomware in the last 12 months, by country.

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.

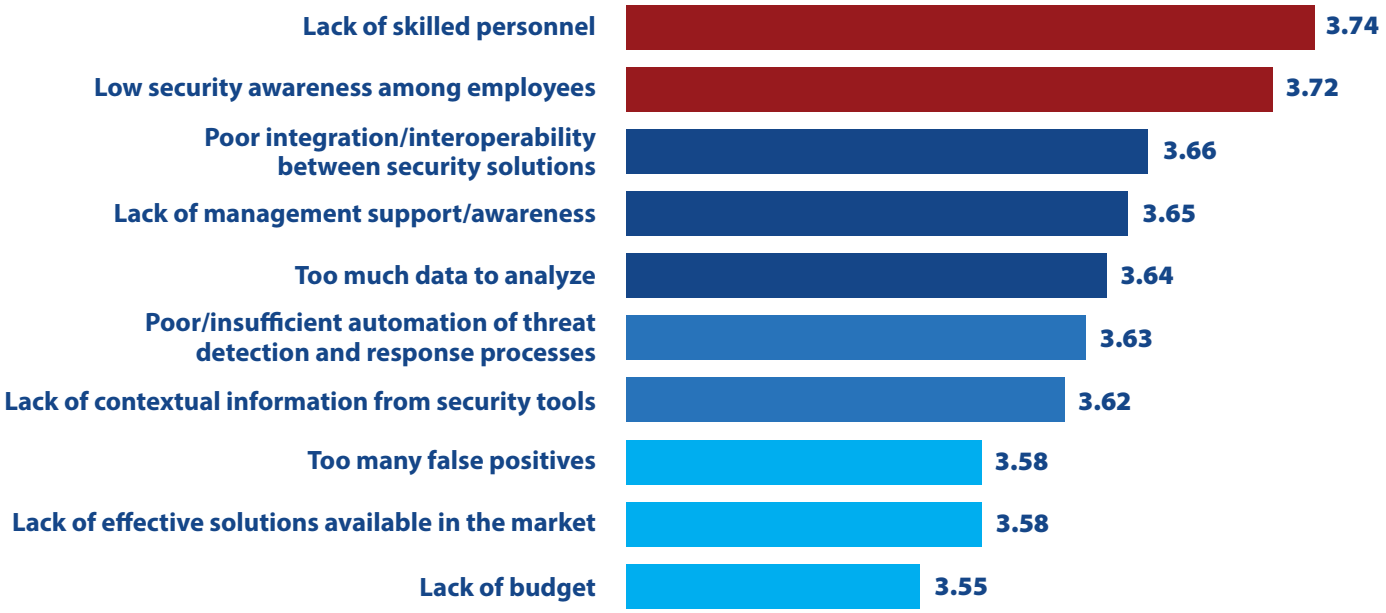

Figure 24: Inhibitors to establishing effective cyberthreat defenses.

Agile software development teams hold daily "standup" meetings where each person briefly answers three questions:

1. What did you do yesterday?
2. What will you do today?
3. What impediments are blocking your progress?

Most of this report explores the answers security professionals give about their current practices and their plans for the coming 12 months. This question focuses on the equally important third query: what is inhibiting your organization from adequately defending itself against cyberthreats? And by implication, what could be changed to make you more successful?

For the third year running, the top two impediments have been lack of skilled personnel and low security awareness among employees (see Figure 24).

"For the third year running, the top two impediments have been lack of skilled personnel and low security awareness among employees."

Section 2: Perceptions and Concerns

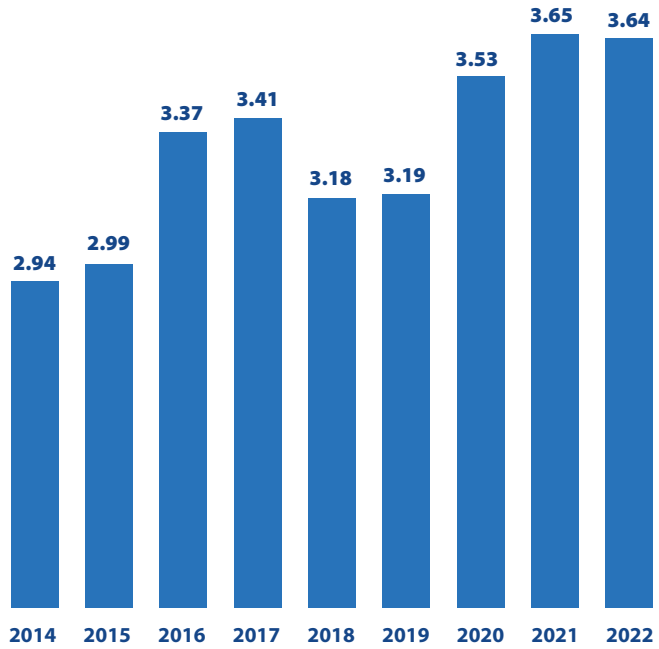

Figure 25: Security Concern Index, depicting the average rating of security inhibitors.

As we saw on page 15, five out of six organizations have not been able to recruit enough skilled IT security personnel. And we know that COVID-19 has put additional strain on existing professionals in the field. They have to defend an ever-expanding attack surface, and today many do so from home, without the resources of a physical operations center. This question highlights the impact of those factors. Not only is lack of skilled personnel the #1 inhibitor to effective cyberthreat defenses, but the average rating for this issue increased by .04 from last year, more than any other item on this list. Our hats are off to the dedicated professionals who have stepped up their workloads despite disruption to their personal lives.

Low security awareness among employees is the second-highest impediment to security. Coincidentally (or perhaps not), Figure 9 on page 13 shows that user security awareness is the IT security function with the second-to-lowest rating for adequate organizational capabilities. Threat actors continue to see employees as the weakest link in defenses, susceptible to phishing campaigns, social engineering attacks, business email compromise (BEC) attacks, and other techniques that play on human (rather than technical) weaknesses. Deep fakes and the availability of personal details on social media are likely to make it even easier to hoodwink employees. A few organizations have begun to take aggressive measures to improve security awareness, such as ongoing security training and simulated phishing and social engineering attacks, but clearly not enough is being done to educate employees.

The next tier of issues are poor integration and interoperability between security solutions, lack of management support, and too much data to analyze.

The inhibitors at the bottom of the list? Lack of effective solutions available in the market and lack of budget. New security technologies continue to come onstream, and organizations are willing to pay for them. The constraint is finding enough people with the right skills to evaluate, deploy, integrate, and manage them.

We have averaged the ratings across all categories to create a "Security Concern Index" (see Figure 25). That index remains at a near-peak level of 3.64. While some inhibitors have become less irksome than in previous years, others have become even more problematic.

Section 2: Perceptions and Concerns

Benefits of Unified App and Data Security Defenses

Which of the following have been the biggest benefits of leveraging a unified platform for application and data security defenses (e.g., WAF, DDoS protection, RASP, API security, data risk analytics, database security)? (Select up to three.)

Figure 26: Benefits achieved by unifying application and data security defenses.

When it comes to sourcing related technologies, security professionals are often faced with a choice between a multiple-source, best-of-breed approach and a single-source, integrated solution approach. The former offers the widest choice of features across the different areas, but usually involves extra costs and hassles related to integration (or lack of it), incompatible management and reporting tools, and the complexity of working with more vendors.

In this question we asked respondents about the benefits of leveraging a unified platform for application and data security defenses (see Figure 26).

Of the organizations that have implemented this type of integrated platform, more than half cite the overall benefit of an improved cloud security posture, and nearly half identified enhanced security incident investigations. An integrated solution gives security professionals confidence that the different technologies work together and that information won't fall through the cracks between them.

Section 2: Perceptions and Concerns

Respondents also highlighted an improved customer support experience and simplified security rules management. These are functions of better information sharing and working with a single, consistent set of security policies. Roughly one-third of the respondents also pointed to easier management of third-party integrations as a major benefit.

The fact that all five benefits were cited by at least 30 percent of the respondents indicates that a unified platform for application and data security is one of those areas in cybersecurity where integration and single-vendor sourcing just make sense.

"The fact that all five benefits were cited by at least 30 percent of the respondents indicates that a unified platform for application and data security is one of those areas in cybersecurity where integration and single-vendor sourcing just make sense."

Section 2: Perceptions and Concerns

Hybrid Cloud Security Challenges

Which of the following hybrid cloud security challenges are most concerning? (Select up to three.)

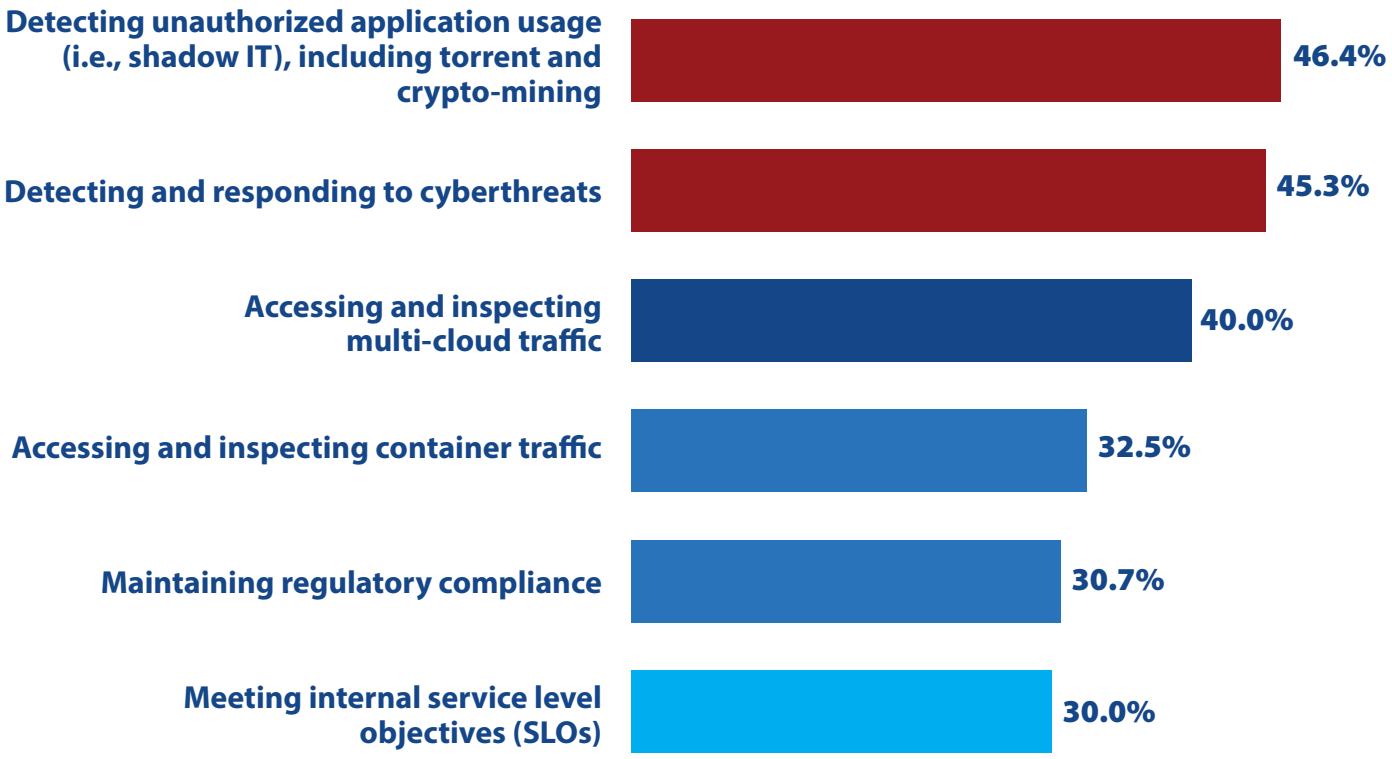

Figure 27: Most concerning hybrid cloud security challenges.

When organizations transition applications to cloud platforms, they don't have to worry about managing the underlying infrastructure. The move can even simplify security – if an organization does *all* of its work on one platform. But in reality, the vast majority of organizations do *some* of their work on each of *several* platforms. These include physical and virtual servers in their own data centers, in private clouds, and in multiple public cloud services such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Alibaba Cloud, and IBM Cloud.

We added a question to our survey this year to get a handle on the challenges created by hybrid cloud environments (see Figure 27).

The top two issues selected by the respondents were detecting unauthorized application usage (46.4%) and detecting and responding to cyberthreats (45.3%). While every server type and platform has tools for detecting issues and alerting on incidents, there is no standardization and little or no out-of-the-box integration. Security professionals are left with the soul-crushing work of collecting and analyzing inconsistent data, filtering out duplicates and false negatives, responding using multiple tools, etc.

Section 2: Perceptions and Concerns

The third- and fourth-place challenges are accessing and inspecting multi-cloud traffic (40.0%) and accessing and inspecting container traffic (32.5%). These two are also related to inconsistent data across environments and the need for multiple tools, sometimes compounded by the need to manage multiple permissions and credentials to access different systems and platforms.

"Security professionals are left with the soul-crushing work of collecting and analyzing inconsistent data, filtering out duplicates and false negatives, responding using multiple tools, etc."

Coming just behind, but still important to almost a third of the respondents, are challenges related to maintaining regulatory compliance (30.7%) and meeting internal service level objectives (30.0%).

How many organizations in fact face these challenges? A lot. A full 96% of the respondents in our survey indicated that they are dealing with a hybrid cloud environment.

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.)

