THE CISOS REPORT

PERSPECTIVES, CHALLENGES AND PLANS FOR 2022 AND BEYOND

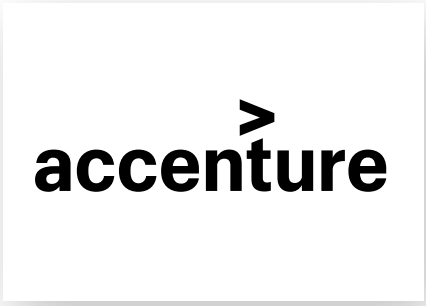
AimPoint Group

CISOs CONNECT

W2Communications

TABLE OF CONTENTS

SPONSORED BY



INTRODUCTION

The role of the Chief Information Security Officer (CISO) has evolved significantly over the past decade as cyber threats have diversified and proliferated. With IT now integral to every aspect of business and mission operations, CISOs carry great responsibility in the ongoing battle to keep their organizations safe from an endless stream of attacks.

Given how quickly both the attack surface and the threat environment change, it can be challenging for CISOs to keep up with what is happening beyond their home borders. To help, this study offers the kind of insights CISOs have long been asking for — to benchmark their situation and experience against others; to learn from what their peers are doing and planning to do; and to validate ideas and obtain solid data to justify investments in these areas.

METHODOLOGY

This study utilized a two-part methodology. First was a quantitative survey that was designed with guidance from a Board of CISOs working at private and public sector organizations in the United States, Canada, Europe, Australia and Asia. Respondents were recruited through direct relationship with CISOs Connect and from a well-screened panel. We received 411 survey completions from respondents identifying as CISOs or CISO-equivalent across a broad range of industry sectors. All responses were anonymous.

Additionally, we conducted in-depth discussions with members of our Board to get detailed perspectives on their experiences as CISOs defending their organizations from rampant cyber threats. These individuals are particularly known for their strong technical and business acumen. You will find insights and best practice recommendations from them throughout this report.

KEY FINDINGS

1. **The battle is not easing.** Ransomware, phishing/spear phishing, and supply chain attacks stand atop the list of threats that concern CISOs the most. The great majority of CISOs see the threat landscape as worse than a year ago; 75% confirm being hit during that period at least once but as many as five times by a cyber attack that caused material damage. Mid-sized organizations especially bear the brunt, with 67.5% of organizations having between 1,000 and 4,999 employees and 62.2% having between 5,000 and 10,000 employees being hit by multiple attacks that caused material damage. **However, no organization is safe from attack.**

2. **CISOs recognize current limitations.** They feel more confident in their ability to detect cyber attacks than to prevent or respond to them. They also struggle with quantifying the cybersecurity domain, from the ROI of their initiatives to the overall financial risks and even the cumulative impacts of an incident.

3. **A wide range of risks, led by supply chain vulnerabilities, cause CISOs worry.** Partners and suppliers are essential to the successful operation of businesses and organizations of all types and sizes, worldwide. However, our respondents report third parties as the top security risk to overcome. Trailing not far behind: unpatched software/systems, gaps in cloud security coverage, and configuration errors by IT administrators. Given conversations with our Board of experts, we expect to see IoT/IIoT moving up this list in the near future.

4. **APIs and data discovery and classification are prime for further attention.** CISOs rate the IT components most in need of security improvements as APIs (which have exploded in use over the last 2-3 years), Cloud apps (SaaS), and Cloud infrastructure (IaaS). The security processes they see most needing improvement include data discovery & classification, data backup & recovery, and DevSecOps. These lists reflect shifts in the IT landscape that have happened with the dramatic escalation of remote work, cloud adoption, BYOD and changing development practices.

5. **External impacts cause the greatest worries.** The impacts of cyber attacks that cause CISOs the most concern are exposure of PII or other sensitive data, and downtime for critical infrastructure or essential services. The consequences of disruption in these areas have the widest-ranging effects beyond the organization's walls. Concerns about them far outweigh internal impacts like financial loss, compliance actions or disrupted operations. A lack of skilled security personnel and too much data to manage are what limit CISOs from establishing better security defenses.

6. **Zero Trust is a *thing*.** Forget the hype cycle, CISOs say implementing or enhancing a Zero Trust model is the top security priority for the next 12 months. Nearly 79% indicate they are already underway with implementation, while another 18% are actively planning for it.

7. **There is strong interest in simplifying and streamlining.** The top capabilities and characteristics CISOs are looking for when purchasing a new security solution are ease of deployment and ease of use. Those are followed by high-fidelity alerts and analysis, and automation. These are all capabilities that will help busy CISOs and security teams to get more of the right things done, faster. Not so important is being part of a broader platform from a single provider.

8. **Top intended security investments map to the newest trends.** When combining projected spending for upgrades with that for new implementations, the security technologies that come out on top for the next 12 months include network/micro-segmentation, container security and security service edge (SSE) platform.

DETAILED FINDINGS

The State of Affairs: Today vs. a Year Ago

We began our exploration by asking respondents how they saw the current threat landscape as compared to one year ago. Unfortunately, but perhaps not surprisingly, things are not improving.

Compared to one year ago, which best describes your perceived level of the cyber threats currently facing your organization?

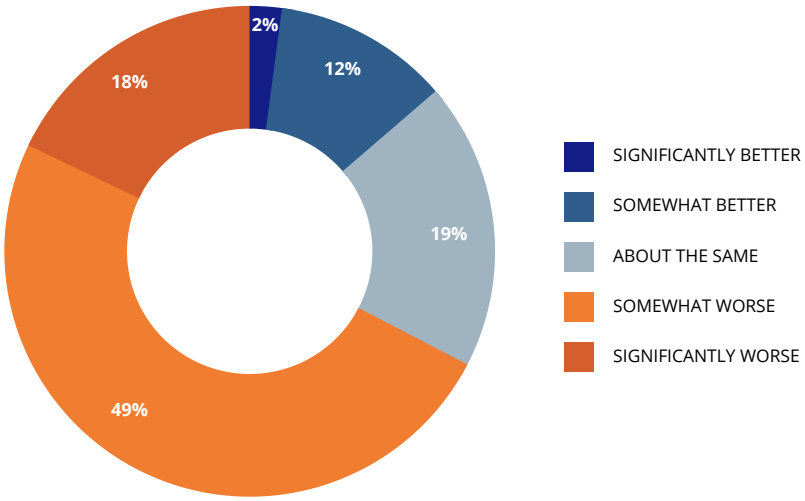


Figure 1. Perception of Threat Landscape — Present vs. 1 Year

Nearly 7 in 10 respondents perceive the threat landscape to be more severe now than it was a year ago. That is a sobering statistic, although such a perception may be at least somewhat influenced by when an organization was last hit and the level of resulting impact. In that case, many respondents would seem to have been hit recently. Just 12% of respondents think the threat landscape is somewhat improved. It is possible that the ransomware fever of a year ago may have lowered just a bit, contributing to this perception. Or, people may just be numbed by too many ransomware headlines.

Whatever the case, the world is now embroiled in a battle against a highly motivated, well-armed set of adversaries ready to exploit any opportunity or distraction. The Ukraine-Russia conflict is certainly having an impact. Our data collection commenced just a week before the conflict got underway. By the time we were finishing, respondents were indicating that the conflict was prompting a notable uptick in attacks — whether due to actual instances of cyber warfare, or opportunistic attackers looking to take advantage of such a disruptive event.

Also over the last year, almost half of respondents experienced material damage from an attack between two and five times, and one in ten experienced it more than five times. Only one in five "lucky" respondents had no material damage from an attack. Note again that this is backward-looking data reflecting the state of affairs prior to the geopolitical disruption in Ukraine.

In the past 12 months, how many times was your organization affected by a cyber attack that caused material damage?

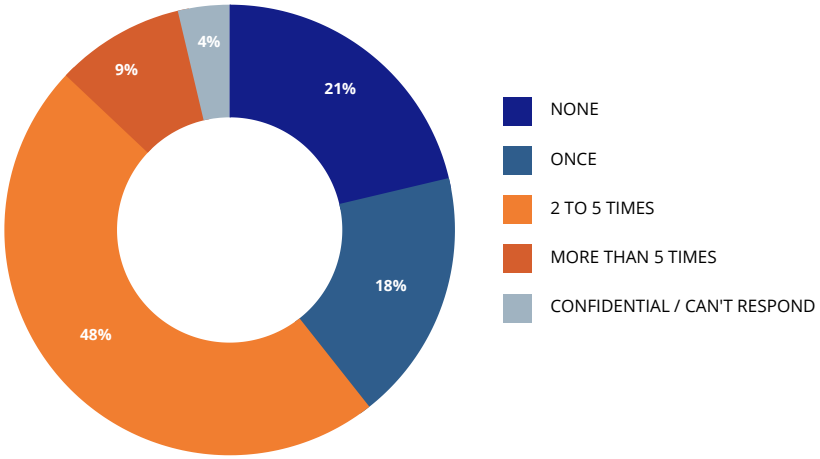


Figure 2. Number of Cyber Attacks Causing Material Damage in Past 12 Months

"I definitely think it's getting worse, especially with the geopolitical environment and everything that is going on in the world. We're seeing that a lot of battles will be fought in cyberspace."
– Christine Vanderpool, VP of IT Strategy, Architecture & Security, Florida Crystals Corporation

"Since the start of hostilities in Ukraine, I am seeing a significant uptick in probing. There seems to be a great deal of bot activity on the internet that is looking."
– Dr. Jorge Llano, CSO, New York City Housing Authority

Mid-sized organizations continue to be the most fruitful targets for threat actors, as we also found through our research for the 2021 Ransomware in Focus Report. Certainly **no organization should count itself as not significant enough to warrant an attack.** However, the focus on the mid-tier is presumably because smaller organizations have fewer valuables that entice attackers, while the largest organizations have greater security defenses to keep them safe.

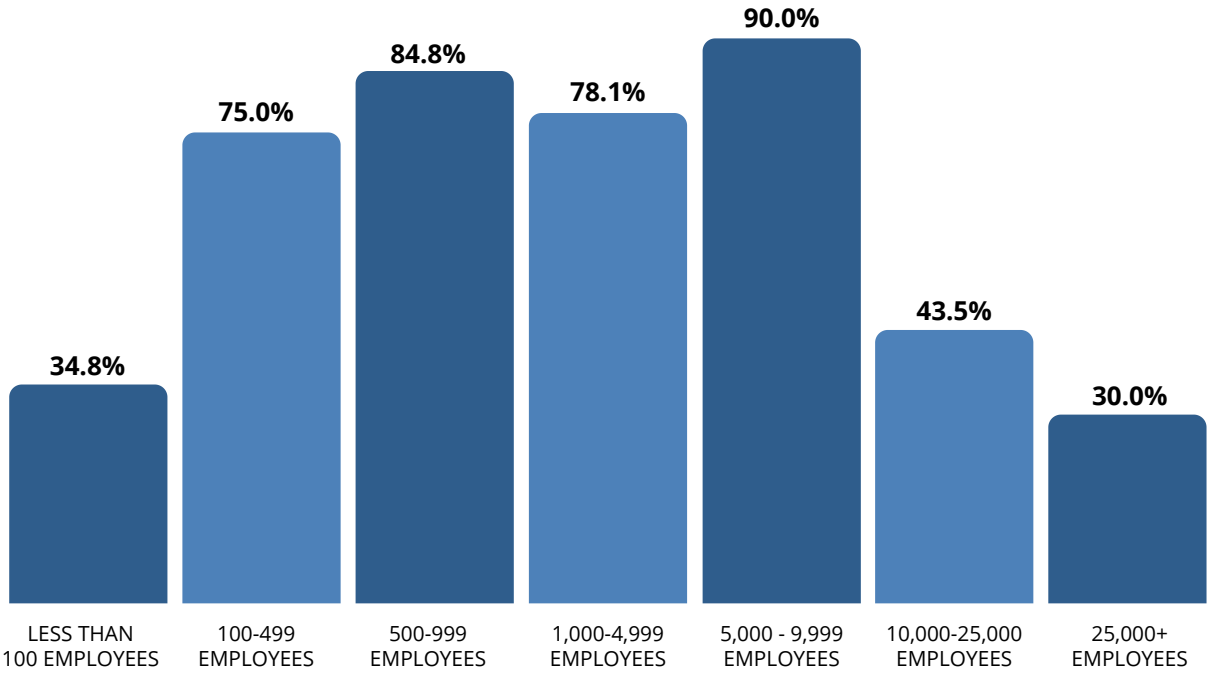


Figure 3. Percentage with Cyber Attacks Causing Material Damage — by Organization Size

In terms of the industry sectors at most risk, the Construction and Manufacturing sectors fared the worst, with 85% and 79%, respectively, having experienced at least one attack that caused material damage. These sectors have historically been less well-defended, and that distinction seems to continue. They are followed closely by Retail, with the online shopping environment being especially ripe for a barrage of attacks. While not the hardest hit, the heavily regulated Healthcare (at 65.1%) and Financial Services (at 63.6%) sectors still face a formidable threat environment.