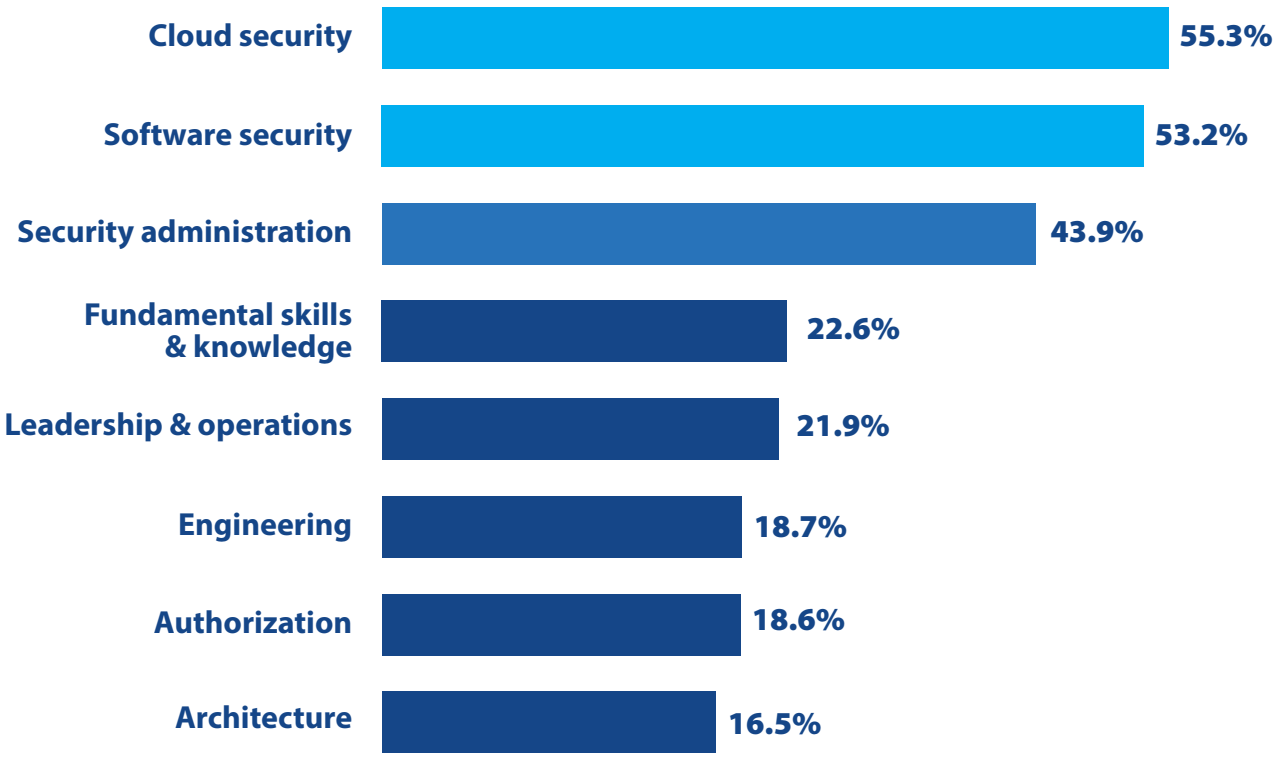

Figure 28: Types of specialty cybersecurity professional certifications deemed most beneficial to IT security career paths.

For knowledge workers, continuing education is essential for getting and keeping good jobs. At least, that is the overwhelming opinion of the respondents to our survey. Except for a few holdouts (1% of the sample - probably people already planning their retirement party), virtually all respondents said that at least one cybersecurity certification would be beneficial for their career (see Figure 28).

The top two choices, both selected by more than half of the respondents, are certifications for cloud security (55.3%) and for software security (53.2%). These are both growth areas. As enterprises migrate more and more application processing to cloud platforms, demand for cloud security expertise is likely to grow and grow. Similarly, many organizations are working on building security into their applications (as opposed to detecting evidence of attacks and compromises after they are in production). People who understand application security and DevSecOps practices don't have to worry about job security.

Section 2: Perceptions and Concerns

The next most beneficial certification is for security administration (43.9%). Security administrators are the backbone of many security teams, where they install, configure, and maintain security tools and infrastructure. As shown in Figure 10 on page 15, there are more vacancies for security administrators than for any other security role.

"Demand for cloud security expertise is likely to grow and grow... People who understand application security and DevSecOps practices don't have to worry about job security."

In fact, interest in all three of these certifications took big jumps from last year to this one: up 4.1% for cloud security, 3.2% for software security, and 5.6% for security administration.

The next two types of certification are of most interest to people making career moves. Fundamental skills and knowledge (22.6%) helps people entering IT security or eager to fill gaps in their basic knowledge of the field, while leadership and operations (21.9%) is for security professionals who want to move into security management roles.

Rounding out the field are certifications for three specialized areas: security engineering (18.7%), authorization (18.6%), and architecture (16.5%).

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)?

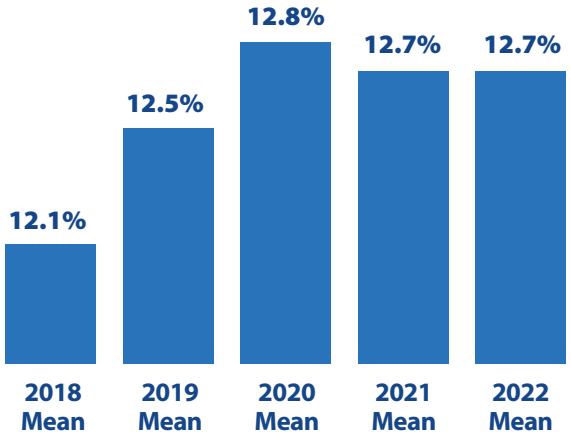

Figure 29: Percentage of IT budget allocated to information security, by year.

For the last five years we have asked respondents what percentage of their organization's overall IT budget is allocated to information security. After rapid growth between the 2018 and 2020 surveys, the amount has leveled off in the 12.7% to 12.8% range (see Figure 29).

Why has the curve flattened out, when dangerous threats continue to emerge and cybersecurity has become more visible to top management and boards of directors? And when the COVID-19 pandemic has placed more stress on security processes and staffs? We think four factors are at work:

1. Many of the expenses required to support the wave of new remote workers created by COVID-19 involved non-security items such as more laptops and mobile devices, more network capacity, and additional help desk support.
2. As shown on Figure 24 on page 24, the gating factor in providing better security is finding personnel with security skills, not budget; it doesn't make sense to throw more money at security if you don't have the people to deploy and use new technologies or equipment.

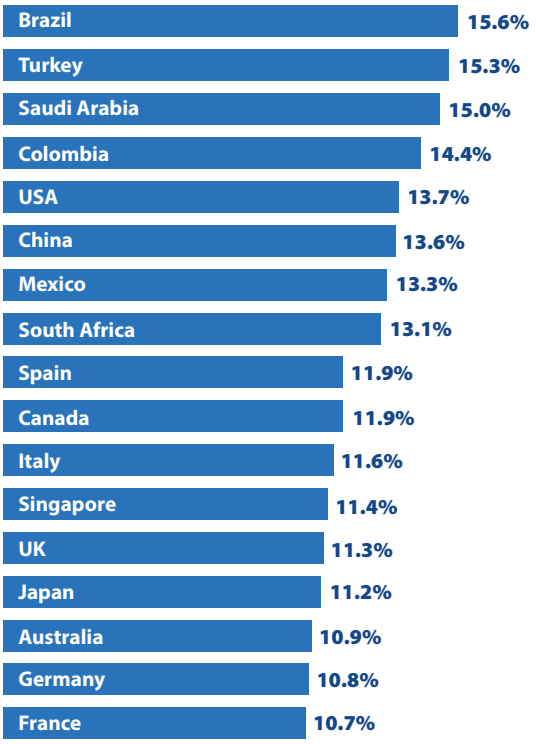

Figure 30: Percentage of IT budget allocated to security, by country.

3. More organizations are outsourcing security tasks that used to be performed in their data centers to cloud platform providers and MSSPs (see page 46).
4. Some organizations are "sidesourcing" security activities (we are coining a new term here, meaning delegating tasks to other groups in the same enterprise) by training software developers to build security into their code and end users to recognize and report phishing, social engineering, and other attacks.

Section 3: Current and Future Investments

"Why has the curve flattened out, when dangerous threats continue to emerge and cybersecurity has become more visible...? We think four factors are at work."

These factors lead organizations to invest more in security, but the additional spending doesn't show up in the security group's budget.

We welcome the fact that security no longer takes bigger bites out of the IT budget. Some might want to see growth in the relative size of the security "empire," but that growth is not sustainable in the long term.

Turning to the global picture, three countries allocate 15% or more of IT budgets to security: Brazil (15.6%), Turkey (15.3%), and Saudi Arabia (15.0%). Also towards the high end of the scale are the United States (13.7%) and China (13.6%). Three countries allocate less than 11%: Australia (10.9%), Germany (10.8%), and France (10.7%) (see Figure 30).

Among major industries, the largest allocations are from telecom and technology and finance (both 13.3%), while the lowest are from education (10.7%) and government (10.6%) (see Figure 31).

From a size perspective, the smallest organizations (500-999 employees) and the largest (10,000-24,999 and more than 25,000) allocate 13% or more. Mid-sized organizations spend slightly less: 12.7% for organizations with 1,000-4,999 employees, and 11.9% for those with 5,000-9,999 (see Figure 32).

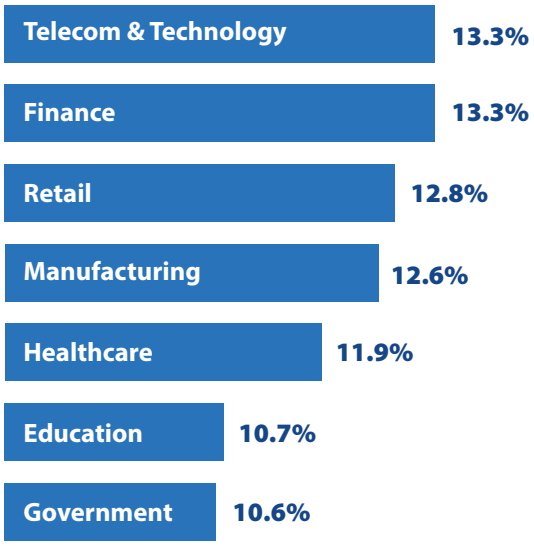

Figure 31: Percentage of IT budget allocated to security, by industry.

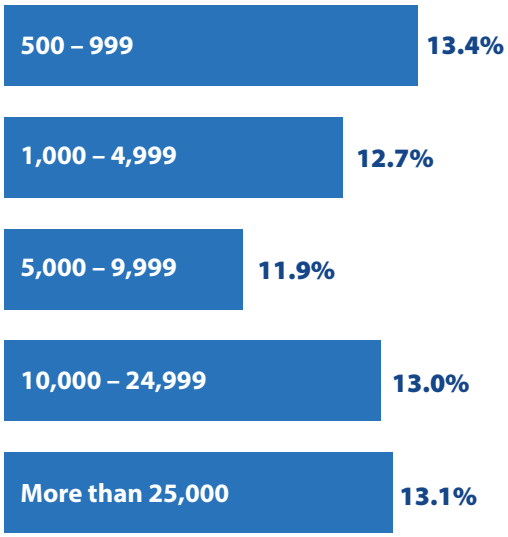

Figure 32: Percentage of IT budget allocated to security, by employee count.

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 2022?

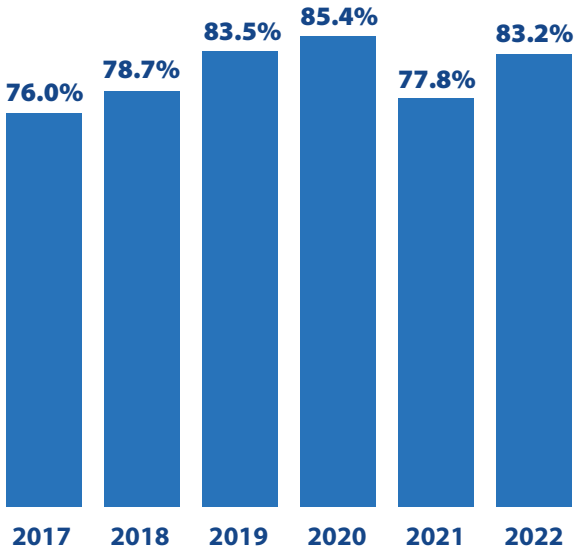

Figure 33: Percentage of organizations with rising security budgets.

On a country-by-country basis, respondents from Brazil and Turkey are expecting the largest budget increases, 6.7% and 6.5%, respectively (see Figure 35). Interestingly, they also report the largest allocations of their organization's IT budgets this year (see Figure 30 on page 32). The smallest increases are forecast for the United Kingdom (3.8%), Italy (3.7%), Canada (also 3.7%), and Germany (3.2%).

Respondents from five of the seven major industries are expecting increases of around 5% (see Figure 36). They are: manufacturing (5.3%), telecom and technology (4.9%), finance (also 4.9%), retail (4.8%), and education (4.7%). But the projected increases are below 4% for government (3.9%) and healthcare (3.6%).

The expected increases for small, medium, and large organizations all fall within a band of 4.2% to 5.5% (see Figure 37).

The previous question examined security spending as a percentage of the overall IT budget. This question looks at whether security spending is rising or falling in absolute terms.

It's mostly rising (see Figure 33). Of the organizations in the survey, 83.2% are predicting a budget increase this year (versus 7.1% that are predicting a decline and 9.7% that expect their budget to stay about the same). Those statistics are pretty consistent with results from the past few years, with the exception of 2021, when the COVID-19 pandemic prevented budget increases in slightly more organizations than usual.

The average increase in security budgets has been fairly steady, ranging between 4.0% and 5.0% for the past five years (see Figure 34). The average expectation is for budgets to rise a healthy 4.6% this year. If you work in cybersecurity, ask for a raise!