Figure 4. Percentage with Cyber Attacks Causing Material Damage — by Industry

When we look at the data across geographic regions, the numbers reflect a general IT maturity curve that has persisted for decades. North America is in somewhat better shape, experiencing 22.5% fewer damaging attacks than European organizations, and 17.9% fewer than Asian-Pacific counterparts.

Figure 5. Percentage with Cyber Attacks Causing Material Damage — by Region

"You can buy best-of-breed tools and have deployed them perfectly, but you can still get attacked. So you've got to be prepared. You've got to have your disaster recovery written down really well. Your business continuity plans are really, really important. You have to do the tabletop exercises"
– Christine Vanderpool, VP of IT Strategy, Architecture & Security, Florida Crystals Corporation

Capabilities, Concerns and Limitations

We asked respondents for a self-assessment on where they are strong — and perhaps not as strong — when it comes to dealing with cyber attacks. Prevention understandably rates lowest (3.66 out of 5), given the volume and constant evolution of threats. How much room for improving defenses an organization perceives that it has may track with its recent experience of attacks that caused material damage, as well as the number of threats they see penetrating their defenses.

Detecting attacks is a bit more challenging because it's difficult to know what you didn't detect unless and until it manifests into something harmful. While respondents rate their capabilities in this area highest (3.88), that may be slightly over-estimating their actual performance. Response and recovery is where the most insight, understanding and control is possible. Yet surprisingly, CISOs rate their capabilities almost equal here (3.68) to prevention. Most CISOs should already have business continuity and disaster recovery plans at the ready; and last year's spike in ransomware attacks likely motivated organizations to bolster their preparations and response/recovery capabilities. Yet CISOs clearly feel they still have a ways to go in this area.

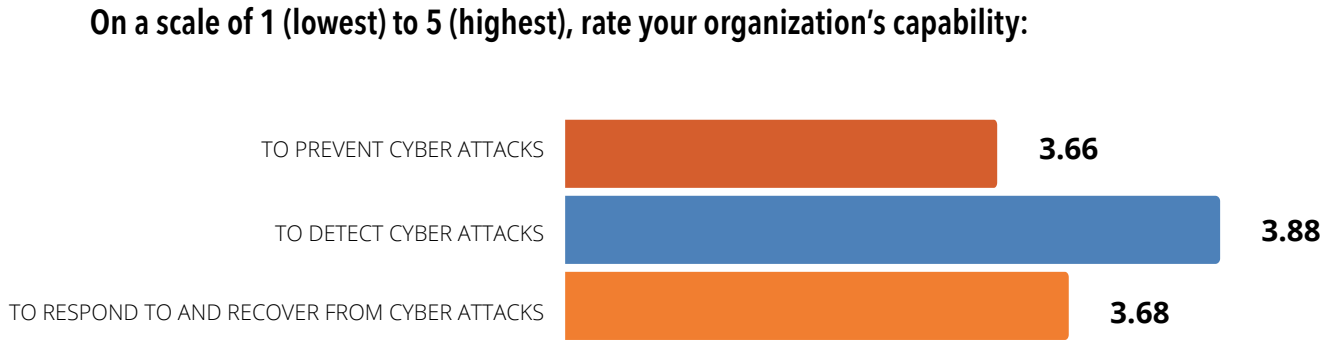


Figure 6. Cyber Attack Mitigation Capabilities — by Lifecycle Stage

"With the Internet of Things, more and more devices are coming. There will be a lot more thanks to 5G. The attack surfaces are increasing. And people plug anything in anywhere."
– CISO, large manufacturing corporation

"What we're seeing is threat actors have come up with a way to trigger low-level alerts across all of your environment. If you were to chain all of these together, you will see that you have malicious activity. Now, as we look at it as a blue team or red team exercise, we look at all of the low-level alerts of activity that are taking place, to see if we can interpret if it is unauthorized or malicious."
– Les McCollum, Executive Director and Chief Information Security Officer, University of Chicago Medical Center

Quantifying the return on cybersecurity investment remains a vagary, as measuring the cost of what didn't happen is a long-standing CISO challenge. The Factor Analysis of Information Risk (FAIR) methodology is a credible attempt at standardizing an international model for information security and operational risk. There is also greater involvement from insurance actuaries attempting to quantify what they are covering (or denying). Still, we are far from a common, acceptable measurement.

Respondents rate their ability to quantify the cumulative financial impact of an incident as the highest of the three capabilities posed, but that is still only a rating of 3.33 out of 5. When all is said and done with a particular incident, the numbers can be calculated, assuming the organization cares enough to invest in the mathematical effort. The CISO, whose job ultimately depends on keeping the organization cyber safe, may be less interested in that number — or conversely, could see it as an opportunity to justify additional future budget.

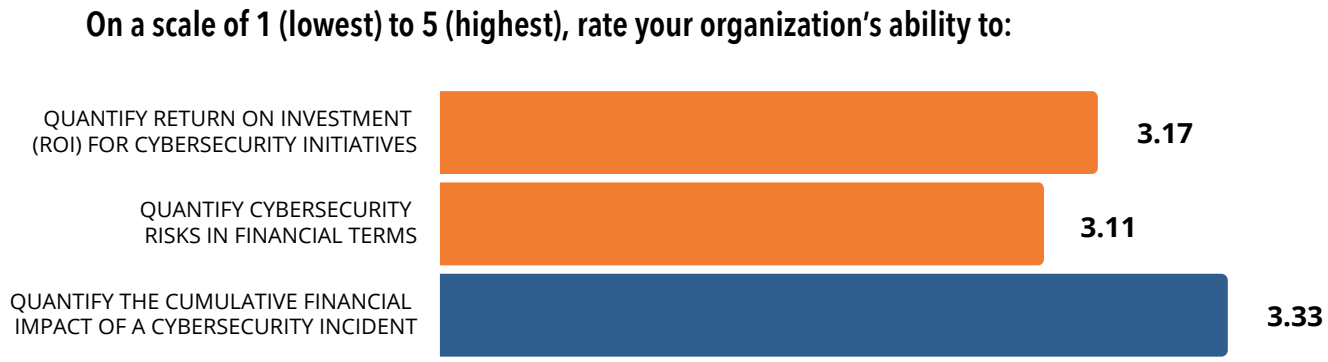


Figure 7. Ability to Quantify Cybersecurity in Financial Terms

"The complexity of digital transformation has presented us with such an expanded threat landscape that we can't anticipate all of the threats. As a result, we are taking a risk-based approach to our cyber strategy that looks at internal, external and operational risks."
– Les McCollum, Executive Director and Chief Information Security Officer, University of Chicago Medical Center

"You can buy best-of-breed tools and have deployed them perfectly, but you can still get attacked. So you've got to be prepared. You've got to have your disaster recovery written down really well. Your business continuity plans are really, really important. You have to do the tabletop exercises"
– Christine Vanderpool, VP of IT Strategy, Architecture & Security, Florida Crystals Corporation

With regard to which impacts of a cyber attack cause the greatest concern, exposure of sensitive data leads, with 65% of respondents indicating it is their highest concern. This situation has been exacerbated by the troubling trend in ransomware attacks for the attackers to steal data and threaten to expose it, even after a ransom is paid. Downtime for critical services comes in second (57.6%) given that the impacts will extend to customers and others dependent on those services. Interestingly however, productivity loss, which would be an internal consequence of downtime (as well as other factors), comes in last (19.7%). That could be because disruption to a subset of internal users can be overcome by making up the lost time. What's more, productivity loss is not visible to those outside of an organization.

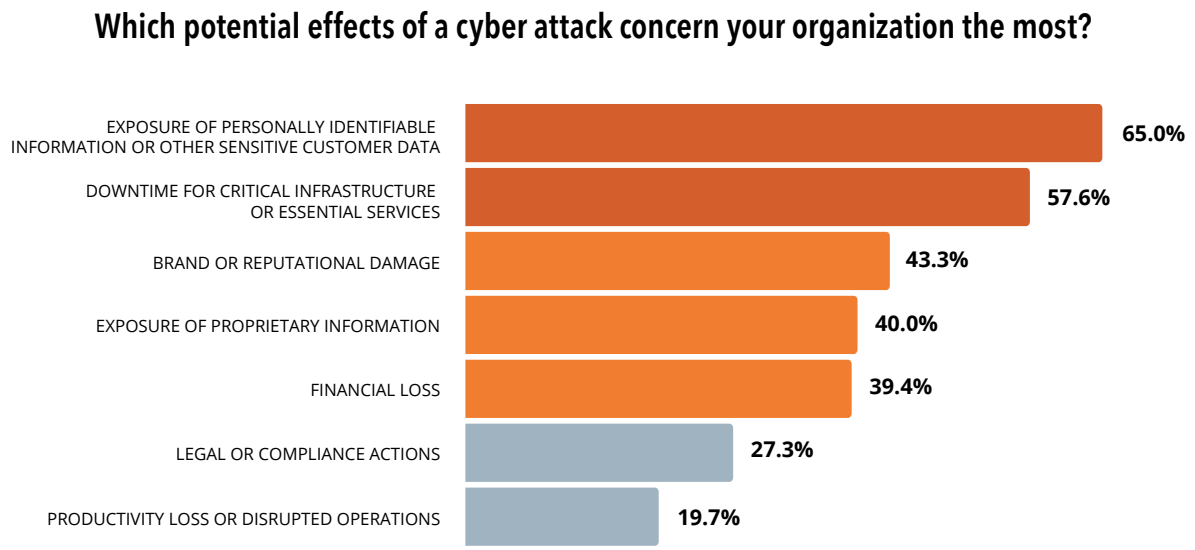


Figure 8. Greatest Impacts Feared from a Cyber Attack

When it comes to the types of cyber threats that are most worrying our respondents, there is a mere 1/3 point differential between ransomware, which tops the list at a rating of 4.06, and social media poisoning, holding the lowest position with a rating of 3.71. In other words — everything on this list deserves attention!

> "(As CISOs) we have been so focused on ransomware, we've almost taken our eye off the ball of regular malware and viruses. We're starting to see some really sophisticated ones that are very low and slow and quiet in the way they proliferate. It's really important to always keep your eye on all the different potential types of attacks, and not just focus on the big one that's in the news."
> *– Christine Vanderpool, VP of IT Strategy, Architecture & Security, Florida Crystals Corporation*

It is clear that phishing (4.0) and account takeover (3.81) go hand-in-hand — as phished credentials are what enable many ATO attacks. Client-side web app attacks (3.79) are a rising concern, particularly for the ecommerce sector, which reinforces Retail's third-place ranking among sectors experiencing materially damaging attacks (see Figure 4). And while certainly not new, social media poisoning (3.71), an insidious and less obvious threat aimed at discrediting or tarnishing a brand, is also on the rise, given the ever-growing usage of social media. Sadly, malicious insiders also still make this list (3.72).

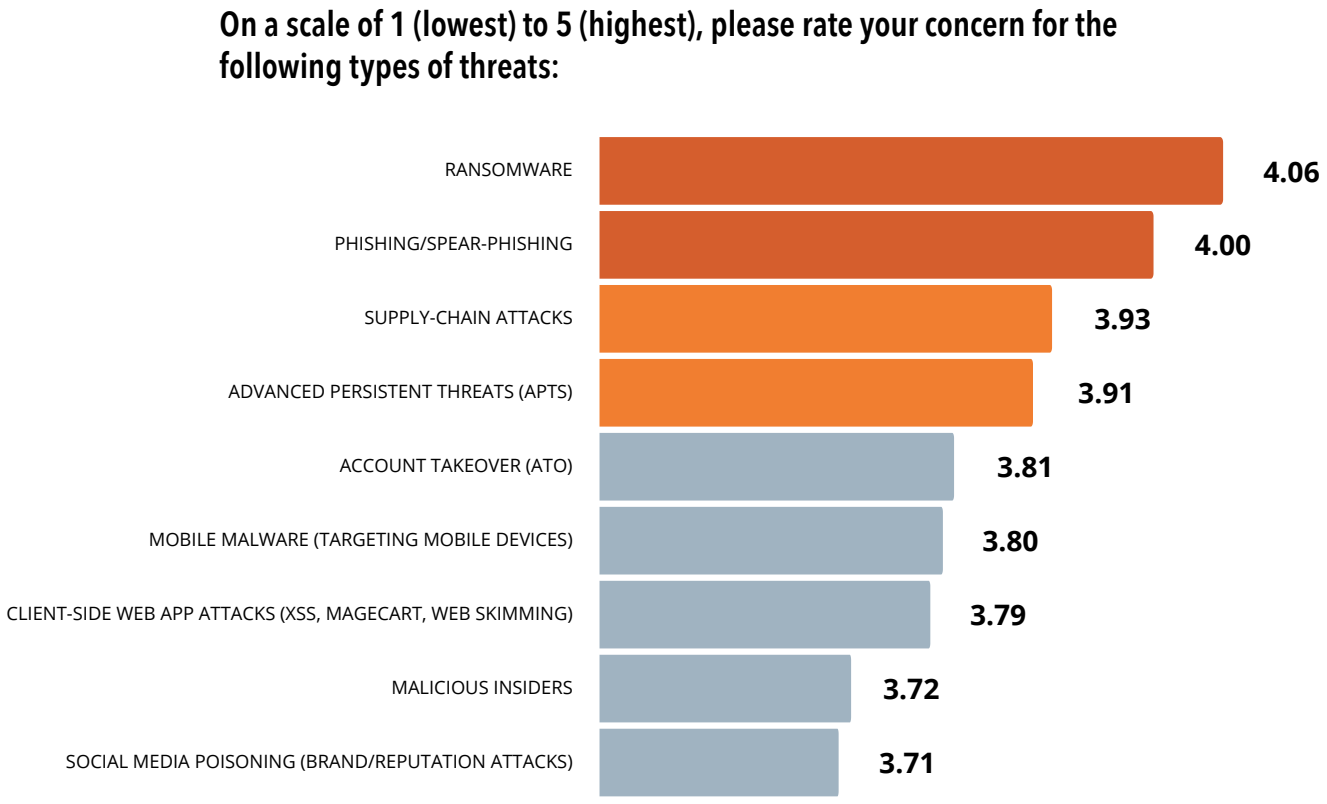


Figure 9. Threats Causing Greatest Concern

In terms of the vulnerabilities causing the most concern, third-party risk tops the list (3.89 of 5), which tracks with the escalation of supply chain security issues over the last two years. While there are measures that can be put in place to contractually obligate (and audit) third-parties' security practices, practically speaking this vulnerability is not completely within an organization's control.

"It is all over the news. Phishing campaigns are still the number one attack vector and are kicking people's butts. You also see more compromises due to cloud-facing misconfigurations and as fast as misconfigurations happen is as fast as exploits can happen. People clicking on links is a problem, if we can just get employees to stop being click happy…"
– Mario Memmo, Vice President, Chief Information Security Officer, Otis Elevator Co

However, this risk rates neck-and-neck with unpatched software and systems (3.88) — something that *is* within organizational control. That patching is still such a high concern indicates more focus, resources or bandwidth needs to be dedicated to this practice — another task that CISOs must juggle in a long list of duties. Configuration errors made by IT administrators rate nearly as high (3.72), suggesting the need for either more training or more time to configure systems. This is an area where automation can make a difference. Pragmatically, as we saw with cyber threats, everything on this vulnerability list deserves attention.

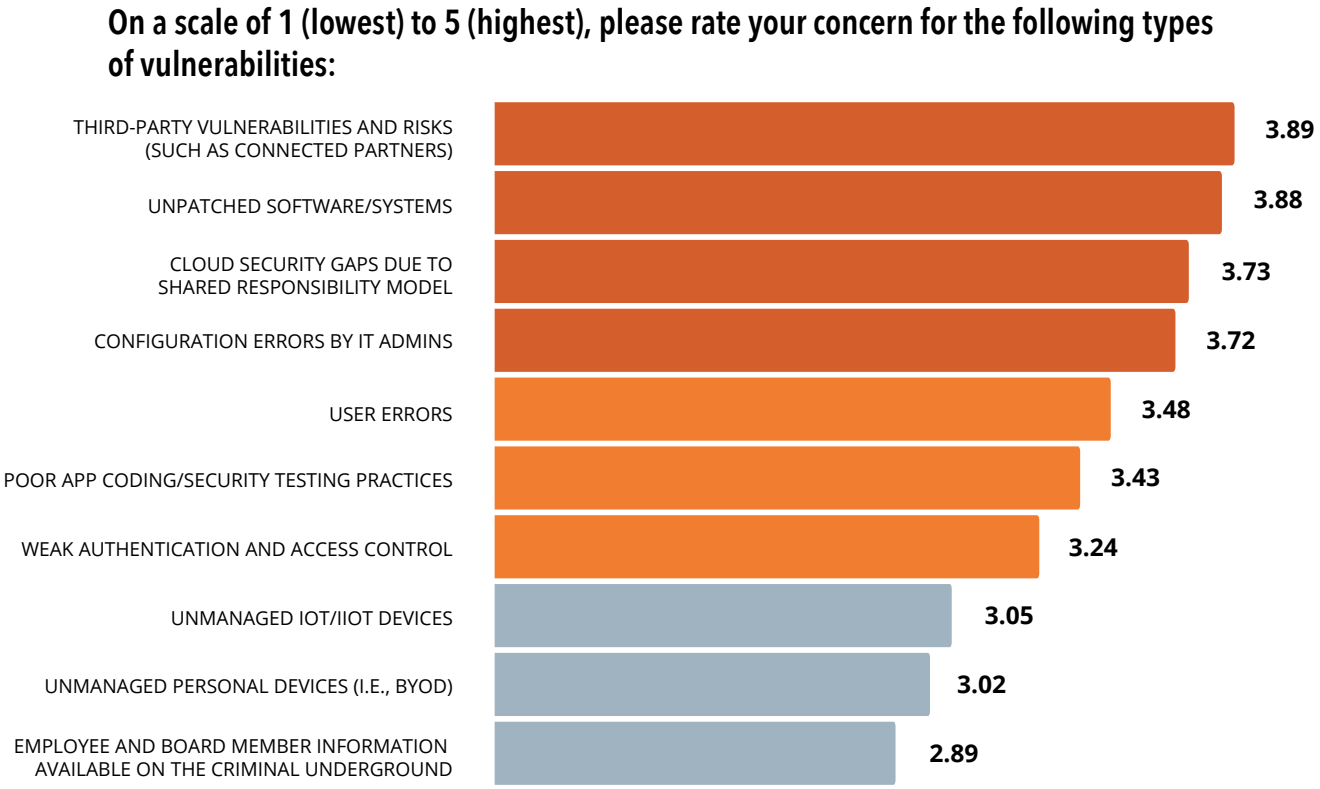


Figure 10. Vulnerabilities and Risks Causing Greatest Concern

"Application vulnerabilities bother me. When you have Log4j, Dirty Pipe and other similar ones coming out, there seems to be a risk in the app development lifecycle that doesn't come out until it's too late."
– Dr. Jorge Llano, CSO, New York City Housing Authority

While the prior two figures represent external threats and vulnerabilities that most worry CISOs, the following data reflects internal challenges — where CISOs need to shore up defenses against those dangers. With APIs (42.1%), SaaS (41.1%) and IaaS (37.9%) topping the list, the greatest concerns clearly reflect the growing dominance of cloud technology being used by respondent organizations the world over.

They also indicate the growing "componentization" of applications and services, and the corresponding prevalence of APIs to connect all of those components together. That is needed for not only standard, expected services, but also to enable innovative combinations and integrations that deliver a breadth of new capabilities, details and, ultimately, new value.

The findings further reflect a growing realization that protection must increasingly center on the data itself. Modern work-from-anywhere and perimeter-less computing environments diminish organizational control over — and trust of — the devices, networks, systems, and even applications used to get work done. That makes delivering protection at the data level increasingly necessary.

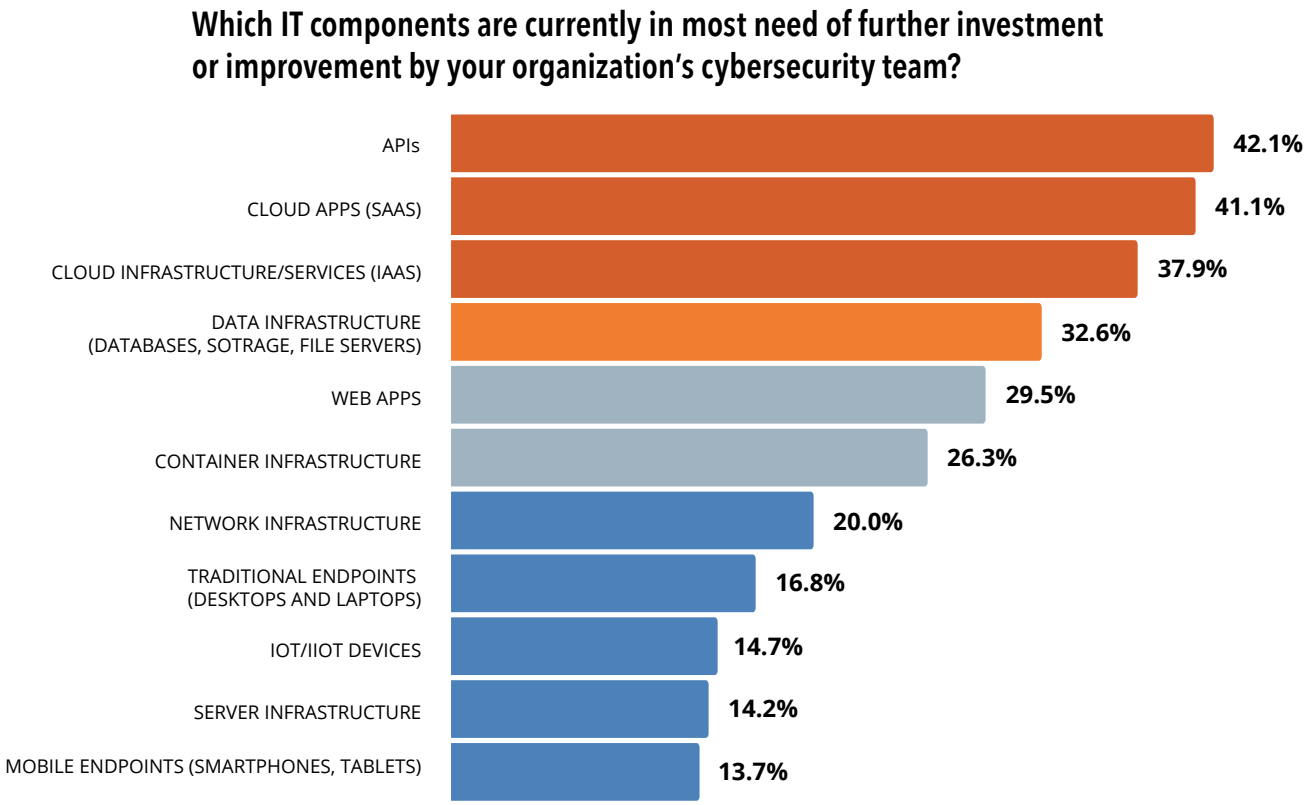


Figure 11. IT Components Most Needing Security Improvement

"Third-party risk management needs to be approached holistically. Each and every member organization that is part of that federation needs to take it to the same level of seriousness and have the same commitment to security. It does take money; it requires investment."
– CISO, large manufacturing corporation

"We have a significant third-party vendor population. When that population has connectivity to our network and is accessing ePHI or other sensitive data, it immediately becomes a top-five risk. It is imperative for us to do a thorough third-party threat and risk assessment of those partners."
– Les McCollum, Executive Director and Chief Information Security Officer, University of Chicago Medical Center

We also inquired about the security processes that CISOs feel need the most improvement within their organizations. Data-centricity is front and center. Given the importance of data-centric protections already discussed, it is not surprising to see data discovery and classification topping the list (37.9%). Discovery and classification have long been challenging, and that situation seems to be continuing. Data backup and recovery follows closely (36%), reflecting the importance of preserving what is discovered and classified. This priority may also be symptomatic of the prolific ransomware attacks seen over the past one to two years.