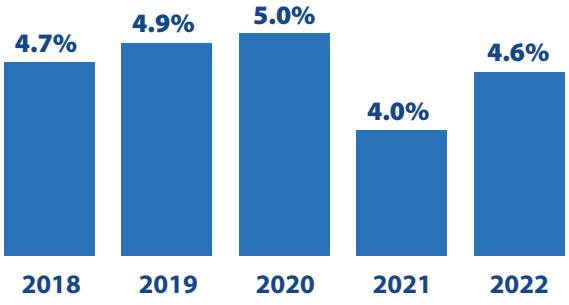

Figure 34: Mean annual increase in IT security budgets.

Section 3: Current and Future Investments

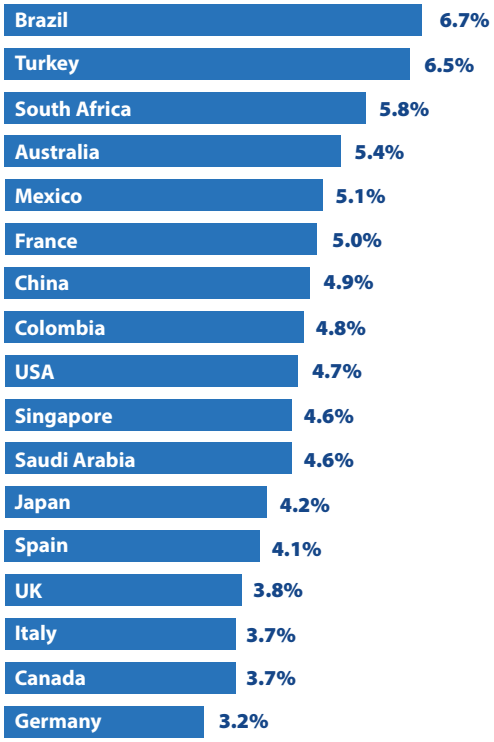

Figure 35: Mean security budget increase, by country.

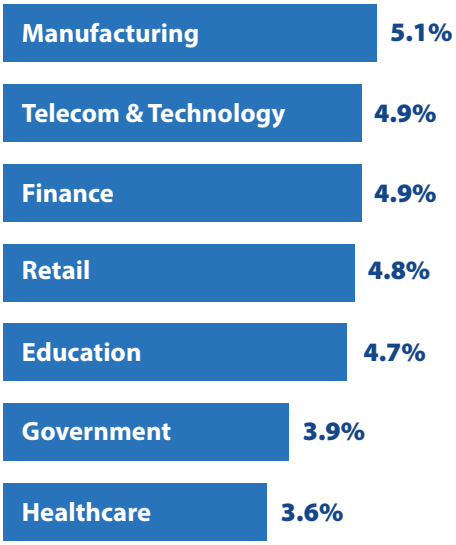

Figure 36: Mean security budget increase, by industry.

"The average increase in security budgets has been fairly steady, ranging between 4.0% and 5.0% for the past five years."

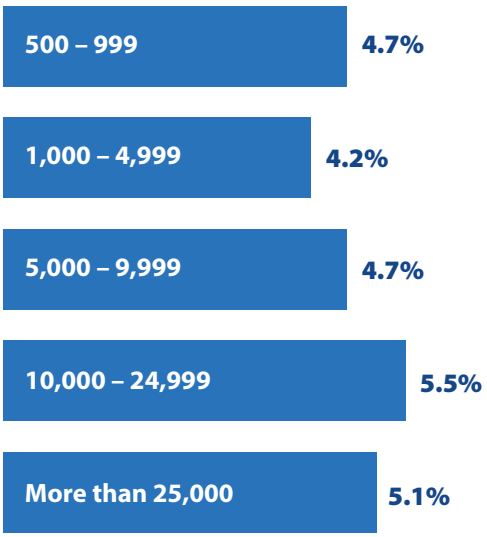

Figure 37: Mean security budget increase, by employee count.

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
Advanced malware analysis / sandboxing	59.7%	31.0%	9.3%
Intrusion detection / prevention system (IDS/IPS)	56.2%	33.7%	10.1%
Secure email gateway (SEG)	56.1%	30.8%	13.1%
Data loss / leak prevention (DLP)	55.0%	34.9%	10.1%
Secure web gateway (SWG)	55.0%	34.2%	10.8%
Network access control (NAC)	54.4%	35.0%	10.6%
Denial of service (DoS/DDoS) prevention	53.9%	35.2%	10.9%
SSL/TLS decryption appliances / platform	51.8%	36.1%	12.1%
Network behavior analysis (NBA) / NetFlow analysis	46.9%	37.5%	15.6%
Next-generation firewall (NGFW)	46.1%	41.9%	12.0%
Deception technology / distributed honeypots	44.3%	37.1%	18.6%

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

There is no shortage of innovative new security products being brought to market. According to the Crunchbase website, in 2021 venture capitalists invested $20 billion in cybersecurity startups, including a record-smashing $7.8 billion in the fourth quarter. And as we saw in Figure 24 on page 24, "lack of effective solutions available in the market" tied for second-to-last place in a list of factors that inhibit defense against cyberthreats. Nobody is worried about having too few options.

But while an abundance is better than a dearth, it does make prioritization more difficult. We want to help. In this question and the next four, we throw light on what your peers think. What cybersecurity offerings are must-haves? Which are the up-and-comers they plan to acquire to address emerging threats? Are some failing to generate much interest?

Section 3: Current and Future Investments

On this and the following tables, the first column shows the percentage of organizations that are currently using each technology. The middle column depicts organizations that are planning to acquire the technology this year. The last column represents organizations that aren't sure they need the technology. To make the results easier to absorb, we color-coded the cells. Dark blue highlights technologies that are widely used now or are most likely to be deployed soon. Lighter shades indicate lower adoption levels and fewer planned acquisitions. The cells with the "no plans" figures are gray.

"While advanced malware and sandboxing remain a 'must have' technology, four other network security technologies are also found in 55% or more of organizations."

We start by examining network security technologies (see Table 1). For the last several years, the one that has been most widely used is advanced malware detection and sandboxing (in use in 59.7% or organizations). The ubiquity of this technology (or really, group of technologies) is not surprising, given that malware concerns our respondents more than any other type of threat (as shown in Figure 13 on page 17).

However, this area is subject to a continuous arms race. Vendors compile more malware signatures; threat actors use obfuscation and polymorphism to disguise files. Vendors use sandboxing to detect malicious behaviors; the bad guys figure out how to delay malicious activities until after the sandboxes stop detecting. Vendors use AI to identify suspicious activities; attackers manage to prevent the anti-malware software from running. Move and countermove.

So, while advanced malware and sandboxing remain a "must-have" technology, four other network security technologies are also found in 55% or more of organizations. Installations of all four grew substantially since the previous survey. They are: intrusion detection/prevention system (IDS/IPS), up 4.4% to 56.2%; secure email gateway (SEG), up 2.8% to 56.1%; data loss/leak prevention (DLP), up 1.5% to 55.0%; and secure web gateway (SWG), up 3.3% to 55.0%. These technologies use a variety of methods to detect anomolous network behaviors, as well as content and hyperlinks that may be related to malicious activities.

The next three network security technologies on our list are in use at more than half of organizations: network access control (NAC), at 54.4%; denial of service (DoS/DDos) prevention, at 53.9%; and SSL/TLS decryption appliances and platforms, at 51.8%.

Lined up for new installations or upgrades in the coming 12 months: next-generation firewall (NGFW) technology (planned for acquisition by 40.3% or organizations), network behavior analysis (NBA) and netflow analysis (37.5%), and deception technology and distributed honeypots (37.1%). We think the last type of technology is especially interesting since it can be used to catch threat actors "in the act" without exposing real networks or data.

Now let's see what endpoint security technologies are exciting your peers (page 38).

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)	74.2%	22.3%	3.5%
Endpoint detection and response (EDR)	57.6%	31.8%	10.6%
Data loss / leak prevention (DLP)	56.6%	31.6%	11.8%
EPP / Advanced anti-virus / anti-malware (machine learning, behavior monitoring, sandboxing)	55.3%	35.8%	8.9%
Browser or Internet isolation / micro-virtualization	55.1%	35.5%	9.4%
Disk encryption	53.3%	36.2%	10.5%
Digital forensics / incident resolution	49.8%	36.4%	13.8%
Deception technology / honeypots	44.1%	40.5%	15.4%

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

Table 2 provides insights into the deployment status and acquisition plans for endpoint security technologies. As with Table 1, percentages in dark blue indicate a higher frequency of adoption and greater likelihood of acquisition, while lighter blues correspond to less-popular options.

The most widely installed endpoint security technology continues to be basic anti-virus and anti-malware solutions based primarily on threat signatures. Despite continued reports that "anti-virus is dead," old but still dangerous viruses and Trojans continue to circulate, and security groups see value in products that detect and block them. That may be why the percentage of organizations currently using this technology actually increased 3.7%, from 70.5% in the previous survey to 74.2% in this one.

In this survey we made a significant change to our endpoint security technology categories, replacing "advanced anti-virus" with endpoint protection platform (EPP) and endpoint detection and response (EDR). This update reflects the evolution of this technology area and current industry terminology.

Broadly speaking, EPP products provide traditional anti-virus features enhanced by an array of newer capabilities such as machine learning, endpoint activity monitoring, and sandboxing. Collectively, they overcome many of the tricks and techniques malware developers use to evade detection. EDR solutions may include certain EPP features, but they also offer tools to help security teams aggregate and analyze endpoint data and respond to campaigns that involve malware.

Section 3: Current and Future Investments

"Our respondents reported EDR solutions in use at 57.6% of organizations, and EPP products installed at 55.3%. These numbers suggest that many organizations use both EDR and EPP technologies – and basic anti-virus packages as well – on their endpoints."

Our respondents reported EDR solutions in use at 57.6% of organizations, and EPP products installed at 55.3%. These numbers suggest that many organizations use both EDR and EPP technologies – and basic anti-virus packages as well – on their endpoints.

What endpoint technology had the biggest jump in usage during the past year? That would be browser or internet isolation and micro-virtualization products. Installations leaped 6.9%, from 48.2% to 55.1%. Instead of viewing web pages and running scripts and apps in browsers on their own systems, end users run them in a virtual browser on a cloud platform. Malware can't spread to the users' systems, and suspicious activities can be observed in the cloud. This technology has a great deal of appeal for organizations where remote work and cloud applications are expanding.

The other technologies in use at more than half of the surveyed organizations are data loss or lead prevention (DLP), at 56.6%, and disk encryption, at 53.3%.

The endpoint security solution most often planned for acquisition in the coming year is deception technology and honeypots. As we mentioned in reference to network security, this can be used to catch threat actors in the act without exposing sensitive data. This solution not only prevents data breaches in the short run, it also derails and misinforms attackers and collects intelligence on the tactics, techniques, and procedures (TTPs) of threat actors. There is also a psychological element: many security organizations welcome the chance to gain an advantage over attackers instead of always being at a disadvantage.

Now it's time to explore application- and data-centric security technologies (see page 40).

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
API gateway / protection	64.1%	28.6%	7.3%
Web application firewall (WAF)	61.1%	29.9%	9.0%
Database firewall	59.5%	30.5%	10.0%
Application container security tools/platform	54.3%	36.5%	9.2%
Cloud access security broker (CASB)	53.3%	33.2%	13.5%
Database activity monitoring (DAM)	53.1%	35.9%	11.0%
Application delivery controller (ADC)	52.2%	33.6%	14.2%
Runtime application self-protection (RASP)	50.4%	35.1%	14.5%
File integrity / activity monitoring (FIM/FAM)	50.2%	37.8%	12.0%
Advanced security analytics (e.g., with machine learning, AI)	50.2%	39.7%	10.1%
Static/dynamic/interactive application security testing (SAST/DAST/IAST)	48.0%	38.2%	13.8%
Bot management	42.6%	39.8%	17.6%

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

In the area of application and data security, the most popular offering continues to be API gateway and protection products (see Table 3). Usage of these technologies has soared over the last few years, rising from 45.1% in our 2018 report to 64.1% today. API gateways enforce authorization and encryption policies, scale resources when traffic spikes, and perform rate limiting to mitigate DDoS attacks and other forms of abuse. API protection solutions provide security teams with tools to understand, detect, and respond to attacks targeting APIs by performing tasks such as mapping the attack surface to uncover rogue and forgotten APIs, blocking injection attacks and other exploits, analyzing attacker behaviors, and correlating API-related data across hybrid and multi-cloud environments.

As we mentioned in our discussion of security posture by IT domain on page 12, protecting APIs has become an increasingly pressing area of concern. As more organizations move to modular, services-based cloud applications, more sensitive data is being accessed through APIs, which are becoming more tempting targets for threat actors. We think API protection will become an even bigger area of focus in coming years.

Section 3: Current and Future Investments

Two other must haves are web application firewalls (WAFs), at 61.1%, and database firewalls, at 59.5%. These technologies have proved themselves in preventing unauthorized access to web applications and databases.

Other application and data security solutions that showed significant growth in installations over the past year are file activity and activity monitoring (FIM/FAM), up 3.3% to 50.2%; runtime application self-protection (RASP), up 2.2% to 50.4%; and application delivery controllers (ADCs), up 1.8% to 52.2%.

The number-one technology for upcoming purchases is bot management, planned for acquisition in 39.8% of organizations. It helps defend websites and mobile applications from the many types of attacks that utilize bot networks, including DDoS attacks, phishing and spam campaigns, credential stuffing, brute force password cracking, content scraping, and click fraud.

"The most popular offering continues to be API gateway and protection products. Usage of these technologies has soared... rising from 45.1% in our 2018 report to 64.1% today."

Other application and data-centric security technologies included on a lot of shopping lists are advanced security analytics, at 39.7%, and static, dynamic, and interactive application security testing (SAST/DAST/IAST), at 38.2%.

Now that we've covered application and data security, let's see what's happening in the world of security management and operations technologies (see page 42).

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	64.5%	27.1%	8.4%
Cyber risk management and reporting	58.0%	31.3%	10.7%
Security configuration management (SCM)	56.5%	32.4%	11.1%
Patch management	54.7%	32.6%	12.7%
Security information and event management (SIEM)	51.7%	36.2%	12.1%
Penetration testing / attack simulation software	50.7%	35.4%	13.9%
Vulnerability assessment/management (VA/VM)	50.6%	38.8%	10.6%
Full-packet capture and analysis	50.4%	36.4%	13.2%
Advanced security analytics (e.g., with machine learning, AI)	50.2%	39.7%	10.1%
Security orchestration, automation and response (SOAR)	49.4%	36.7%	13.9%
Threat intelligence platform (TIP) or service	46.3%	39.7%	14.0%
User and entity behavior analytics (UEBA)	45.7%	38.9%	15.4%

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

Security management and operations technologies support a number of activities that make security programs effective and reliable, including:

- Providing basic security hygiene and reducing the attack surface
- Automating security-related processes
- Collecting, analyzing, and reporting on security data to identify weaknesses, respond to breaches, and prioritize investments
- Testing security defenses using the techniques of likely attackers

We added two new categories to our survey this year, and they immediately occupied the top two spots in terms of installations (see Table 3)!

Active Directory protection is already in use in almost two-thirds of organizations (64.5%). For many, Microsoft Active Directory is the single source of truth for information about employee and business partner identities, as well as a repository for information on group membership and privileged access. It is also a critical resource for implementing ZTNA concepts. Therefore organizations must protect Active Directory from cybercriminals attempting to create new accounts, escalate privileges, circumvent network segmentation, and otherwise gain unauthorized access to networks and applications.

Section 3: Current and Future Investments

Cyber risk management and reporting, currently used in 58.0% of organizations, helps align security activities with business risks and needs. It also helps IT groups justify investments in security professionals, processes, and technologies to top management and boards of directors.

Other security management technologies that are widely in use include security configuration management, or SCM (employed in 56.5% of organizations), patch management (54.7%), and security information and event management, or SIEM (51.7%).

One of the leaders in year-over-year growth was penetration testing and attack simulation. The percentage of organizations using it increased 2.8%, to 50.7%. We think the use of penetration testing and attack simulation will continue to grow, along with practices such as red team exercises and bug bounty contests. As many organizations place more emphasis on developing secure applications, they are recognizing that some application security issues can only be uncovered by thinking like an attacker.

Our data for threat intelligence platform (TIP) or service adoption is interesting. Of all the options in the security management and operations section, this technology had:

1. The biggest year-to-year increase in usage, up 3.3% to 46.3%
2. The highest planned for acquisition number, 39.7%

In the past, we have rarely seen that combination. Threat intelligence helps organizations validate and prioritize security alerts more quickly and accurately, focus on the threats most likely to affect their specific industry and systems, and better understand threat actor TTPs. Our data about TIP indicates a growing appreciation of threat intelligence and the advantages it provides.

"On this year's application and data security shopping list, a new CDR entrant, bot management, takes the top spot (40.4%)."

The other technologies with high planned for acquisition percentages are advanced security analytics (also 39.7%), user and entity behavior analysis (38.9%), and vulnerability assessment and management (38.8%).

And now, on to our final category: identity and access management, or IAM (see page 44).

Section 3: Current and Future Investments

Identity and Access Management Deployment Status

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

	Currently in use	Planned for acquisition	No plans
Password management / automated reset	62.1%	28.5%	9.4%
Adaptive/risk-based authentication	61.8%	28.7%	9.5%
Two-/multi-factor (2FA/MFA) authentication	56.8%	31.8%	11.4%
Single sign-on (SSO)	53.6%	33.4%	13.0%
Privileged account/access management (PAM)	52.8%	33.7%	13.5%
User/account provisioning and de-provisioning	52.3%	35.9%	11.8%
Identity-as-a-Service (IDaaS)	50.3%	35.5%	14.2%
Smart cards	46.8%	38.6%	14.6%
Federated identity management (SAML, Oauth)	46.7%	36.0%	17.3%
Biometrics	44.6%	40.9%	14.5%

Table 5: Identity and access management technologies in use and planned for acquisition.

Identity and access management (IAM) is not the most glamorous segment of information security. It involves a number of cutting-edge technologies, but also a lot of operational, administrative, and support tasks related to roles, permissions, account provisioning and deprovioning, password resets, access controls, etc., etc.

Yet today, as never before, organizations need to perform these tasks quickly and accurately, with maximum security but the least possible annoyance to users and minimum disruption to business processes. That's because more and more business is being done with web and mobile applications, which lead employees and customers to expect consumer-level convenience, but in an environment where nobody can be trusted to be who they say they are (hence "zero trust" practices).

Who says IAM is increasingly important? Well, our data does. Since our last survey, organizations increased their use of nine out of the 10 technology categories listed in Table 5. The percentage using two of the categories increased 7.5%, which is more than any technology in any of our other tables. IAM is not the most glamorous segment of information security, but in some respects it is getting the most attention.

The use of password management and automated reset, the most widely deployed IAM technology, increased by 7.5% year over year, to 62.1%. It automates a very basic set of tasks, but provides a big payoff in both user satisfaction and time savings for IT support staff and administrators.

Section 3: Current and Future Investments

"IAM is not the most glamorous segment of information security, but in some respects it is getting the most attention."

Adaptive and risk-based authentication was up 5.5% this year, on top of 4.9% growth last year, to reach 61.8% of organizations. It balances security and convenience by ensuring that employees and customers provide just the appropriate amount of credentials and information, but no more, based on factors like the value of the transaction, information about the user and the device, and past behaviors.

The use of two-factor and multi-factor authentication (2FA and MFA) also surged 7.0% from the previous survey, reaching 56.8%. They have become requirements for many classes of application, and vendors and security groups are coming up with ingenious ideas for the second and nth factors.

Several other IAM technologies are currently in use in half or more of all organizations. These include single sign-on (SSO), up 3.8% to 53.6%; privileged account management (PAM), up 1.4% to 52.8%; and user and account provisioning and deprovisioning, which are up 1.7% to 52.3%.

The clear winner in the middle column of Table 5 is biometrics, with 40.5% of organizations planning to acquire or upgrade technology in that area. Biometric technologies go even further than other MFA approaches in combining better security with increased convenience.

It is noteworthy that the US Cybersecurity and Infrastructure Security Agency (CISA) highlights identity as one of the five pillars of its Zero Trust Maturity Model. CISA emphasizes that organizations should validate identities continuously, not just when initially granting access. Additionally, organizations should fully implement just-in-time and just-enough access controls and have global identity awareness across cloud and on-premises environments. We are likely to see more organizations move in these directions.

And whatever you may see in the movies, it is not possible to chop off someone's finger and use it to open the door of a top-secret laboratory. That's because of things like tissue deterioration and capacitive sensors in the fingerprint reader that must be activated by electrical charges in skin. We thought you would want to know that.

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)

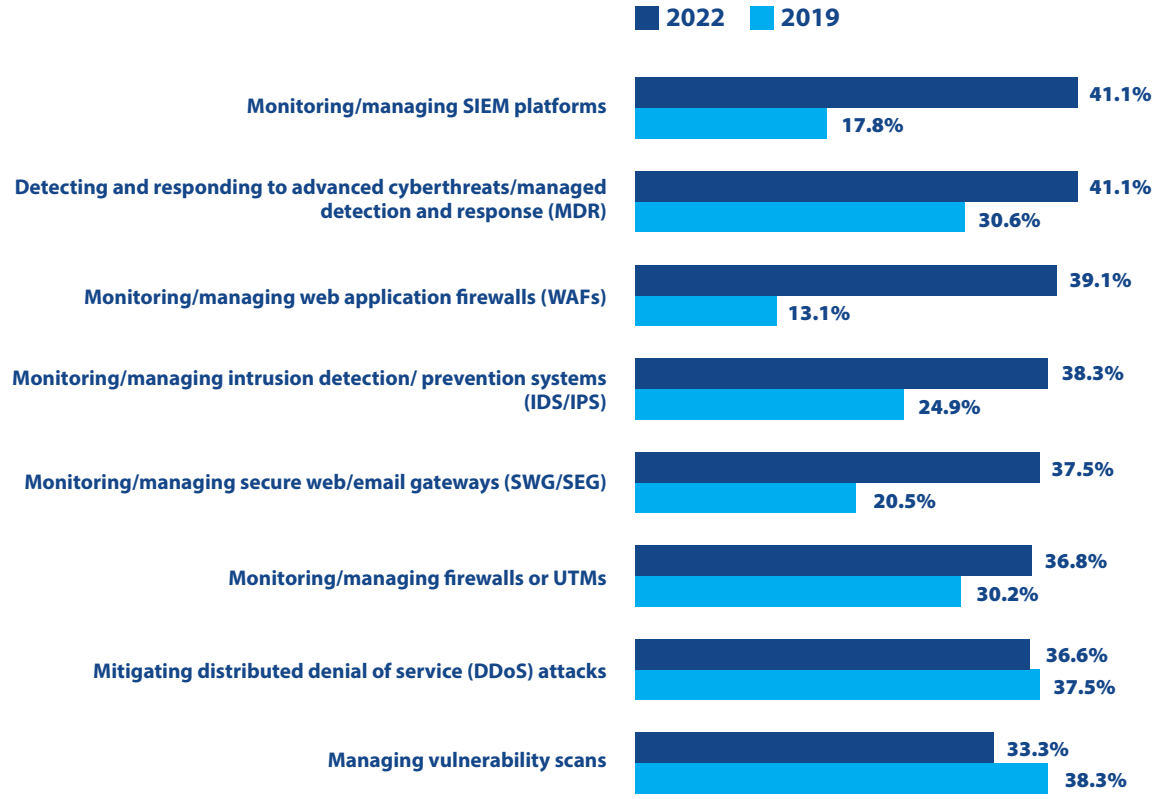

Figure 38: Functions outsourced to an MSSP in 2019 and 2022.

We have observed a trend toward greater use of managed security service providers (MSSPs), driven primarily by the shortage of skilled IT security staff. If you can't hire enough experienced security professionals, why not outsource routine, repetitive tasks? Or activities that require special skills that are in short supply? Or jobs that someone else has figured out how to automate?

Hmm. What are enterprises using MSSPs for? We asked that question in older editions of the Cyberthreat Defense Report, then dropped it for a few years. We decided to ask again and compare the results with those from the 2019 report. Figure 38 shows responses of organizations that outsource at least one task to an MSSP, and Figure 39 shows how many organizations were not using an MSSP at all in those two years.

As we can see from Figure 39, only 10% of organizations didn't work at all with an MSSP in 2019, and that figure was even lower in 2022: 6.8%. In the big picture that isn't much of a difference.

But Figure 38 shows that many of the security teams that were using MSSPs for one or two tasks in 2019 are now working with them on three or more.

Section 3: Current and Future Investments

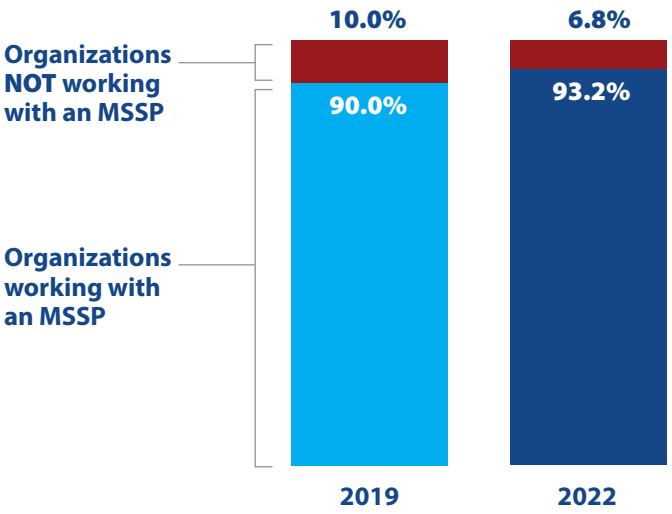

Figure 39: Percentage of organizations not working with an MSSP in 2019 and 2022.

"What are enterprises using MSSPs for? We asked that question in older editions of the Cyberthreat Defense Report, then dropped it for a few years. We decided to ask again and compare the results with those from the 2019 report."

We can also see a significant shift in the mixture of the tasks being outsourced to MSSPs. Actually, the ones that were the leaders in 2019 – managing vulnerability scans, mitigating DDoS attacks, detecting and responding to advanced threats, and monitoring and managing firewalls and UTM devices – are still common today, if at somewhat lower rates. But the categories that were less popular in 2019 have shown tremendous increases over the past three years.

Specifically, 23.3% more organizations are using MSSPs to monitor and manage SIEM platforms. The use of MSSPs to monitor and manage WAFs has increased 26.0%. Monitoring and managing IDS/IPS systems is up 13.4%, and monitoring and managing SWG and SEG platforms has risen 17.0%.

Why the dramatic upswing in the use of MSSPs for all of these monitoring and managing tasks? It is partly attributable to the fact that these are very labor-intensive activities, particularly when they involve filtering and prioritizing alerts. Organizations would like to free up their security professionals for more-strategic jobs. Another major factor is that MSSPs have achieved a high level of automation of these tasks, so they can provide these services very economically to their clients.