Vulnerability remediation (35.8%) and secure coding and testing (35.1%) show the need to reduce the effective attack surface — an excellent strategy, especially since these activities are directly within an organization's control.

What is somewhat surprising in our findings is the low placement of event management (15.8%) as needing improvement. This may reflect organizations having already made considerable investments in visualization, analytics and prioritization (whether those have sufficiently progressed or not), and now deciding to shift attention to other areas deserving of or demanding attention.

It is also curious that user awareness comes in as last (13.7%), when it is well known and often discussed that human users remain one of the weakest links. [The 2021 Verizon Data Breach Investigations Report found that a whopping 85% of breaches involved a human element].

Perhaps CISOs have accepted that trying to "fix" human behavior is a never-ending battle, and are refocusing priorities on what is within their power to control when those errors inevitably happen. Our recommendation in this regard: don't give up on user awareness and education — at least not entirely. The dividends may be challenging to quantify (see Figure 7), but they're almost certainly there to be had given the high volume of security incidents that continue to have user action as a key component.

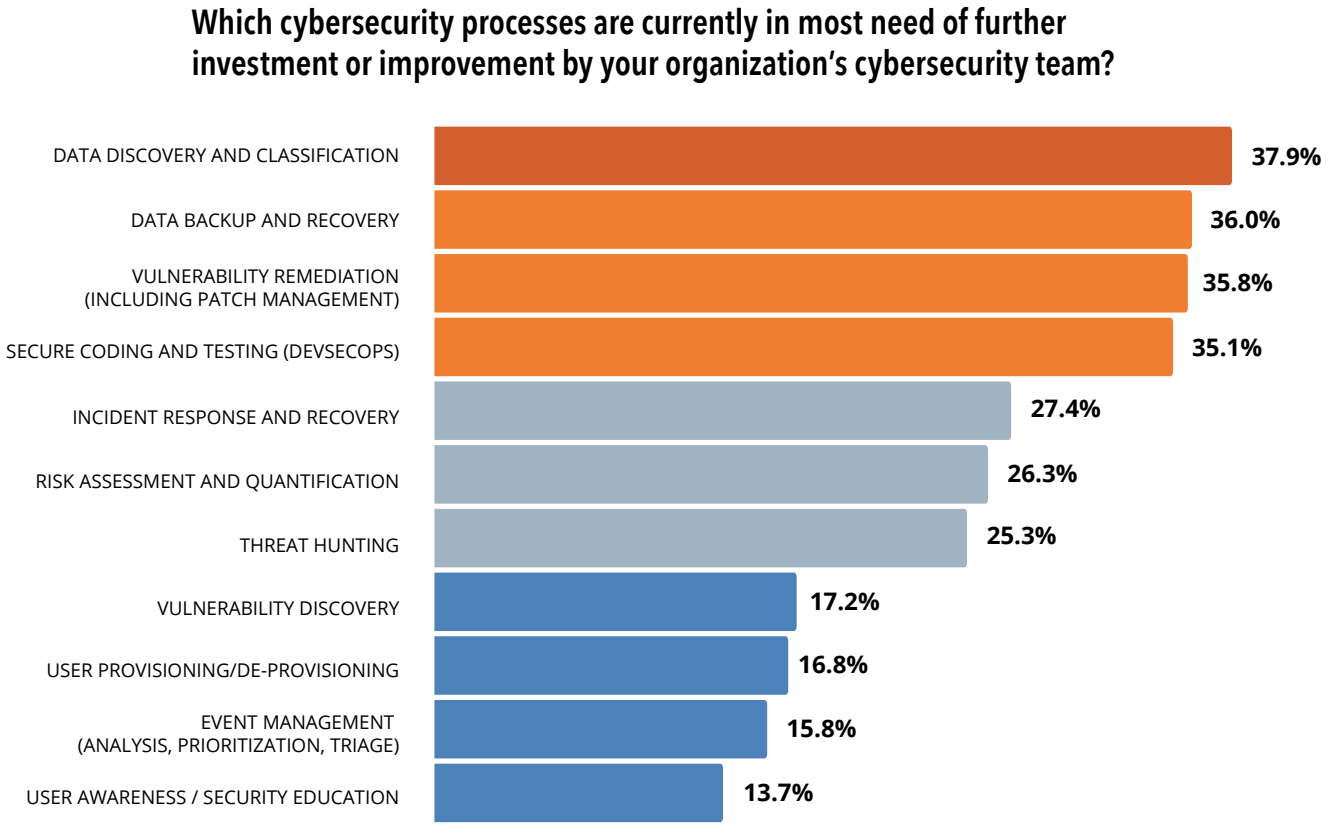


Figure 12. Security Processes Most Needing Improvement

Finally in this line of inquiry, we asked what is holding CISOs back. As has long been the case, the shortage of qualified talent still tops the list (3.83 out of 5). That is followed by six additional challenges that all rate within one tenth of a point in their perceived severity as an obstacle. This list, from alert overload (3.71) to difficulty integrating tools and technology (3.62), shows a wide range of issues that CISOs need to overcome. Happily, lack of support from senior leadership and the Board ranks lowest (3.51), indicating the shift in executive understanding of and concern about security as a critical business issue. Indeed, increased board awareness and support may be the one silver lining to come out of the extensive ransomware wave of the past few years.

On a scale of 1 (not at all) to 5 (significantly), rate how much each of the following inhibits your organization's ability to establish effective cybersecurity defenses:

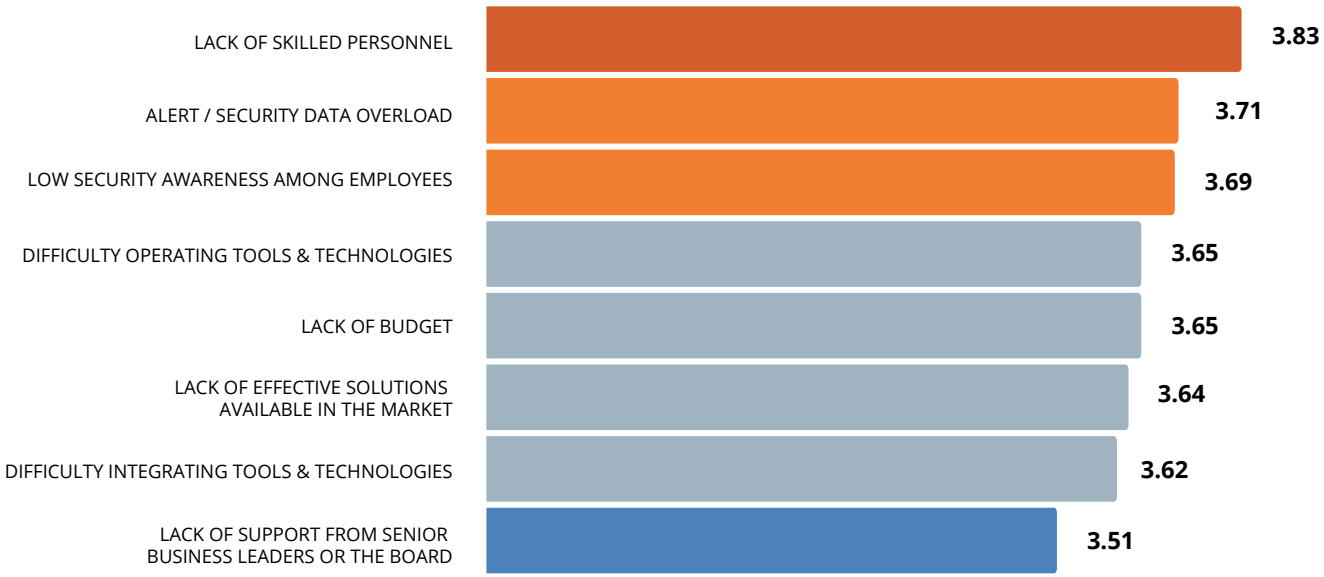


Figure 13. Greatest Barriers to Establishing Effective Cybersecurity Defenses

"For our governance program, I have global monthly audit and compliance meetings. I also have a Cyber steering committee made up of executives to make sure we align with all aspects of the business, followed by a Cyber Council, which is made up of senior executives including the CEO. And I do bi-yearly briefings to the audit committee. That governance structure has worked out really well."
– Mario Memmo, Vice President, Chief Information Security Officer, Otis Elevator Co

Plans for the Next Year+

Once respondents provided input about where their challenges lay, we then asked about their plans to address those challenges over the next year and beyond.

Better ensuring customer data privacy topped the list of respondents' priorities (52.6%). That is a significant gap from vendor consolidation, which trails the list at just 7.4%. Of course that does not mean it isn't an objective, but consolidation of security vendors — and, presumably of the toolsets being used — is clearly secondary to other things more closely tied to effectiveness rather than cost, efficiency and complexity.

Pursuing Zero Trust also rated very high (50.5%). We will discuss Zero Trust in the next section of this report, but note here that it is certainly a top priority. The need to better address those third-party supplier risks we saw topping the list of vulnerability concerns (see Figure 9), comes in third for intended actions (43.2%).

While it is much needed, better measuring security program effectiveness came in as the fourth place priority (35.8%), perhaps because it is has been regarded as an intractable problem for the entire history of cybersecurity. However, with Board-level attention increasing significantly due to ransomware and other major threats, security teams may now be either realizing the need for — or being pressured to find — more objective and provable ways to demonstrate progress in this area.

Better securing a remote or hybrid workforce comes in as a lower priority, likely because so much was already done on an emergency basis through the height of the Covid-19 pandemic. It may also be that many organizations are or will soon be returning to in-office operations, easing the need to secure remote access.