However, our data included one surprise. The conventional wisdom is that MSSPs are more popular with small organizations that can't fill their staff with security specialists. However, as shown in Figure 40, 87.4% of small organizations (500-999 employees) use an MSSP, and 92.7% of medium-sized ones (1,000-4,999 employees), but large and very large enterprises employ MSSPs even more often (94.3% or higher). Evidently, even very large security groups want to save money and free up their expert personnel for strategic projects.

Of course, some organizations outsource tasks related to specific applications or business units, while using their internal staff to perform the same tasks for other applications and business units. Probably many of the large and very large enterprises are using MSSPs selectively rather than across the board. But they do use them.

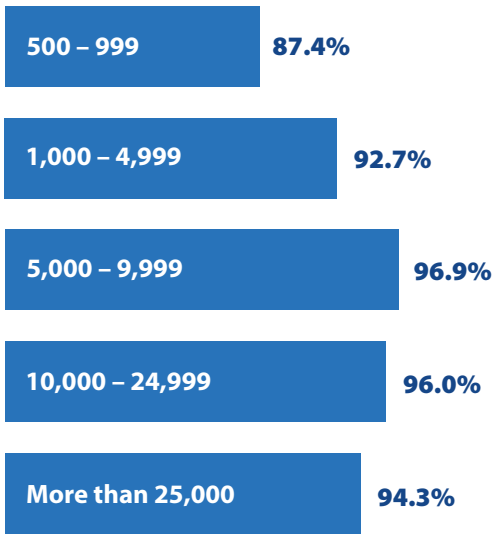

Figure 40: Percentage of organizations using an MSSP, by employee count.

Section 4: Practices and Strategies

Security Applications Delivered via the Cloud

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

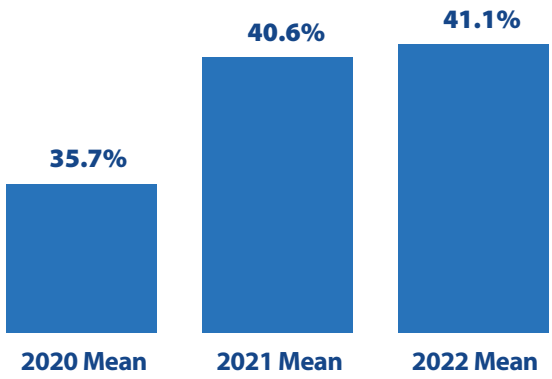

Figure 41: Percentage of security applications and services delivered via the cloud.

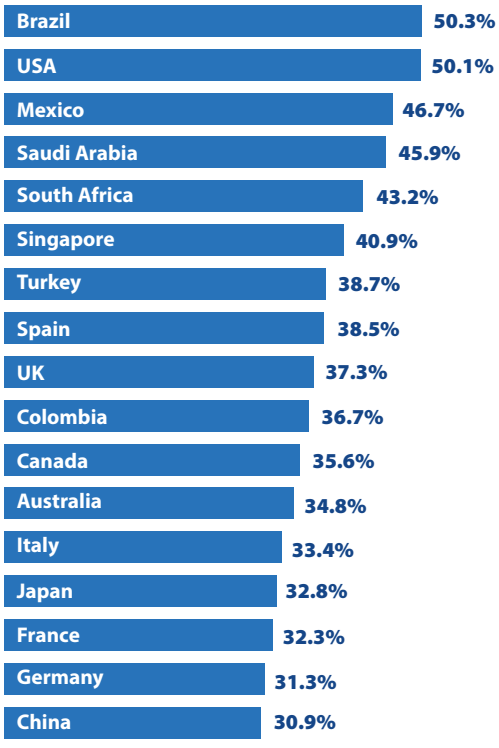

Figure 42: Percentage of security applications and services delivered via the cloud, by country.

In August 2020, CyberEdge conducted a survey that was published as "The Impact of COVID-19 on Enterprise IT Security Teams." Of the 600 IT security professionals surveyed, three-quarters indicated a significant preference for cloud-based security solutions over traditional on-premises products.

That preference resulted in action. Organizations made a heroic effort to support remote work, BYOD policies, and cloud-based applications with cloud-based security. Between our 2020 and 2021 reports, the percentage of security applications and services delivered via the cloud jumped from 35.7% to 40.6%, an increase of 4.9% (see Figure 41).

Between the 2021 and 2022 reports, the percentage moved up a more modest 0.5%, as security groups shifted from deploying new cloud-based security solutions to tuning and consolidating the ones implemented earlier. And the new record level, 41.1%, is pretty impressive, given that only a few years ago most people thought they couldn't trust security products outside their organization's data centers.

We believe the share of cloud-based security offerings is likely to increase at a steady pace of around 0.5% to 1.0% per year for several years. These offerings include security tools from public cloud platform providers like Amazon, Microsoft, and Google, cloud-based versions of existing on-premises security products, and new security solutions developed from the ground up for cloud deployment.

The appetite for cloud-based security applications and services varies considerably around the globe (see Figure 42). Half of all security is cloud-based in Brazil (50.3%) and the United States (50.1%). Not far behind come Mexico (46.7%) and Saudi Arabia (45.9%). At the other end of the spectrum, cloud-based security solutions have not been so widely adopted in Japan (32.8%), France (32.3%), or Germany (31.3%). The nation with the lowest level of interest is China (30.9%).

Section 4: Practices and Strategies

As shown in Figure 43, the major industries most aggressively adopting cloud-based security are finance (48.7%), healthcare (44.3%), and retail (42.1%). Slower adopters include educational institutions (30.6%) and government agencies (30.4%).

"These days, smart IT security teams are turning to cloud-based security solutions like never before."

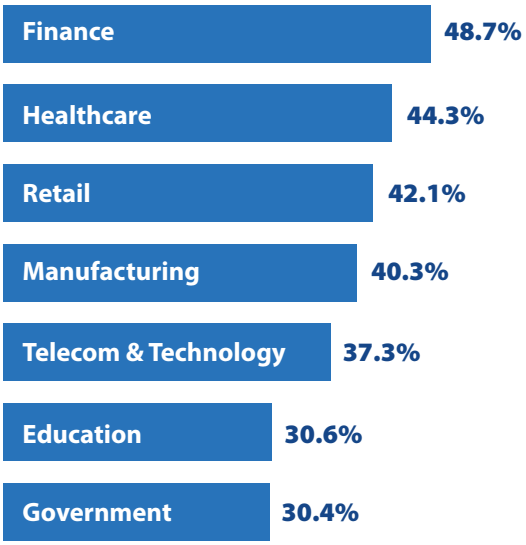

Figure 43: Percentage of security applications and services delivered via the cloud, by industry.

Section 4: Practices and Strategies

Practices That Support Application Security

Which of the following practices does your organization embrace to enhance application security? (Select all that apply.)

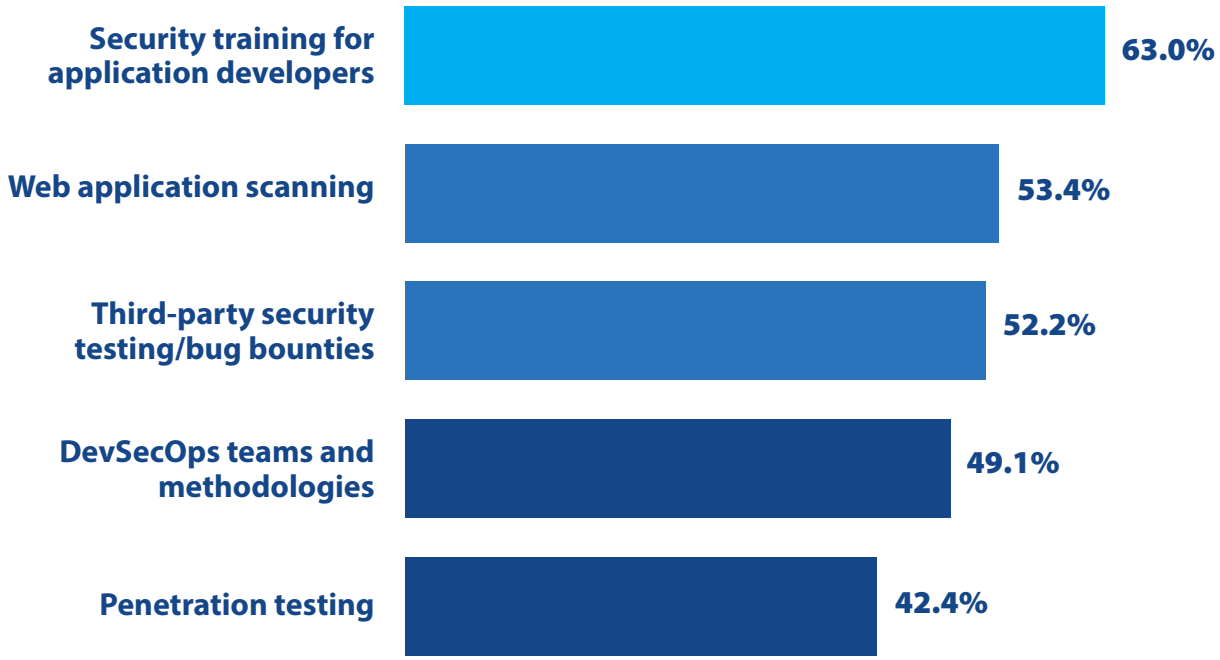

Figure 44: Practices organizations use to enhance application security.

Many organizations are investing in application security. You can prevent a lot of data breaches if you can build good security into an application and catch security-related defects before it is put into production.

But what exactly are organizations doing to enhance application security? We added this question to the survey so you could find out what your peers are doing (see Figure 44).

The most popular practice is security training for application developers, provided by 63.0% of the organizations surveyed. Traditionally, coders focused on functionality and did not have the knowledge or incentive to address security issues. Security training encourages development teams to follow security best practices for architecting applications (e.g., segmenting application components and controlling access between them), coding (e.g., validating user input and using parameterized queries to block injection attacks), adding risk-based authentication, encrypting data at rest and in motion, and other areas where security can be built into the application.

Section 4: Practices and Strategies

"You can prevent a lot of data breaches If you can build good security into an application and catch security-related defects before it is put into production."

Developers can also be trained to test their own work to find security weaknesses in the code and in business logic.

Web application scanning is an automated way to uncover a wide range of vulnerabilities and defects in online applications. It is performed at 53.4% of organizations.

Also widely used are third-party security testing and bug bounty programs (52.2%) and penetration testing (42.4%). Both encourage human testers to think like attackers and replicate their techniques to find weaknesses that conventional scanning and software testing tools won't detect. Bounty programs are economical and can enlist a large number of freelance testers, but the participants get to choose what they test, so they may not cover all features of an application. Penetration testing, either by internal staff or service providers, is more expensive, but the testers' activities can be directed to ensure complete coverage.

Finally, development/security/operations (DevSecOps) practices, in use in 49.1% of organizations, ensure that software code is tested early and continuously during the application development process. In the 2021 CDR we asked respondents about the benefits of DevSecOps practices. They cited increased speed of deploying application updates and new applications, improved relations between development and security personnel, reduced costs, and fewer application security vulnerabilities.

Section 4: Practices and Strategies

Protecting Employees Working from Home

Which of the following technologies and/or architectures does your organization use to enable employees to securely work from home? (Select all that apply.)

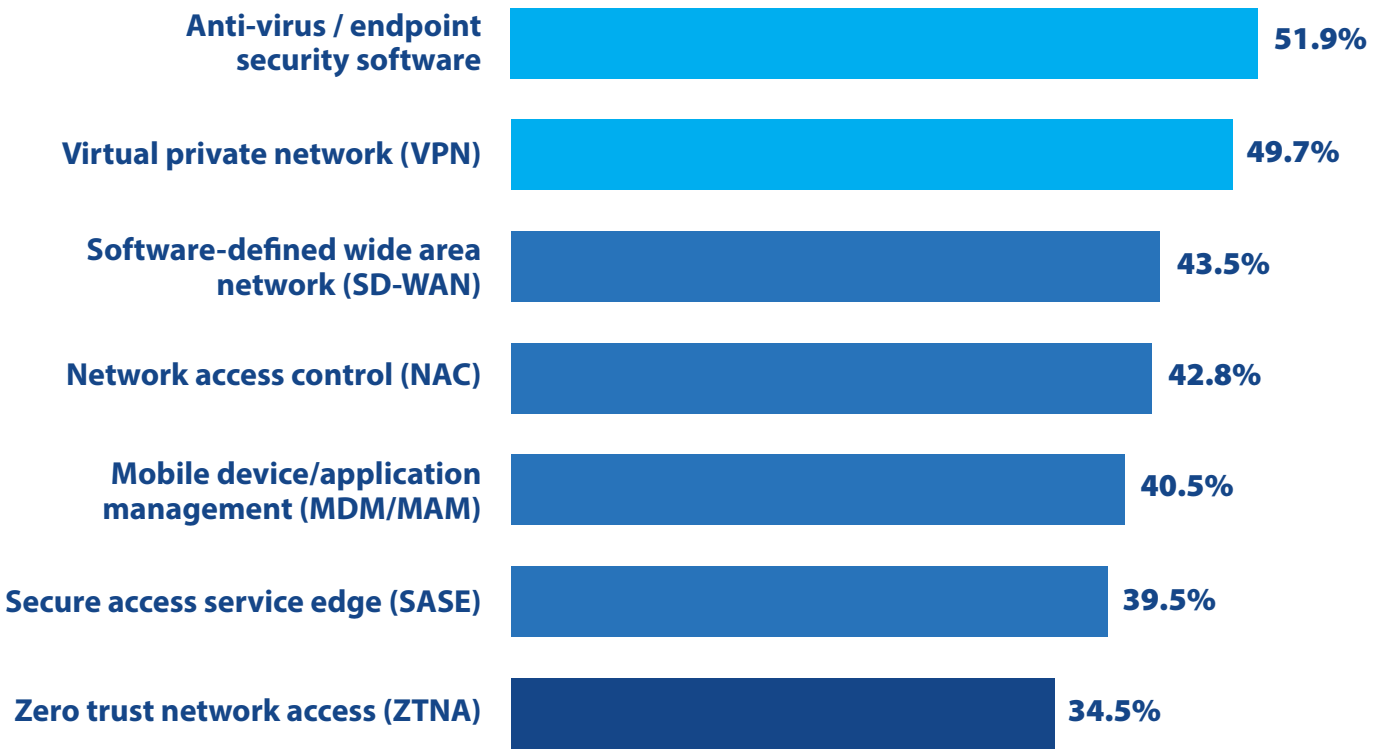

Figure 45: Technologies and architectures to enable secure work from home.