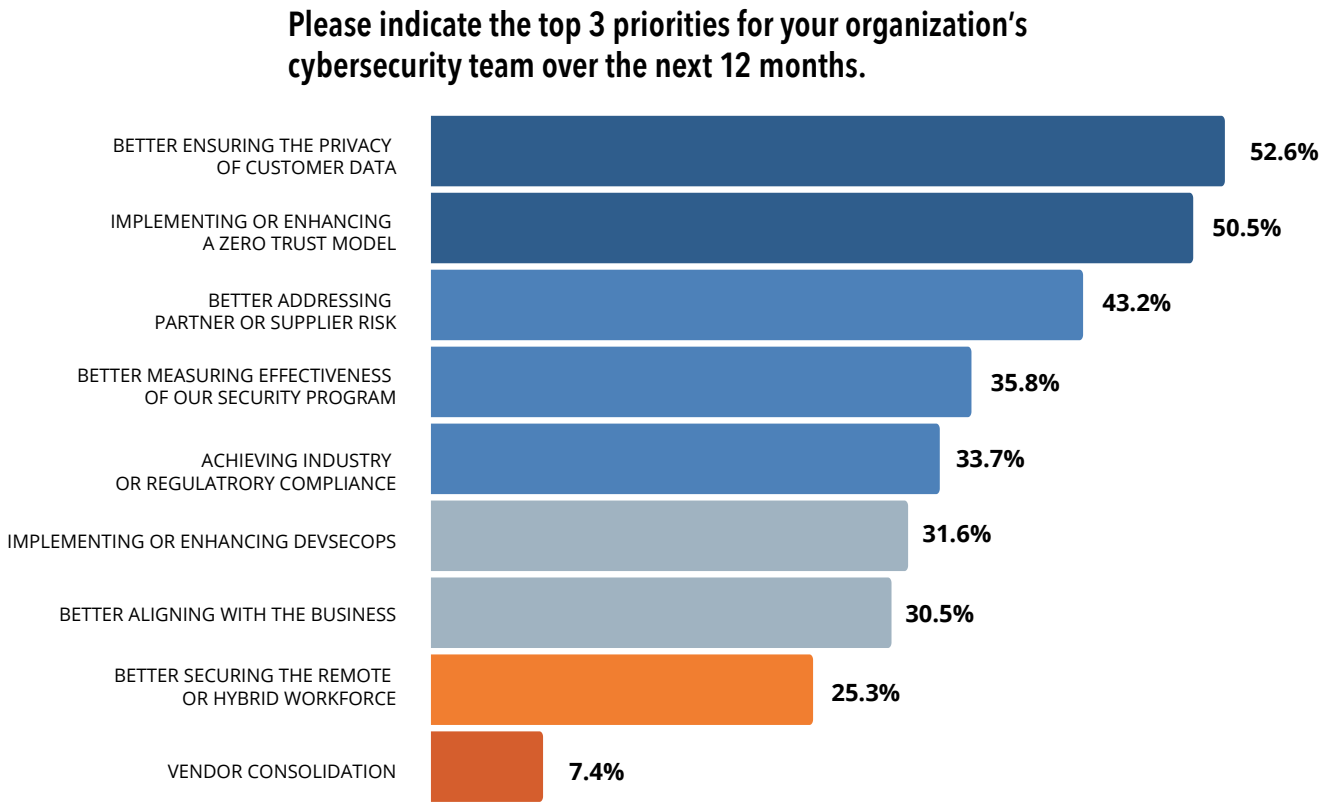


Figure 14. Top Security Priorities for the Next 12 Months

"One of the top challenges is people understanding the criticality and urgency. You've got people making money in the business, and to put more controls in front of them slows them down from making money."
– John Whiting, Global Director of Cyber Risk for Omnicom New York

"Security management is a dynamic, cyclical process, not a one-stop-shop. You have to be on your toes all the time."
– CISO, large manufacturing corporation

With these plans in place, what kinds of solutions will CISOs be looking for to help them meet their goals? In a nutshell — streamlined, but top quality. Sixty two percent of respondents want solutions that are easy to deploy. That likely reflects the complexity of the environments they are trying to manage, as well as the volume of alerts to be chased, patching to be done and systems to configure, all falling on the shoulders of overworked staff. Skilled talent remains in tight supply. In that same vein, ease of use is the second most desirable characteristic (47.4%). Automation capabilities (41.1%) are gaining ground over the past couple of years, as fears ease about machines replacing humans in this domain. Given the scope of what CISOs are required to manage, getting more done with the limited number of qualified people they have simply must be prioritized.

Being a best-of-breed solution rates higher (32.6%) than being part of a broader platform (15.8%). It seems the demand for effectiveness exceeds the alternative consideration of convenience and (potentially) lower complexity. It is also reflective of vendor consolidation as secondary to activities more closely tied to effectiveness that is illustrated in Figure 14.

This certainly does not mean that a platform approach should not be considered. Broader platforms should be able to achieve higher degrees of effectiveness IF all of the parts are actually working together. But when is their improved effectiveness enough to tip the scales away from the less efficient adoption of disparate best-of-breed solutions? This is a challenging dynamic for both the providers and consumers of security solutions, and one that will likely be with us for a while.

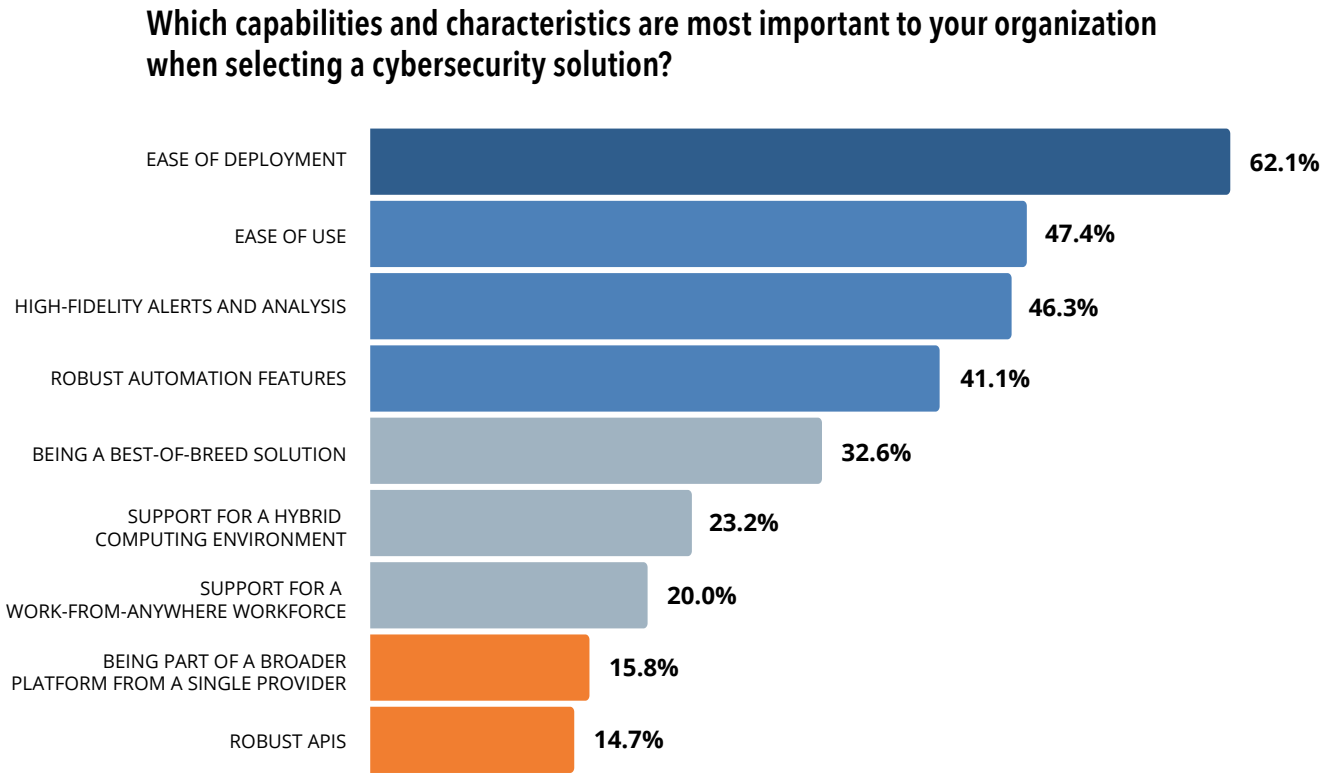


Figure 15. Top Capabilities Desired in New Security Solutions

"One of our biggest initiatives is to have more immutable technology. We need to ensure we have backups that are tamper proof. We're also looking for threat intelligence that can make us aware of what we don't know. The problem with networked devices today is they're tuned to find out what you do know. We need to use artificial intelligence and machine learning that can flag something unusual that we're not already looking for."
– Dr. Jorge Llano, CSO, New York City Housing Authority

"Anything that we can automate, we are going to do it. Time is of the essence; there are just not enough human hands and eyes to deal with it, and seconds matter so much in this world of cyber incidents."
– Christine Vanderpool, VP of IT Strategy, Architecture & Security, Florida Crystals Corporation

Zero Trust Moves from Hype to Reality

For all of the hype around the term "Zero Trust," it *is* something that CISOs are actively pursuing. Our findings show that 96.5% are already in various stages of implementation or actively planning to be. Zero Trust is real. But what actually is it?

That is perhaps best defined by what it is not — a single product or technology. It is a strategy, an architectural approach, the pursuit of an end state vision that will never be 100% attainable because the threat landscape and attack surface are continually changing. Zero Trust assumes the threat is without and within, so nothing can or should be trusted except down to the extreme micro level that demands verification every time. Think of it as the principle of least privilege on steroids.

Any Zero Trust approach should focus first on aggressively controlling who and what can get access to an IT asset, conditional upon a wide range of trust-related factors like the state of endpoint security, geo location, strength of authentication and sensitivity of what's being accessed. Then focus on progressively shrinking and containing the extent of that access to limit what a user (or attacker) can do once inside a system or network.

"My security program from the beginning has been centered around the trifecta of identity, zero trust and software-defined perimeter. If you build technology, people and process in the right manner, that foundation lets you tackle the multi-cloud environment much better than if you start signing-up all these cloud services willy-nilly…It's not just identity of people; it's identity of things too."
– CISO, large manufacturing corporation

"It's important not to have that trust for anything."
– Dr. Jorge Llano, CSO, New York City Housing Authority

"Identity is a new governance."
– Les McCollum, Executive Director and Chief Information Security Officer, University of Chicago Medical Center

Seventy one percent of respondents indicate their Zero Trust implementation is a work-in-progress, which makes sense given the scope and complexity of the effort. An additional 7.5% claim to already have a robust implementation. While those few may be well underway, there will be a continual and ongoing need to adjust and improve, particularly when extending Zero Trust practices beyond the network and system layers to more thoroughly address and account for applications and, ultimately, the data layer.

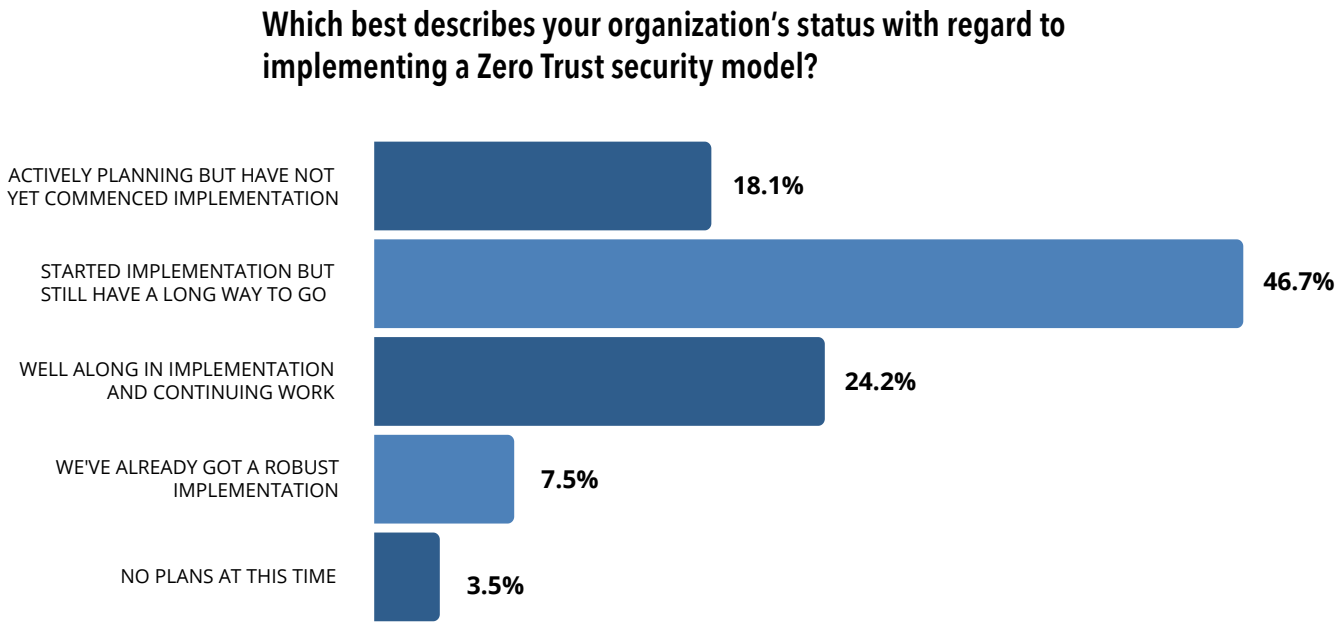


Figure 16. Status of Zero Trust Adoption

"Zero Trust is a multitude of solutions. You really have to get certain things in order first before you consider it. But I truly believe in it."
– Les McCollum, Executive Director and Chief Information Security Officer, University of Chicago Medical Center

"Zero Trust is a set of principles. It's all about least privilege access control. If you're doing that as a fundamental practice, you're already well on your way."
– Christine Vanderpool, VP of IT Strategy, Architecture & Security, Florida Crystals Corporation

Identity as the New Perimeter

The access control that is fundamental to Zero Trust extends to a new reality — that identity is, in effect, becoming the new perimeter. This is a consequence of there no longer being a well-defined *network* perimeter on which security practitioners can rely to delineate trusted from untrusted, and to implement controls to maintain this distinction. It stems from several shifts: the migration of systems and applications out of the datacenter and into the cloud; the increase in user mobility; and the greater use of BYOD which introduces unknown (and potentially less secure) devices into the environment. The erosion of what could previously be used as a proxy for trust means reliance must now shift to user identity. This new reality elevates the importance of several security attributes.