According to a recent blog post by the Gallup polling and analytics firm (Bet on It: 37% of Desks Will Be Empty), of the 60 million Americans who could potentially work from home:

- 30% would prefer to never come into the office during the week.
- 60% want a blend of working one to four days per week at home.
- 10% prefer working all five days in the office.

If everyone's wish is granted, something like 54 million U.S. workers will need to be able to work securely from home at least one day a week, even after the COVID-19 pandemic subsides. If you add in similar figures for other countries around the world you get… a really, really big number.

We added a question to this year's survey about what technologies and architectures enterprises are deploying to cope with this imperative (see Figure 45).

Section 4: Practices and Strategies

The top two responses, each selected by about half the respondents, were those steady workhorses, anti-virus and endpoint security software (51.9%) and virtual private network (VPN) technology (49.7%). Anti-virus and various flavors of endpoint detection and response solutions are still considered key elements in a defense-in-depth strategy, and are likely to retain that status well into the future. However, we think the use of VPNs may fall off in coming years as organizations adopt a variety of alternative network encryption methods that are easier to manage.

Software-defined wide area networks (SD-WANs) are used by 43.5% of organizations to help protect home workers. Besides ensuring that network traffic from remote locations travels over encrypted channels, many SD-WAN products contribute to security with built-in firewall, intrusion detection, and anti-malware features.

Network access control (NAC) and mobile device and application management (MDM/MAM) solutions are deployed by 42.8% and 40.5% or the organizations in our survey, respectively. These technologies prevent unauthorized connections to networks by enforcing access control policies, supporting advanced forms of authentication, and confirming that required security defenses are installed and active on computers and mobile devices.

Secure access service edge (SASE) architectures and ZTNA frameworks are seen as helping to protect remote employees in 39.5% and 34.5% of organizations. We will be discussing them more (along with SD-WANs) on page 54.

"Something like 54 million workers in the USA will need to be able to work securely from home at least one day a week... If you add in similar figures for other countries around the world you get… a really, really big number."

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.

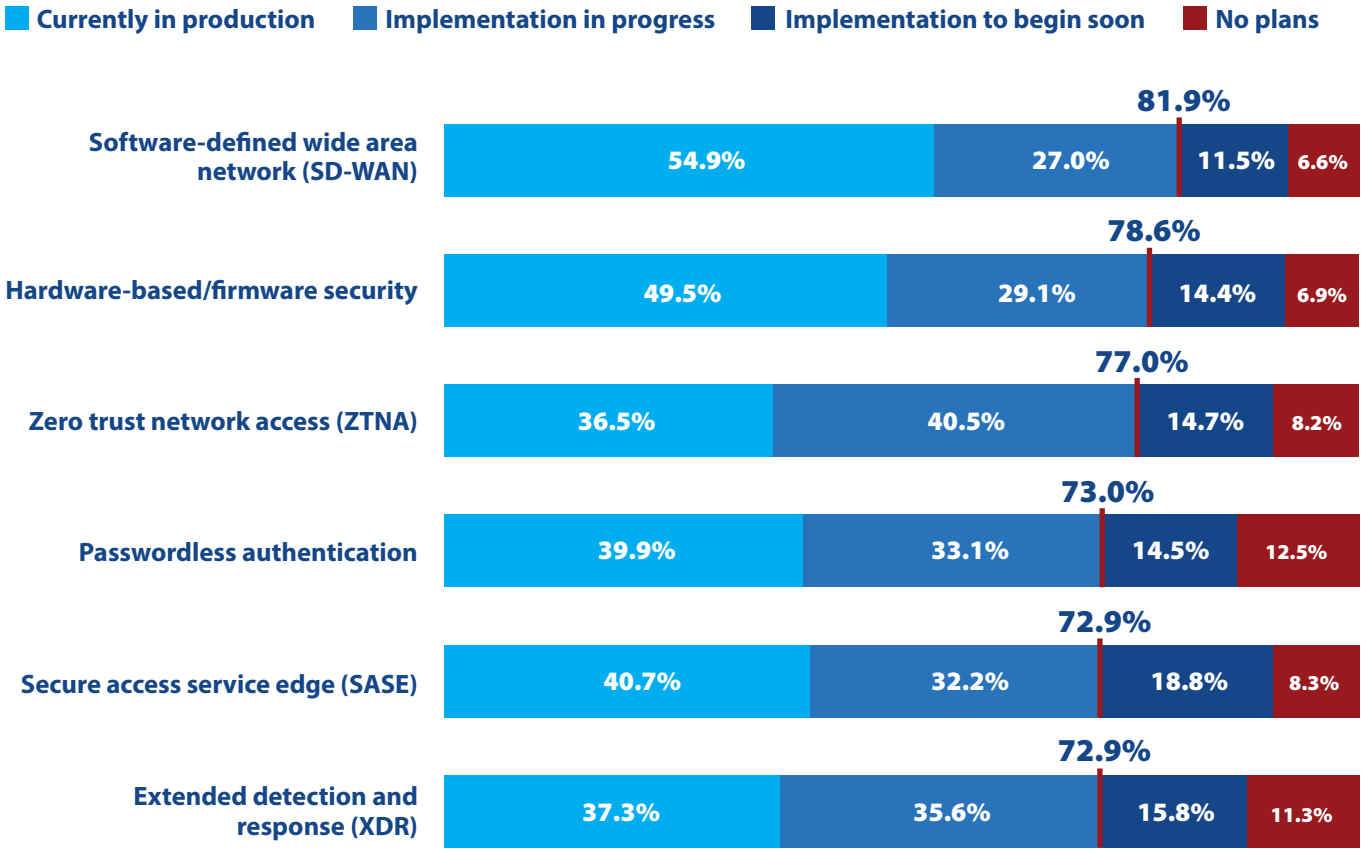

Figure 46: Plans for implementing emerging IT security technologies and architectures.

The final topic in this 2022 edition of the Cyberthreat Defense Report is a look at deployment plans for six emerging technologies and architectural approaches to security (see Figure 46).

The technology at the top of the list for "currently in production" plus "implementation in progress" is software-defined wide area network (SD-WAN). SD-WAN products allow enterprises to replace dozens or hundreds of individually configured routers and expensive MPLS circuits with simple broadband connections to the internet. Besides cutting networking costs, they dynamically route high-priority traffic to faster links and provide higher levels of redundancy. To strengthen security, they encrypt network traffic and sometimes enforce firewall and intrusion prevention rules. With all these advantages, it is not surprising that SD-WANs are in production or being implemented in four out of five organizations (81.9%).

Section 4: Practices and Strategies

"These emerging technologies and architectures can help your organization move toward more integrated, effective, and economical IT security. If you are not familiar with any of them, we hope this report will prompt you to investigate."

Second on this list is hardware-based and firmware security, which is in production or implementation stages at 78.6% of organizations. This category refers to security features that are embedded in chips or firmware, and therefore cannot be tampered with even if attackers take control of operating systems and hypervisors. Hardware-based and firmware security features can check at bootup to make sure operating systems and other software modules have not been corrupted or changed. They can also securely store cryptographic keys and provide cryptographic services to applications.

Zero trust network access is also being implemented or used in more than three-quarters (77.0%) of organizations. ZTNA is a security framework that reduces network security risks by removing implicit trust of users on LANs and internal networks and enforcing strict user and device authentication for everyone. Also, ZTNA solutions restrict users to only the applications and systems to which they have been explicitly granted access. ZTNA is proving very popular. Between the last survey and this one, the "currently in production" figure for ZTNA rose 6.3%, from 30.2% to 36.5%.

Passwordless authentication is currently in production or being implemented in 73.0% of organizations. This solution involves technologies and standards that provide effective, convenient authentication without the use of passwords or other memorized credentials. Authentication factors can include one-time codes sent to smartphones, hardware tokens, fingerprints, facial features, voices, retinal patterns, behavioral patterns, gestures, and even pressure on keyboard keys. Passwordless authentication techniques significantly reduce security risks (including the use of passwords for multiple accounts) and lower the costs of password reset and other support tasks. We expect their use to grow.

Secure access service edge (SASE) is a cloud architecture that combines SD-WAN and other key networking concepts with security functions such as firewall as a service (FaaS), secure web gateway (SWG), cloud access security broker (CASB), and features that support ZTNA. In fact, there are so many elements in the SASE model that no one organization is ever likely to implement all of them. But the model provides excellent guidance to enterprises and vendors that want a long-term plan for implementing and integrating essential networking and security services, so it is now being adopted at 72.9% of organizations.

The final item on this list is extended detection and response (XDR), also in production or being implemented in 72.9% of organizations. XDR platforms collect and correlate data from multiple security threat detection and incident response tools across an entire enterprise.

All these emerging technologies and architectures can help your organization move toward more integrated, effective, and economical IT security. If you are not familiar with any of them, we hope this report will prompt you to investigate.

The Road Ahead

Russia, Ukraine, Cyberwar, and Cyber Preparedness

These paragraphs are being written during the first weeks of Russia's invasion of Ukraine. So far, cyberwarfare, including attacks on Ukrainian government agencies and banking institutions and the dissemination of data-wiping malware, have played a relatively minor role in the conflict. While it is impossible at this point to know how the invasion will end or the part cyberattacks will play, we can make a few predictions about the effect it will have on security teams and the cybersecurity industry.

The invasion is ringing alarm bells across the world, not because we have learned anything new about the damage cyberwarfare can cause, but because we have been forced to reassess the likelihood that cyberwarfare will be used in future conflicts. A few weeks ago, it seemed unthinkable that a nation like Russia would launch a brutal, unprovoked invasion of a neighbor, with cyberattacks as one component. Today, how can we believe that future adversaries will hold back from unleashing one of the most powerful weapons in their arsenal, especially if they have fewer conventional arms than Russia?

Clearly, one likely effect is that national governments will become more aggressive in promoting, and often mandating, expanded cyber preparedness standards for both government agencies and commercial enterprises. They will widen the definition of "critical infrastructure" to include not only power grids, financial networks, energy pipelines, and transportation equipment, but also networks and organizations that capture and communicate digital information, facilitate supply chains, provide healthcare, and perform other necessary functions. Look also for governments to encourage, and often require, better and faster information sharing between organizations about cyberthreats.

There will be more pressure on security teams to prepare and test detailed incident response and business continuity plans so they can respond quickly to the types of attacks likely to be launched during cyberwarfare. There will also be more scrutiny of unglamorous but essential processes like backup and recovery, vulnerability scanning, and identity management.

We also expect heightened interest in threat intelligence relative to state-controlled hacker groups. Many organizations that have been focusing on blocking cybercriminals with financial motivations will need to put more emphasis on bad actors working toward military and political goals. There will be a premium on up-to-date information about the TTPs of groups who might conduct cyberwars.

Similarly, cybersecurity vendors will want to recalibrate their products and services toward thwarting the attacks expected in cyberwarfare. Cybercriminals and cyberwarriors use many of the same tools, but their targets, techniques, and objectives differ. It is still vital to protect personal data and credit card information, but there are going to be a lot of market opportunities in the near future for defending trains, planes, container ships, pipelines, factories, medical equipment, GPS systems, self-driving vehicles, media outlets, and first responder and emergency response systems.

The Effects of COVID-19 Continue to Play Out

In 2020 and 2021 security professionals scrambled to cope with the sudden disruptions caused by the COVID-19 pandemic. Their main focus was upgrading security for the huge surge of people working from home, often with unmanaged devices located far outside the corporate firewall and other perimeter defenses, and using new technologies to communicate and collaborate. In many industries, COVID-19 response also involved paying additional attention to the security of web and mobile applications as face-to-face interactions diminished and more and more activities and transactions were accomplished entirely by computer or smartphone. In addition, security staff and other IT personnel had to learn how to work effectively from their own homes, with all the attendant distractions.

The scrambling isn't so frantic anymore, but it has become clear

The Road Ahead

that many of the effects of COVID-19 on the workplace are not going to be reversed. As mentioned on page 52, in a recent Gallup survey, 90% of American workers want to continue to work at least one day a week at home (of which 30% prefer full-time WFH). And consumers are going to keep shopping, studying, sightseeing, and schmoozing in pajamas (at least below the waist).

We are expecting many of the technologies and programs initiated or accelerated because of the pandemic to stay on the front burner. These include:

- Enhancing security and ease of use for remote workers by applying ZTNA concepts
- Increasing the security of BYOD programs and mobile apps
- Improving visibility and security of applications, data, and identities housed on cloud platforms
- Combining security and network management by implementing SD-WANs and SASE architectures
- Building security into web and mobile apps through DevSecOps practices and security training for developers
- Increasing the security awareness of employees and other end users so they are less susceptible to phishing, social engineering, BEC, and ransomware attacks

Ransomware Might Be Topping Out

We are going to go out on a limb here. The ransomware industry may have peaked, or at least be approaching its peak. True, the number of organizations victimized continues to rise (see page 21). True, exfiltrating data gives ransomware gangs another club to hold over the heads of victims. And true, the gangs have gotten better at finding new categories of victims (such as hospitals, schools, and local governments) and at judging what the market will bear regarding their ransom demands.