First and foremost is the level of assurance that an organization can have in verifying that a user actually is who they claim to be. This comes down to the strength (and reliability) of the credentials being presented. For example, passwords convey less certainty than multi-factor methods; and multi-factor methods that don't rely on passwords as one of the factors are stronger than those that do. As a result of the perimeter shift, respondents rate investing in solutions to mitigate risks from exposed credentials as their top change to be made (3.30 out of 5). That is just a hair ahead of investing in next generation multi-factor authentication (3.29 out of 5). Additionally, this shift compels CISOs to also consider the identity and security state of user's devices, reflected in noted priorities to invest in increasing inspection of user devices before granting access, and solutions that protect against browser-based attacks (3.23 and 2.93 out of 5, respectively).

The need for robust client-side security

With users connecting from everywhere, it has become critically important to protect end devices from incidents, vulnerabilities, and attacks that occur on dynamic web pages accessed from an end user's browser. Because these attacks, like formjacking, e-skimming, Magecart and more, are sophisticated and subtle, they can be hard to detect until it is too late. CISOs need to factor this unique attack surface into their security strategy in order to provide a safe and secure online experience.

Identity is effectively becoming the new perimeter. On a scale of 1 (not at all) to 5 (very significantly), rate the extent to which this is influencing your organization to make the following changes in the next 12 months:

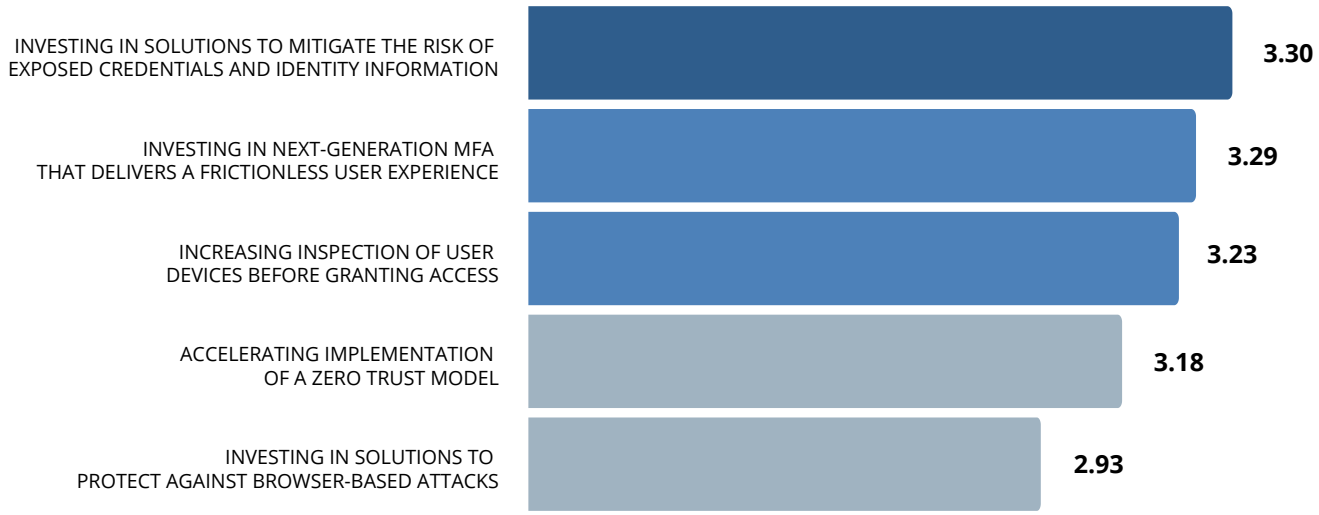


Figure 17. Planned Changes due to Identity Becoming the New Perimeter

"We're trying to move away from passwords and be more identity-based. Ultimately, the context of who you are and what you are accessing has to be married. We think in the next two to three years, passwords will not be sufficient for us to protect ourselves."
– Dr. Jorge Llano, CSO, New York City Housing Authority

Cloud and API Concerns

We next turned to the issue of cloud adoption and integration, which has exploded over the last decade. As organizations continue to embrace cloud applications and services, the potential for greater diversity of solution providers grows. Along with that is growth in the complexity of managing the resulting hybrid and/or multi-cloud environments, particularly from a security perspective. Our findings shed some light on how CISOs are planning to address this complexity.

That seven in ten respondents are planning to or have already implemented a unified platform for multi-cloud security reflects: 1) the inadequacy of cloud platform provider security; and 2) that multi-cloud environments by their nature are inconsistent and complex, making security even more difficult than for on-premise solutions. Thus CISOs are looking for help to overcome inconsistencies in security features, functions and configuration settings among different cloud environments.

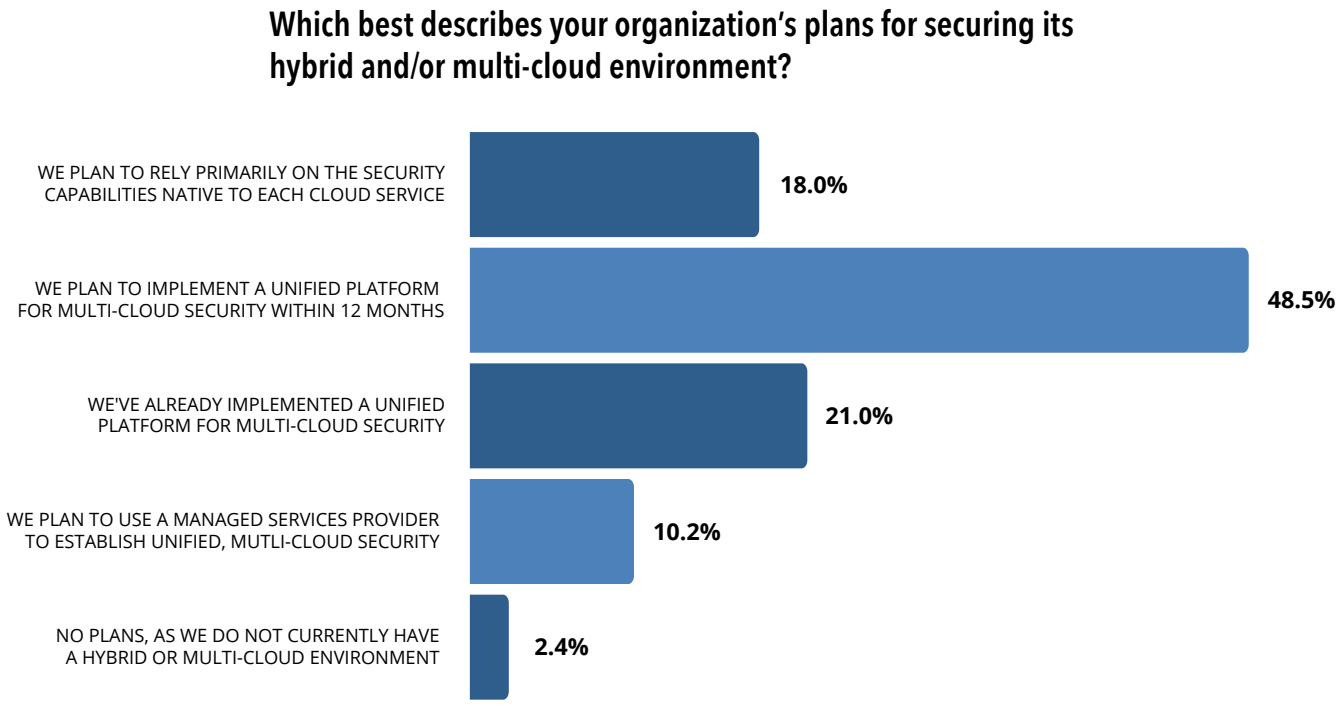


Figure 18. Plans for Securing Multi-Cloud Environments

"For SaaS, I build into our contracts that we can get the indicators sent to our SIEM so that I can see what the SaaS is seeing, even though they are responsible for those indicators and the security of that environment. If something from the SaaS falls into our actionable alert bucket, we isolate first, then I get on the phone with them to ask questions."
– Mario Memmo, Vice President, Chief Information Security Officer, Otis Elevator Co

"API security is something that people don't think about enough. Do the vulnerability testing of the API itself, because if the API is not designed properly, it's fairly easy to hack. I worry for supply chain security because of the weaknesses of APIs."
– CISO, large manufacturing corporation

Of course, adoption of cloud-based services and web applications means APIs are involved. These client-side to server-side connections are essential to business-critical, customer-facing applications, development environments, and partner-facing services. Exploding use of APIs also results from the shift to the component-based microservices architecture used in many of today's applications. Unfortunately, these useful and necessary APIs are also a top target for attackers.

Because APIs are unique, attacks on them have to be as well. An attacker can take days, weeks, or even months to probe and learn your APIs, so they use "low-and-slow" techniques that stay under the radar of traditional security tools. Detecting these low-and-slow techniques depends on having context, which is built from deep analysis of massive amounts of API traffic. This capability is fast becoming a critical component of an effective security strategy.

> "Identity has always been important. Even more important right now are the API protections. Especially when you have people that do custom development, you don't know how well-written those APIs are. There are security controls out there to actually examine your APIs. You can put certain signatures and other things, but you have to monitor to make sure they don't change."
> *– John Whiting, Global Director of Cyber Risk for Omnicom New York*

The top respondent concerns about APIs are around the potential for exposure of sensitive data (58.7%), which is most closely tied to material impact. We saw back in Figure 2 that 66% of respondents experienced such impacts between one and five times in the last year alone. We also saw in Figure 8 that exposure of sensitive data was the top impact of a cyber attack about which CISOs are concerned.

Only 6% of respondents claim to already be using an API security platform. That aligns to the relative newness of the problem. This is certainly one market area where we expect rapid growth over the next few years. That is reinforced by our finding in Figure 11 that APIs top the list of IT components most in need of security improvements.

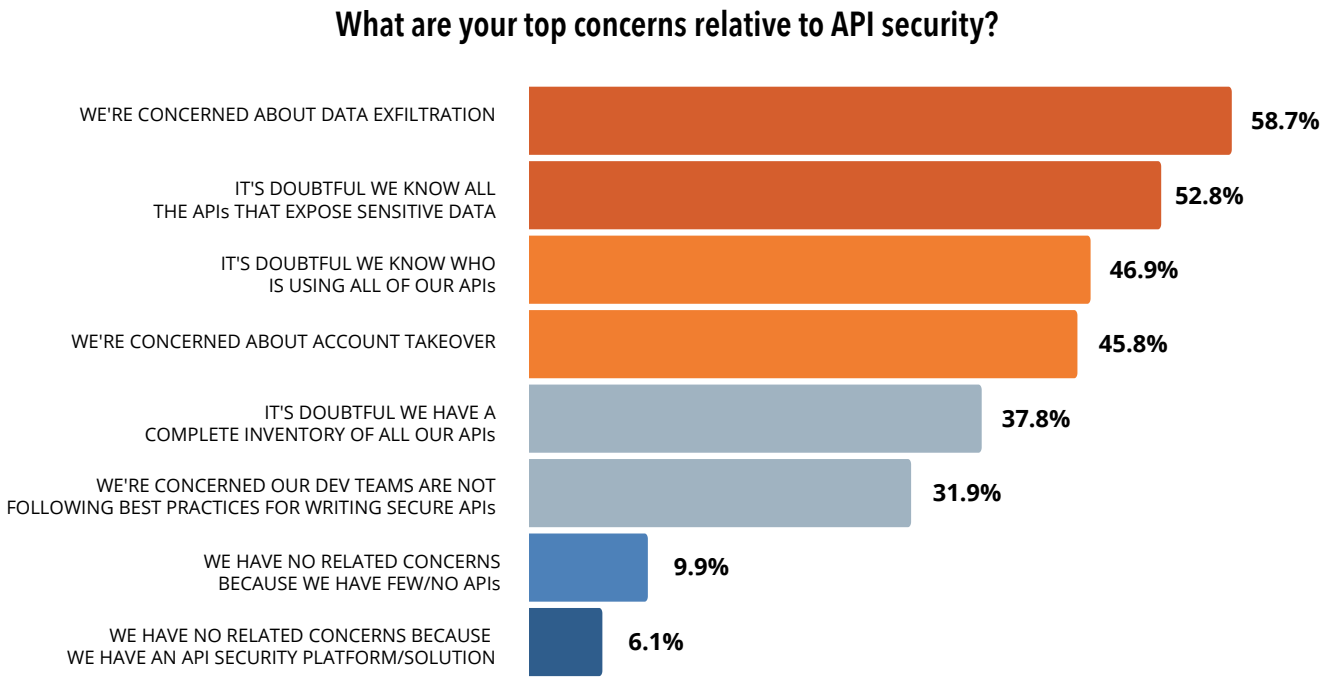


Figure 19. Top Concerns for API Security

What's on the Shopping List?

Given the many duties and challenges CISOs are facing for the next year and beyond, we wanted to know what kinds of technologies they will rely on to support their efforts. While the table below does not reflect all categories of available tools (too numerous to list), it does include a dozen of the leading kinds of tools that are designed to combat cyber attacks as they have currently evolved.

The results for those "already in good shape" track well to the timing of solution availability in the market, with network detection and response (46.6%) and third-party security and/or risk management (45.5%) leading by a significant margin.

The three top technologies that CISOs will be investing most in (either planning to add or upgrade) reflect themes uncovered elsewhere in this research. Network and micro-segmentation (the leader at 64.8%) ties back to the focus on Zero Trust, where segmentation is extensively applied for North-South traffic control, and micro-segmentation applied for East-West traffic. Container security (56.8%) maps to the evolution of application architecture and growing organizational adoption of containers and microservices.

Security service edge (SSE) (55.7%) takes third place on the list. SSE is a subset of the secure access service edge (SASE) framework, focused solely on security capabilities. Because SSE consolidates security functionality needed for connecting from anywhere to any cloud, its growing adoption links closely to the increase in remote and/or hybrid work. It's also a part of the Zero Trust equation.

Which technologies and solutions are currently in use, planned for upgrade, or planned for initial use by your organization within the next 12 months?

	Already in good shape	Plan to upgrade	Plan to add	No plans
Network detection and response (NDR)	**46.6%**	**28.4%**	**15.9%**	**9.1%**
Third-party security and/or risk management (TPSRM, TPRM)	**45.5%**	**28.4%**	**12.5%**	**13.6%**
Extended detection and response (XDR)	**38.6%**	**29.5%**	**20.5%**	**11.4%**
Client-side web application protection	**31.8%**	**18.2%**	**22.7%**	**26.1%**
Passwordless multi-factor authentication (MFA)	**30.7%**	**19.3%**	**27.3%**	**22.7%**
Security orchestration, automation and response (SOAR)	**27.3%**	**26.1%**	**28.4%**	**18.2%**
Network/micro-segmentation	**23.9%**	**37.5%**	**27.3%**	**11.4%**
Container security	**22.7%**	**30.7%**	**26.1%**	**20.5%**
Security service edge platform (SSE)	**20.5%**	**22.0%**	**33.0%**	**25.0%**
Breach and attack simulation (BAS)	**19.3%**	**17.0%**	**26.1%**	**37.5%**
Deception / active defense	**18.2%**	**22.7%**	**18.2%**	**39.8%**
Cloud-native application protection platform (CNAPP)	**17.0%**	**27.3%**	**26.1%**	**28.4%**

Table 1: Security Technologies in Use and Planned for Acquisition

Uncertainty, with More of the Same

CISOs continue to have their work cut out for them. On many fronts, great progress has been made; determined, sometimes heroic efforts keep organizations far more secure than they would otherwise be. But right now, at least, there is no letting up. The evolution of new models like Zero Trust and new solutions like API protection platforms and client-side web application security will help CISOs extend capabilities and capacity to augment what their over-stretched teams can do. Thoughtful adoption, careful planning, and perhaps a little bit of luck will help these leaders keep their organizations safe.

RESPONDENT DEMOGRAPHICS

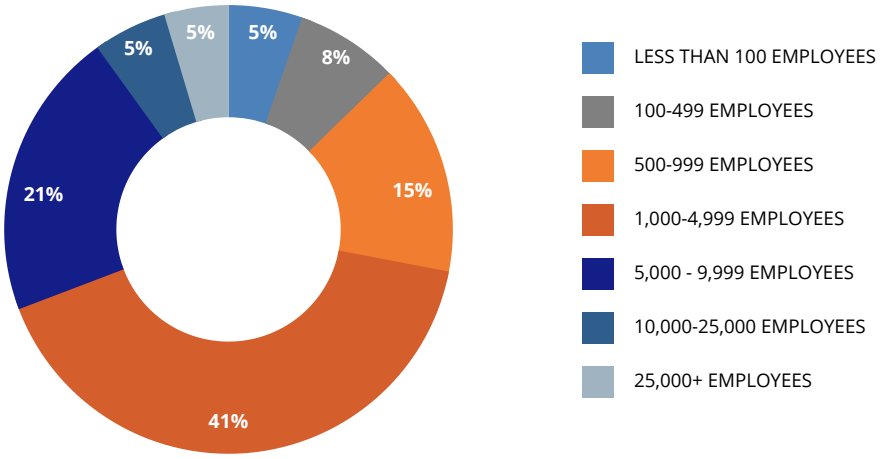


Figure 20. Survey Participants by Organization Size

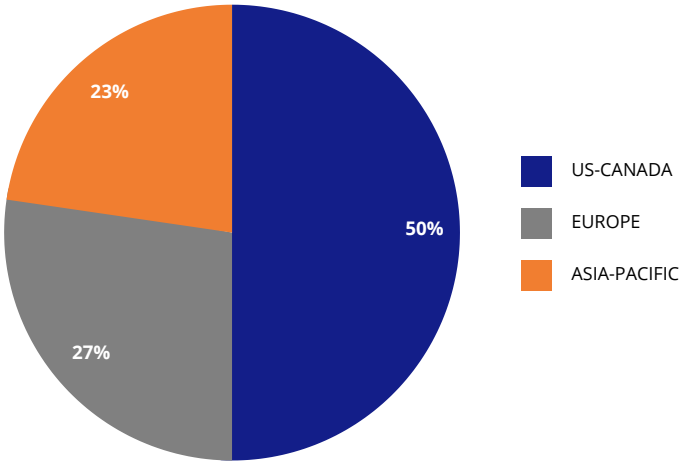


Figure 21. Survey Participants by Region

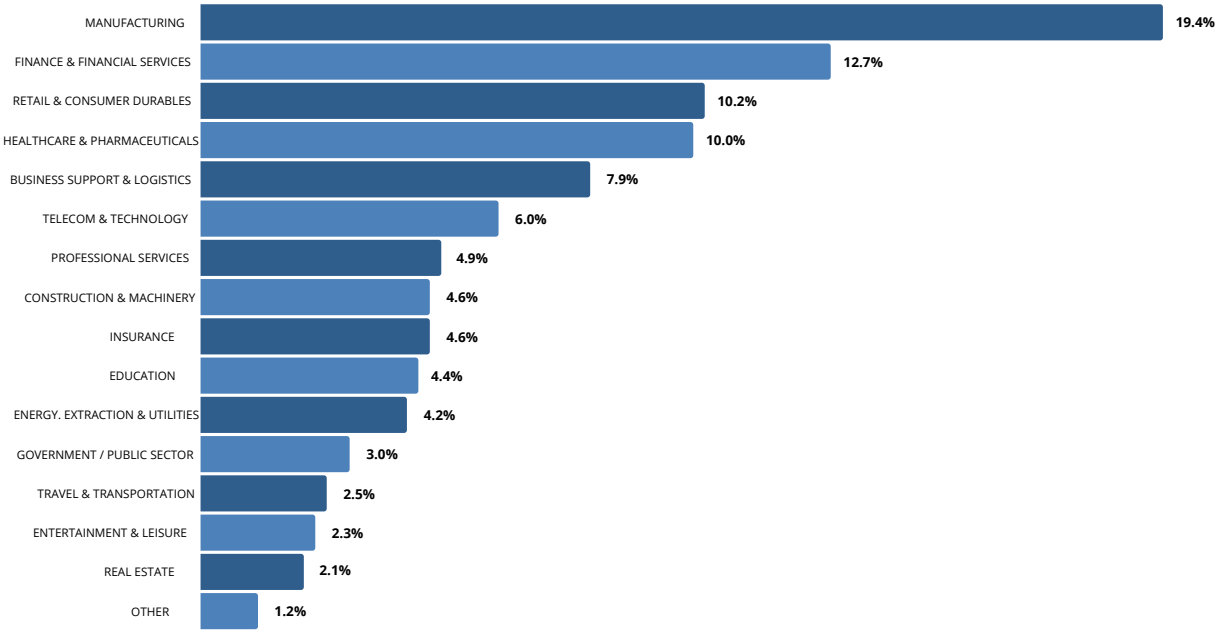


Figure 22. Survey Participants by Industry Sector

ABOUT OUR SPONSORS

Accenture Federal Services, a wholly owned subsidiary of Accenture LLP, is a U.S. company headquartered in Arlington, Virginia. Accenture's federal business serves every cabinet-level department and 30 of the largest federal organizations. Accenture Federal Services transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations. Visit us at www.accenturefederal.com.

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 699,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

Beyond Identity is fundamentally changing how the world logs in with a groundbreaking invisible, un-phishable MFA platform that provides the most secure and frictionless authentication on the planet. We stop ransomware and account takeover attacks in their tracks and dramatically improve the user experience. Beyond Identity's state-of-the-art platform eliminates passwords and other phishable factors, enabling organizations to confidently validate users' identities. The solution ensures users log in from authorized devices, and that the device meets the security policy requirements during login and continuously after that. Our revolutionary approach empowers zero trust by cryptographically binding the user's identity to their device and analyzing hundreds of risk signals on an ongoing basis. The company's advanced risk policy engine enables organizations to implement foundationally secure authentication and utilize risk signals for protection, rather than just for detection and response. For more information on why Intuit, Snowflake, and Roblox use Beyond Identity, please visit www.beyondidentity.com.

One in four organizations suffered from a cyber-attack in the last year, resulting in production, reputation and financial losses. The real problem is adversaries attack companies via third parties, island-hopping their way into target organizations. At Black Kite, we're redefining vendor risk management with the world's first global third-party cyber risk monitoring platform, built from a hacker's perspective. With 350+ customers across the globe and counting, we're committed to improving the health and safety of the entire planet's cyber ecosystem with the industry's most accurate and comprehensive cyber intelligence. While other security ratings service (SRS) providers try to narrow the scope, Black Kite provides the only standards-based cyber risk assessments that analyze your supply chain's cybersecurity posture from three critical dimensions: **technical, financial and compliance.**

Feroot Security protects client-side web applications so that businesses can deliver a flawless and safe digital user experience to their customers. Our automated data protection capabilities help cybersecurity and application security professionals guard the customer experience by increasing web application visibility. Feroot Security solutions take the pain and ambiguity out of client-side security threat analysis, detection, response, and prevention.

We designed our products — Inspector and Pageguard — to significantly diminish a threat actor's ability to breach customer data and damage websites via client-side attacks. Our solutions:

- Prevent and protect from client-side attacks, such as Magecart, cross-site scripting (XSS), JavaScript injection, and other threats focused on front-end web applications.
- Help organizations uncover supply chain risks and protect their client-side attack surface.
- Expose and remediate client-side security vulnerabilities in real-time.
- Discover client-side web assets in seconds.
- Identify and report on all JavaScript web assets and their data access.
- Facilitate constant client-side attack surface security management and defense.