But the industry is starting to become a victim of its own successes, in that ransomware is now a top-of-mind issue for businesses, governments, and law enforcement agencies. For example, national governments have been implementing plans to harden security for agencies, expand police powers and increase criminal penalties, create new cybersecurity standards for businesses, prevent funds (primarily ransoms in the form of cryptocurrencies) from reaching attackers, and mandate information sharing among private, public, and law enforcement organizations. Examples include the US government's Executive Order on Improving the Nation's Cybersecurity, the Australian government's Ransomware Action Plan, and the international Counter Ransomware Initiative.

Equally important, law enforcement agencies have finally begun to take direct action against the bad actors. Notably, Russia's FSB conducted a round-up of members of the REvil ransomware gang, and Europol has helped facilitate arrests in Ukraine, Romania, Kuwait, and other countries.

These are just the first steps, but they are significant. Until recently, participants in the ransomware industry were essentially immune from punishment. Now, they must take into account a serious possibility that they might be arrested and prosecuted. Also, CEOs and boards of directors of enterprises of all sizes and in all industries are putting direct pressure on their IT security teams to do everything possible to thwart ransomware attacks. In addition, security solution vendors are gearing up to deliver technologies that will help.

Looking at the big picture, we think there is good reason to believe that the growth curve of the ransomware industry will start to turn down in 2022, or at least 2023.

Third-party Risks Will Be Top of Mind

We discussed on page 13 that third-party risk management (TPRM) is one of the security capabilities that most of our survey respondents are least confident about. We believe that their concern is well founded, and that over the next couple of years enterprises will be paying more attention than ever to vulnerabilities and risks created by third parties. They include risks that:

The Road Ahead

- Suppliers, contractors, and other third parties could be hacked or bribed into giving up credentials that attackers can use to access an organization's applications and data.
- Equipment and software from third parties might contain vulnerabilities that can be used to penetrate networks.
- Third-party scripts that run in browsers could be compromised and allow threat actors to capture credentials and data from customers and employees.

The second bullet is undoubtedly the most visible of those issues now, because of the vulnerabilities in the Apache Log4j software and recent memories of the backdoor in SolarWinds software. For this and other reasons, we think that in the near future, organizations will expend significantly more effort monitoring and managing third-party risks.

For the IT Skills Shortage, Necessity Can Be the Mother of Invention

As we noted on pages 15 and 24 and elsewhere in this report, a shortage of skilled IT security professionals is a serious problem for almost every organization and the biggest single impediment to improving the performance of security teams. This shortage has been getting worse, and it is increasingly clear that supply may not catch up to demand in our lifetimes.

But as Plato said in The Republic: "our need will be the real creator" (later loosely translated as "necessity is the mother of invention"). When the need is pressing, people find answers. We have discussed several in this report:

- Training new security professionals and upgrading the skills of existing ones
- Outsourcing selected security tasks to MSSPs
- Automating security tasks so experts can focus on more-strategic work

But we predict that security groups will also try creative new ideas. Redefine security jobs to make them more attractive? Make better use of part-time employees and freelancers for specific tasks? Recruit and train candidates from overlooked groups? Run apprenticeship programs with local schools and colleges? Crowdsource good ideas? Recruit gamers with VR cybersecurity games and simulations?

We don't know what will succeed, but we think if some of the really smart people in cybersecurity put their minds to it, we can put a dent in this serious problem.

Communicating Security Issues to Management and Boards

As we mentioned on page 43, this year we added a response about cyber risk management and reporting to our question about security management and operations technologies – and found that it is already the second-most popular item on our list.

There is no doubt that CEOs and boards of directors are giving unprecedented attention to IT security issues. That means that IT management and security teams are under pressure to do a better job of explaining their work, aligning security programs with business objectives, and justifying investments in people and technology in terms of benefits to the business (not just by the number of vulnerabilities fixed or the indicators of compromise detected).

We think IT organizations are going to demand more, better, and easier ways to collect security data and present it to executives and boards in the context of business issues, and where possible, quantify risk reduction. And we expect security solutions vendors to respond by improving management reporting capabilities in existing security products and by delivering new solutions and services aimed specifically at compiling and presenting risk-based data to help manage security programs.

The Road Ahead

More Innovative Technologies

Here are other innovative concepts and technologies that we expect to hear more about in 2022 and beyond:

- **API gateway and protection products** help organizations protect applications designed with microservices and cloud-native architectures (see page 40). API gateways sit in front of application APIs and perform tasks such as enforcing authorization and encryption policies, scaling resources when traffic spikes, rate limiting to mitigate DDoS attacks and other forms of abuse, and sending usage data to billing systems. API protection solutions provide security teams with tools to understand, detect, and respond to attacks targeting APIs. Their capabilities can include mapping the attack surface to create an inventory of legitimate, rogue, and forgotten ("zombie") APIs, blocking injection attacks and other exploits, analyzing attacker behaviors, and fingerprinting attackers so they can be tracked even when they change IP addresses. API protection solutions can also help security teams correlate and analyze data across multiple data centers and cloud platforms. In the future, more threat actors are going to be targeting APIs with more sophisticated attacks, which will make API gateways and API protection products increasingly essential for well-rounded security programs.
- **Hardware- and firmware-based security solutions** prevent rootkits and other types of malware from corrupting operating systems and firmware and from capturing encryption keys. They can play a part in thwarting ransomware attacks and detecting vulnerabilities and misconfigurations in unmanaged BYOD devices and in systems acquired from third parties.
- **Tools for hybrid cloud and multi-cloud environments** will be a growth area. On page 28 we discussed security challenges facing organizations that have spread computing workloads over multiple data centers and private and public clouds. These challenges are going to become more pressing. As security vendors respond, we will see more products that offer "single pane of glass" monitoring and unified policy enforcement across all (or at least most) of the popular data center and cloud platforms.
- **Better security for operational technology (OT)** and the Internet of Things (IoT) is desperately needed to protect utilities, critical infrastructure, and manufacturing plants, as well as emerging applications for smart devices, from cybercriminals, ransomware gangs, and hackers sponsored by hostile militaries. As we discussed on page 12, governments have started to pay more attention to this, and even to fund research and development, and we expect to see progress over the next couple of years.
- **Deepfake detection technology** is still in its early phases, but will become very important as threat actors master sophisticated techniques for creating convincing deepfakes: images and recordings digitally altered to present a known person doing or saying something they did not do or say. Deepfakes have already been involved in a small number of BEC attacks (e.g., phone calls supposedly from the CEO ordering a subordinate to transfer money to a phony supplier). Unfortunately, there are numerous opportunities for deepfakes to enhance phishing and misinformation campaigns, attacks on brands, and many other malicious activities.

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

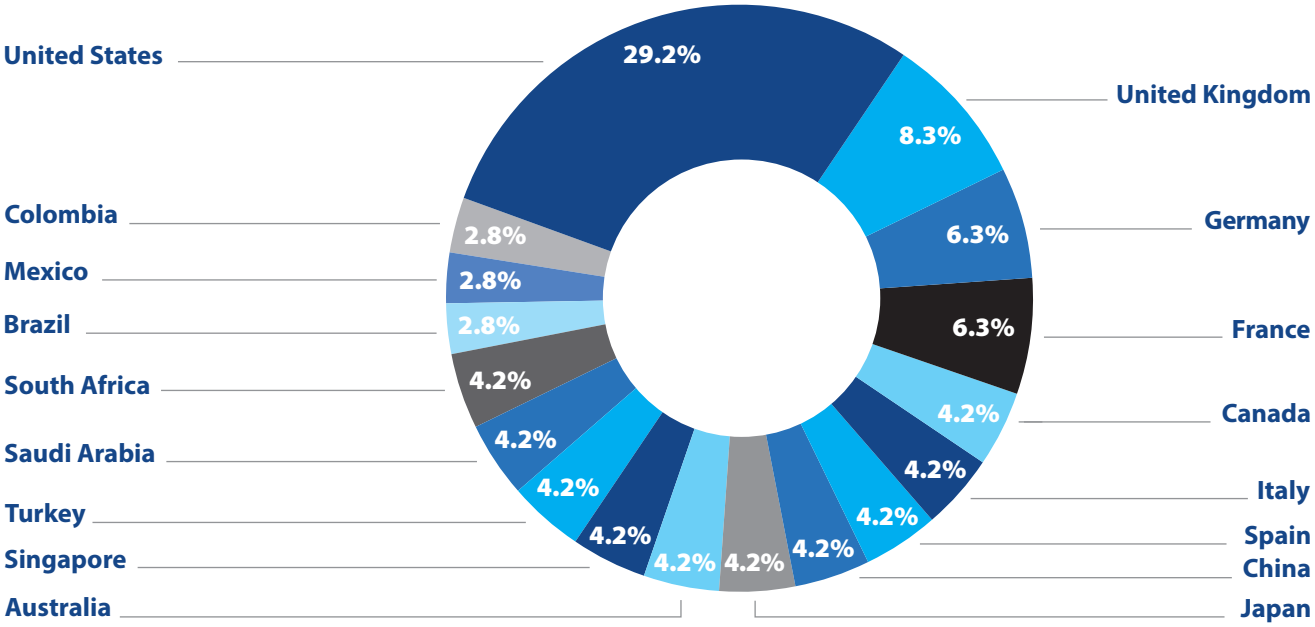

Figure 47: Survey participation by country.

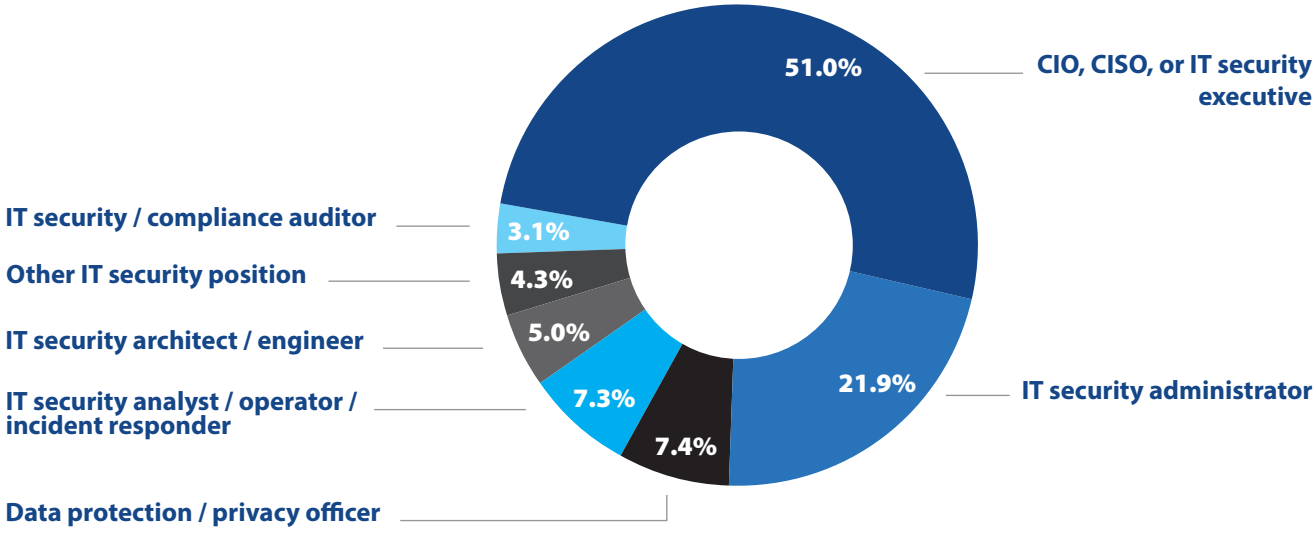

Figure 48: Survey participation by IT security role.

Appendix 1: Survey Demographics

This study addresses perceptions and insights from research participants employed by commercial and government organizations with 500 to 25,000+ employees (see Figure 49). A total of 19 industries (plus "Other") are represented in this year's study (see Figure 50). The "big 7" industries – education, finance, government, healthcare, manufacturing, retail, and telecom and technology – accounted for nearly two-thirds of all respondents. No single industry accounted for more than 15.1% of participants.

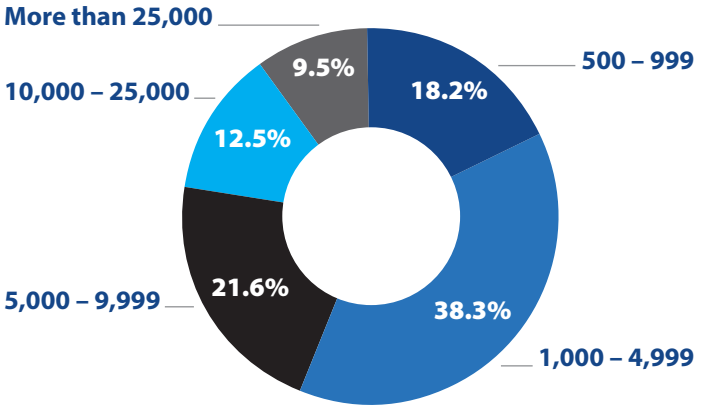

Figure 49: Survey participation by organization employee count.