Learn more at www.feroot.com.

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Horizon3.ai's mission is to help you find and fix attack vectors before attackers can exploit them. NodeZero, our autonomous penetration testing solution, enables organizations to continuously assess the security posture of their enterprise, including external, identity, on-prem, IoT, and cloud attack surfaces. Like APTs, ransomware, and other threat actors, our algorithms discover and fingerprint your attack surface, identifying the ways exploitable vulnerabilities, misconfigurations, harvested credentials, and dangerous product defaults can be chained together to facilitate a compromise. NodeZero is an unlimited, self-service SaaS offering that is safe to run in production, available on-demand, and requires no persistent or credentialed agents. You will see your enterprise through the eyes of the attacker, identify your ineffective security controls, and ensure your limited time and resources are spent fixing problems that matter. Not just a compliance checkbox; this is effective security. Founded in 2019 by industry, US Special Operations, and US National Security veterans, Horizon3.ai is headquartered in San Francisco, CA.

Lynx Technology Partners delivers dynamic Cyber Security and Risk Management solutions empowering every organization to effectively, proactively and seamlessly manage risk. The Lynx Team is made up of experienced, industry recognized experts who have led governance, risk management, compliance and cybersecurity programs and served as subject matter experts (SMEs) for Fortune 500 enterprises and government agencies. We recognize the gaps in traditional risk management approaches which do not provide visibility and interoperability between the various layers of defense. Our Lynx 360o Security services and solutions enable mature, risk management process and program integration. For more information, please visit LynxTechnologyPartners.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.

NetRise has developed an automated, cloud-based platform that provides comprehensive insight into the many risks present in a firmware image. These risks and associated artifacts are presented in a clear and concise manner allowing consultants, operators and SOC analysts alike to take appropriate action and begin to address the risks presented by firmware in their environment.

SpyCloud transforms recaptured data to protect businesses from cyber attacks. Its products leverage a proprietary engine that collects, curates, enriches and analyzes data from the criminal underground, driving action so enterprises can proactively prevent account takeover and ransomware, and protect their business and consumers from online fraud. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to over 150 cybersecurity experts who aim to make the internet a safer place. To learn more and see an overview of your company's exposed data, visit spycloud.com.

VMware is a leading provider of multi-cloud services for all apps, enabling digital innovation with enterprise control. As a trusted foundation to accelerate innovation, VMware software gives businesses the flexibility and choice they need to build the future. Headquartered in Palo Alto, California, VMware is committed to building a better future through the company's 2030 Agenda. For more information, please visit www.vmware.com/company.

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyber attacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

Additional Resources:

- Zscaler Security Research
- Zscaler Ransomware Protection
- Comprehensive Security
- Risk Assessment

CISO BOARD OF ADVISORS

DR. ARUN DESOUZA, CHIEF INFORMATION SECURITY & PRIVACY OFFICER, NEXTEER AUTOMOTIVE CORPORATION

Arun has extensive global IT and security leadership and organizational transformation experience including as CISO and CIO. Arun's areas of expertise include strategic planning, risk management, identity management, cloud computing and privacy. His current interests include the Internet of Things (IoT), Blockchain, Zero Trust, Software Defined Perimeter & Self-Sovereign Identity. Arun is a respected industry thought leader and keynote speaker.

Arun earned Master's and PhD degrees from Vanderbilt University. He is a Certified Information Systems Security professional (CISSP) and has earned the Certificate of Cloud Security Knowledge (CCSK) certification. He was honored by the 1st Global Cyber Observatory by induction into the CISO Hall of Fame in September 2019. He has won multiple other industry honors including CISO of the Week, CSO50 Award, Computerworld Premier 100 IT Leaders Award, CIO Ones to Watch Award and the Network World Enterprise All Star Award. He is a member of the Society for Information Management and the International Association of Privacy Professionals.

DR. JORGE LLANO, CSO, NEW YORK CITY HOUSING AUTHORITY

As CSO at the largest public housing authority in North America, Jorge's responsibilities include, but are not limited to, providing leadership to the enterprise's information security organization, developing, implementing and monitoring a strategic and comprehensive enterprise information security as well as partnering with business stakeholders across the company to raise awareness of risk management concerns. As a trusted partner with strong business acumen, Jorge also advises senior leadership and the board of directors on evolving cyber and business risks.

Jorge holds several of the top industry certifications in information security, including ISC2, SANS, ISACA, and ITIL in addition to a BS in Information Technology, a Masters Degree in Cyber Security, and a Doctorate in Information Assurance Digital Forensics. Prior to his role at NYCHA, Jorge served as the Chief Information Security Officer to Deluxe Entertainment Services and before that he was the Global Chief Information Security Officer at iHeartMedia.

LES MCCOLLUM, EXECUTIVE DIRECTOR AND CHIEF INFORMATION SECURITY OFFICER, UNIVERSITY OF CHICAGO MEDICAL CENTER

Les McCollum II is an accomplished Senior Cybersecurity and Risk Management Executive with over 25+ years of experience spanning various industries. Presently, he serves as the Chief Information Security Officer (CISO) for the University of Chicago Medical Center. Les' core responsibilities involve oversight of information security programs, including Governance Risk and Compliance, Identity Access Management, Disaster Recovery, Security Operations, and Application Security.

Les has instituted and governed security programs that include cyber and IT operational risk across several organizations in the public and private sectors. His unparalleled and distinguished career trajectory has equipped him with the skill sets required to enable strategic business objectives while providing cyber and operational risk management direction.

Les is involved in several Client Advisory Boards of industry-leading security and not-for-profit organizations. He has held several not-for-profit board seats while continuously remaining engaged in various mentoring efforts across many institutions, formally and informally. Les is an advocate of continuous learning in the cyber risk space. He holds a Master of Professional Studies from Georgetown University in Cyber Risk Management.

JOHN WHITING, GLOBAL DIRECTOR OF CYBER RISK, OMNICOM NEW YORK

John has over 25 years of experience in building Cybersecurity programs to manage risk, while facilitating business objectives. In his current role at Omnicom New York, John advises in all aspects of global risk management, partnering throughout the organization to support the company's risk management activities while optimizing operational performance. Since taking on this role in 2021, John has overseen the establishment of an Enterprise Security Steering Committee consisting of key IT, security, and business stakeholders to provide strategic direction for the enterprise-wide security model.

Prior to his role at Omnicom, John was the first Chief Information Security Officer for DDB Worldwide, a $3 billion annual revenue holding company, where he was quickly promoted to Chief Security Officer and the interim Data Protection Officer. While at DDB Worldwide, he implemented a comprehensive Global Cyber Program. Before this, he was the first Business Information Security Officer for AIG Corporate where he transformed the security function into a trusted business partner for the organization by aligning security priorities with crucial business strategies.

MARIO MEMMO, VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER, OTIS ELEVATOR CO.

As Otis' first CISO, Mario built a business-driven, risk-based global Cyber Security program from the ground up, where he developed, implemented, and maintains all aspects of the global Cybersecurity program including Governance, Risk, and Compliance, Threat Intelligence, and Identity and Access Management in a continuously evolving cyber security landscape. Mario also developed a Cyber Governance program that includes regular briefings to the Board of Directors and Otis Executive leaders.

Mario is also responsible for cloud and vulnerability assessments that set the standard for ongoing Otis initiatives. Some notable achievements include his starting the Security Operations Center where threats are monitored 24/7 – including protocols for Incident Response and recovery as well as a Product Security Program that focuses on protecting products deployed at customers sites As Otis is an international company with 69,000 employees, he has worked with global regulatory compliance mandates including Sarbanes Oxley, ISO, NIST, GDPR, SOC2, CCPA, FAR, CMMI, PCI, and CMMC.

Prior to Otis, Mario was Deputy Program Director at ActioNet, INC. ActioNet is an IT company that focuses on cloud-based solutions, cybersecurity, and agile engineering. He led major programs where he aligned and executed IT objectives for the Department of Energy), successfully leading a team of 700 contractors to achieve this. He was responsible for creating the Incident Response Center, a next-gen initiative that focused on Enterprise and Security Ops.

As CIO at the Naval Surface Warfare Center, Mario was responsible for the IT environment that included Classified and unclassified systems as well as High-Performance Computing Environments and Data Center Operations infrastructures. He defined new system requirements for new technology initiatives. He chaired the senior leader Cyber Council and Governance Board groups.

Mario is passionate about cyber security and the protection of Intellectual property as well as safeguarding consumer data. This drive pushes him to tackle complex and interwoven cybersecurity and business challenges with acute attention to detail, discipline, and cost-consciousness. He holds a Bachelor's in Engineering from Widener University in Chester, PA.

CHRISTINE VANDERPOOL, VP OF IT STRATEGY, ARCHITECTURE & SECURITY, FLORIDA CRYSTALS CORPORATION

Christine has been at FCC for 3 years. For the past 3 years, she has worked on building out the Cyber Security Program based on the NIST Framework focusing on implementing capabilities that help FCC/ASR identify threats, protect against attacks, detect when things do happen, respond to them quickly and appropriately and recover from any incidents by taking the lessons learned and making improvements. Christine is now focusing on how to build out our next 3 year and beyond IT strategy including things like strong vendor relationships, alignment with architecture principles and engaging communications. Christine brings experience in building such strategies from her prior roles with Molson Coors Brewing Company and Kaiser Permanente.

Christine has received many awards in her career including the 2019 Cyber Security Woman Leader of the Year award and the 2020 Executives Who Matter award. She has also been featured in several industry magazines including Sync Magazine and a feature in 2020 Profile Magazine Executive Feature edition. She is also a published author of many articles and a chapter in the Complete Compliance and Ethics Manual used across many college campuses in the audit curriculum.

RESEARCH TEAM

MARK BOUCHARD, CISSP

As CEO at AimPoint Group, Mark oversees the firm's research and consulting operations, while also serving as a senior research and marketing consultant. Mark's areas of specialization include information security, compliance management, application delivery, and infrastructure optimization. Before APG, Mark co-founded and was COO for CyberEdge Group, a marketing firm catering to the needs of high-tech solution providers. Previous positions include operating as an independent IT research and marketing consultant (7 years) and Vice President at META Group (acquired by Gartner), where he analyzed business and technology trends across a wide range of information security, networking, and systems management topics, helping hundreds of organizations worldwide address their IT challenges.

KATHY STERSHIC

Kathy is VP of Research, Messaging and Content Marketing at W2 Communications. She leads the agency's research efforts, and applies research findings as an informed foundation for client messaging and marketing initiatives. She is well versed in many of the leading technology issues relevant to modern private and public sector enterprises, including AI, cybersecurity, cloud, data-privacy, and risk-management. Prior to joining W2 Communications, she headed boutique consultancy Dialog Research & Communications for 17 years. She previously served as Vice President for Cognitiative, Inc., a San Francisco-based consultancy specializing in marketing research and communication strategy for e-commerce clients; she also worked as a Senior Analyst for Jupiter Media Metrix Custom Research Group; and earlier in her career, worked on staff for several fast-growth software and hardware companies. She holds a Master's Degree from the George Washington University's Elliott School of International Affairs.

AIMEE RHODES, CEO, CISOS CONNECT

Aimee is a former foreign correspondent with the Reuters News Agency serving out of Israel where she interviewed leading politicians and influencers as well as covered the then burgeoning cybersecurity sector. Previously, she served as Director of Israel Radio's English News Service where she was responsible for management and execution of four daily broadcasts, aired locally and internationally. Aimee also worked as an on-air news presenter for Jerusalem Online, broadcast globally. Aimee also is a seasoned marketer having led marketing at several security companies including Corero Network Security, Inc., Xceedium, AlgoSec and Whale Communications Ltd., acquired by Microsoft. She also served as Vice President of Media and Editorial Content at GenerationA, where she was responsible for launching an Internet-based news and information portal. She holds a Masters in Journalism and a Bachelors in Political Science both from Michigan State University.

AimPoint Group

https://aimpointgroup.com

CISOs Connect

201-835-9205

https://cisosconnect.com

W2 Communications

https://w2comm.com