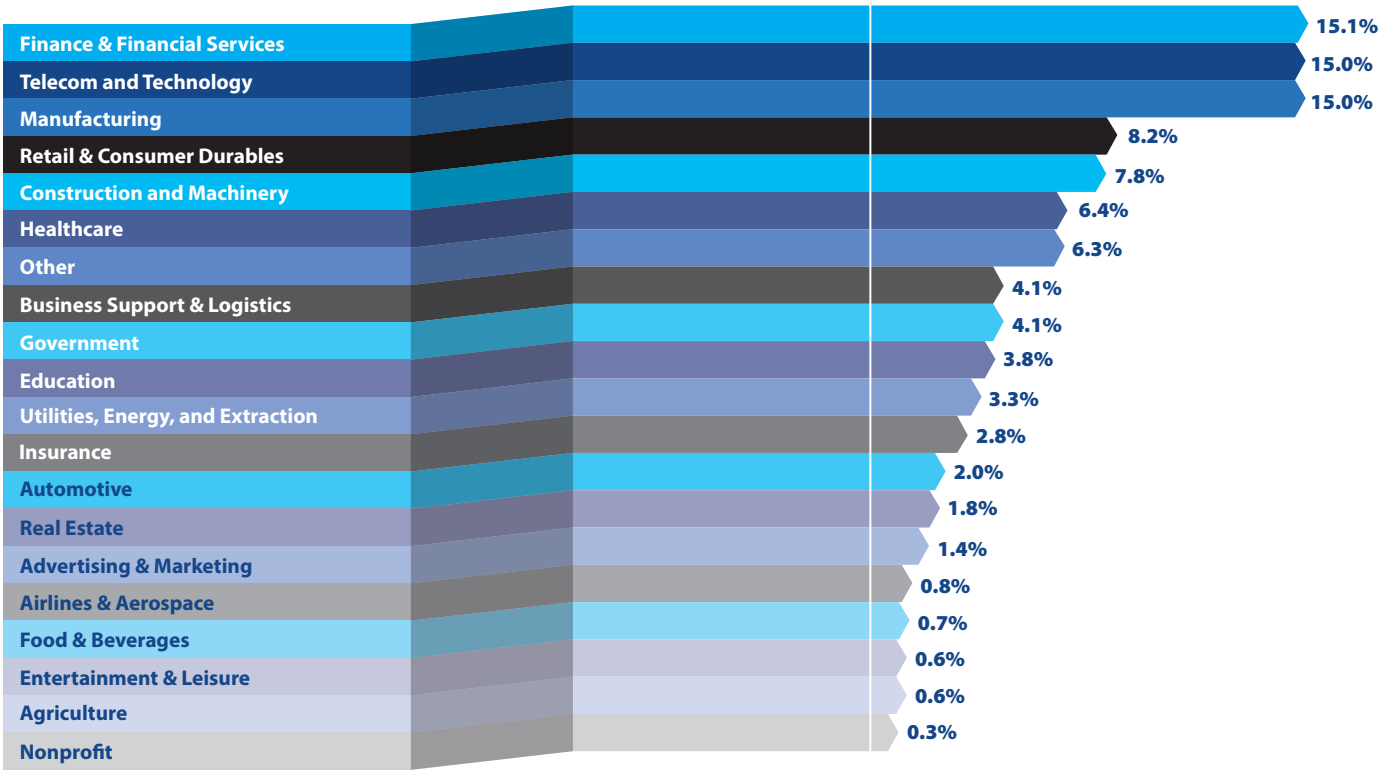

Figure 50: Survey participation by industry.

Appendix 2: Research Methodology

CyberEdge developed a 27-question, web-based, vendor-agnostic survey instrument in partnership with our research sponsors. The survey was promoted via email to 1,200 IT security professionals in 17 countries and 19 industries in November 2021. The global survey 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 survey 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

(ISC)² | www.isc2.org

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, more than 160,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the public through our charitable foundation – The Center for Cyber Safety and Education.

Gigamon | www.gigamon.com

Gigamon helps the world's leading organizations run fast, stay secure and innovate. We provide the industry's first elastic visibility and analytics fabric, which closes the cloud visibility gap by enabling cloud tools to see the network and network tools to see the cloud. With visibility across their entire hybrid cloud network, organizations can improve customer experience, eliminate security blind spots, and reduce cost and complexity. Gigamon has been awarded over 125 technology patents and enjoys world-class customer satisfaction with more than 4,000 organizations, including over 80 percent of the Fortune 100 and hundreds of government and educational organizations worldwide.

Imperva | www.imperva.com/

Imperva is a cybersecurity leader with a mission to protect data and all paths to it. We protect the data of over 6,000 global customers from cyber attacks through all stages of their digital transformation. Our products are informed by the Imperva Research Lab, a global threat intelligence community, that feeds the latest security and compliance expertise into our solutions.

Menlo Security | www.menlosecurity.com

Menlo Security enables organizations to outsmart threats, completely eliminating attacks and fully protecting productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure zero-trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.

PerimeterX | www.perimeterx.com

PerimeterX is the leading provider of solutions that detect and stop the abuse of identity and account information on the web. Its cloud-native solutions detect risks to your web applications and proactively manage them, freeing you to focus on growth and innovation. The world's largest and most reputable websites and mobile applications count on PerimeterX to safeguard their consumers' digital experience while disrupting the lifecycle of web attacks.

ThreatX | www.threatx.com

ThreatX's API protection platform makes the world safer by protecting APIs from all threats, including DDoS attempts, BOT attacks, API abuse, exploitations of known vulnerabilities, and zero-day attacks. Its multi-layered detection capabilities accurately identify malicious actors and dynamically initiate appropriate action. ThreatX effectively and efficiently protects APIs for companies in every industry across the globe.

Appendix 3: Research Sponsors

Gold Sponsors

Aqua Security | www.aquasec.com

Aqua Security is the largest pure-play cloud native security company, providing customers the freedom to innovate and accelerate their digital transformations. The Aqua Platform is the leading Cloud Native Application Protection Platform (CNAPP) and provides prevention, detection, and response automation across the entire application lifecycle to secure the supply chain, secure cloud infrastructure and secure running workloads wherever they are deployed. Aqua customers are among the world's largest enterprises in financial services, software, media, manufacturing and retail, with implementations across a broad range of cloud providers and modern technology stacks spanning containers, serverless functions and cloud VMs.

Attivo Networks | www.attivonetwork.com

Attivo Networks, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Attivo has 180 awards for technology innovation and leadership.

ConnectWise | www.connectwise.com

ConnectWise is an IT software company that empowers Technology Solution Providers to achieve success in their As-a-Service business with intelligent software, expert services, an immersive IT community, and a vast ecosystem of integrations. The unmatched flexibility of the ConnectWise platform fuels profitable, long-term growth for our Partners. With an innovative, integrated, and security-centric platform, ConnectWise enables TSPs to drive business efficiency with business automation, IT documentation, and data management capabilities. And increase revenue using remote monitoring, security, and backup disaster recovery technologies.

Delinea | www.delinea.com

Delinea is a leading provider of privileged access management (PAM) solutions that make security seamless for the modern, hybrid enterprise. Our solutions empower organizations to secure critical data, devices, code, and cloud infrastructure to help reduce risk, ensure compliance and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide, including over half of the Fortune 100. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies.

LookingGlass | www.lookingglasscyber.com

LookingGlass Cyber Solutions develops cybersecurity solutions that empower organizations to meet their missions and reduce cyber risk with a comprehensive view of their attack surface – outside-in and inside-out – layered with actionable threat intelligence. By linking the risks and vulnerabilities from an organization's attack surface to customized threat actor models, LookingGlass Cyber Solutions provides a more accurate view of cyber risk and enables systematic definition and deployment of mitigations to defend against the threats that matter.

Netsurion | www.netsurion.com

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward.

PhishLabs | www.phishlabs.com

PhishLabs by HelpSystems is a cyber threat intelligence company that delivers Digital Risk Protection through curated threat intelligence and complete mitigation. Specialized teams use threat-specific technology and operations to safeguard critical digital assets and protect against brand impersonation, account takeover, social media, data leakage, and advanced email threats across the digital landscape. Developed over a decade in partnership with the world's leading brands and companies, the PhishLabs Platform is the foundation of our Digital Risk Protection solution, providing comprehensive collection, expert curation, and complete mitigation of digital risks.

Appendix 3: Research Sponsors

Silver Sponsors

Agari | www.agari.com

Agari protects brands, customers and employees from devastating phishing and socially engineered attacks. Using an identity-centric approach that uniquely learns sender-receiver behavior, Agari builds a model of trust that protects the workforce from inbound business email compromise, supply chain fraud, spear phishing, and account takeover-based attacks, reducing business risk. Agari also prevents spoofing of outbound email from the enterprise to customers, increasing deliverability and preserving brand integrity. With Agari you can restore trust to your inbox.

Binary Defense | www.binarydefense.com

Binary Defense is a managed security services provider and software developer with proprietary cybersecurity solutions that include SOC-as-a-Service, Managed Detection & Response, Security Information & Event Management, Counterintelligence and Threat Hunting. Binary Defense uses a human-driven, technology-assisted approach to provide their clients with immediate protection and visibility, combating and stopping the next generation of attacks that their business faces. Recognized as a "Leader" on The Forrester Wave: Managed Detection and Response, Q1 2021 report, the Ohio-based organization earned high marks for threat hunting and threat intelligence. Visit BinaryDefense.com/Forrester to learn more.

Drawbridge | www.drawbridgeco.com

Drawbridge is a specialized technology firm providing comprehensive cybersecurity solutions to the financial services and alternative investment communities. Drawbridge's unique all-in-one platform and tech-enabled professional services provide firms with foundational, turnkey solutions that scale as their businesses evolve. With over 800 clients, Drawbridge has quickly become the leading provider among private equity firms, hedge funds, and venture capital firms.

Eclypsium | www.eclypsium.com

Eclypsium is the firmware security company. Eclypsium's SaaS platform identifies, verifies and fortifies firmware throughout networks and technology supply chains, from endpoints and servers to network gear and connected devices. Eclypsium secures networks against stealthy firmware attacks, provides continuous firmware monitoring, patches firmware at scale, and prevents firmware-level ransomware and implants from crippling your organization. Eclypsium serves Global 2000 enterprises and federal agencies, was named a Gartner Cool Vendor, and is one of Fast Company's 10 Most Innovative Security Companies.

Netwrix | www.netwrix.com

Netwrix makes data security easy thereby simplifying how professionals can control sensitive, regulated and business-critical data, regardless of where it resides. More than 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, pass compliance audits with less effort and expense, and increase the productivity of IT and security teams. Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

SailPoint | www.sailpoint.com

SailPoint is the leader in identity security for the modern enterprise. At the core of SailPoint Identity Security is artificial intelligence and machine learning. A foundation that protects organizations against cyber threats by automating the discovery, management, and control of ALL user access. SailPoint ensures that each identity, human or nonhuman, has the right access needed to do their job – no more, no less. We meet customers where they are with an intelligent identity solution that matches the scale, velocity and environmental needs of your business. Trusted by the world's largest, most complex organizations.

Telos | www.telos.com

Telos Corporation empowers and protects the world's most security-conscious organizations with solutions for cyber, cloud, and enterprise security. Telos' offerings include cybersecurity solutions for IT risk management and information security; cloud security solutions to protect cloud-based assets and enable continuous compliance with security standards; and enterprise security solutions for identity and access management, secure mobility, organizational messaging, and network management and defense. We serve organizations in financial services, healthcare, state and local government, education, and other highly regulated sectors; military, civilian and intelligence of the U.S. federal government, and allied nations around the world.

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. Today, approximately one in six IT security vendors (with $10 million or more in annual revenue) is a CyberEdge client.

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 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)
- API Security
- Application Security
- Cloud Security
- Data Security
- Deception Technology
- DevSecOps
- DoS/DDoS Protection
- Endpoint Security (EDR & EPP)
- Extended Detection & Response (XDR)
- Firmware Security
- ICS/OT Security
- Identity and Access Management (IAM)
- Intrusion Prevention System (IPS)
- Managed Detection & Response (MDR)
- 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 Orch., Automation, and Response (SOAR)
- Software-defined Wide Area Network (SD-WAN)
- SSL/TLS Inspection
- Supply Chain Risk Management
- Third-Party Risk Management (TPRM)
- Threat Intelligence Platforms (TIPS) & Services
- User and Entity Behavior Analytics (UEBA)
- Unified Threat Management (UTM)
- Virtualization Security
- Vulnerability Management (VM)
- Web Application Firewall (WAF)
- Zero Trust Network Access (ZTNA)

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

CyberEdge Acceptable Use Policy

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

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

1. **Report distribution.** Only CyberEdge and its authorized research sponsors are permitted to distribute this report for commercial purposes. However, organizations are permitted to leverage the report for internal uses, including training.
2. **Source citations.** When citing a textual and/or graphical element from this report, you must incorporate the following statement into a corresponding footnote or citation: "Source: 2022 Cyberthreat Defense Report, CyberEdge Group, LLC."
3. **Quotes and excerpts.** Quotes and excerpts extracted from this report must not be modified in any way. Rephrasing is not permitted.
4. **Figures and tables.** Figures and tables extracted from this report must not be modified in any way. Artwork for figures and tables for the most recent Cyberthreat Defense Report are available for download at no charge on the CyberEdge website at https://www.cyber-edge.com/cdr.
5. **No implied endorsements.** CyberEdge does not endorse technology vendors. Cited CyberEdge content should never be used to imply favor from CyberEdge.

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

HEAT attacks: The new era of web threats

Highly Evasive Adaptive Threats (HEAT) are currently evading multiple layers of security detection in current security stacks.

The result is the delivery of ransomware payloads and account takeovers. Discover how Menlo Security helps prevent these attacks and protect productivity, allowing your users to work without limits, while you work without worry.

Learn more at
menlosecurity.com

MENLO SECURITY