censys

The 2023

State of Security Leadership

Exploring the Struggles of CISOs in a Shifting Digital Terrain

Table of Contents

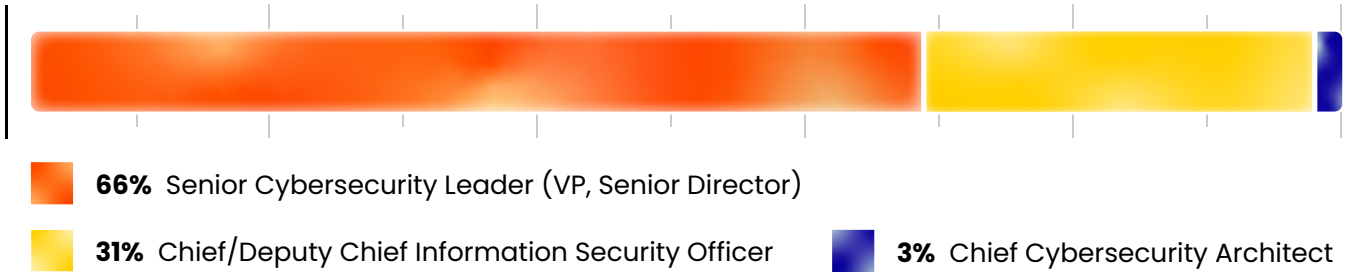
Methodology

Methodology

This Spring 2023 study utilized a blind quantitative survey to explore senior cybersecurity leaders' perspectives on strategic issues – from the current threat environment to geopolitical influence to personnel burnout, and more.

Respondents were professionally recruited from a well-screened panel. The total number of responses was 208, from respondents identifying as CISOs or CISO-equivalents or other senior-level security leaders across a broad range of industry sectors. They all worked at companies with greater than 5000 employees in organizations based in the United States, western Europe and Australia. All responses were anonymous.

Participants by Job Role

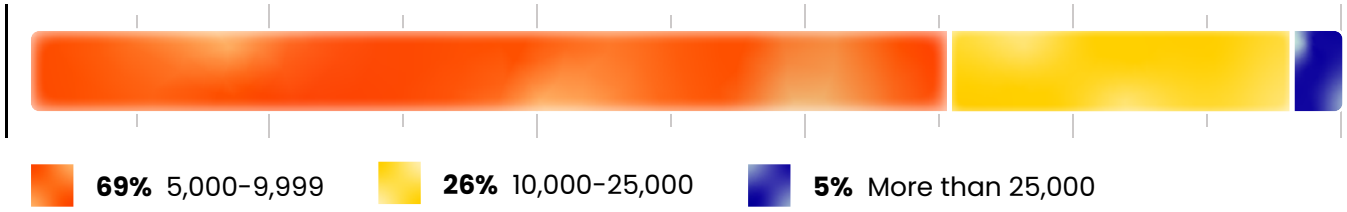


66% Senior Cybersecurity Leader (VP, Senior Director)

31% Chief/Deputy Chief Information Security Officer

3% Chief Cybersecurity Architect

Participants by Number of Employees

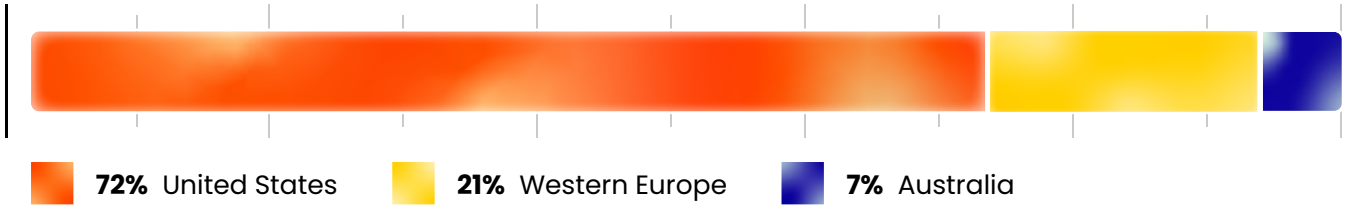


69% 5,000-9,999

26% 10,000-25,000

5% More than 25,000

Participants by Geo Location

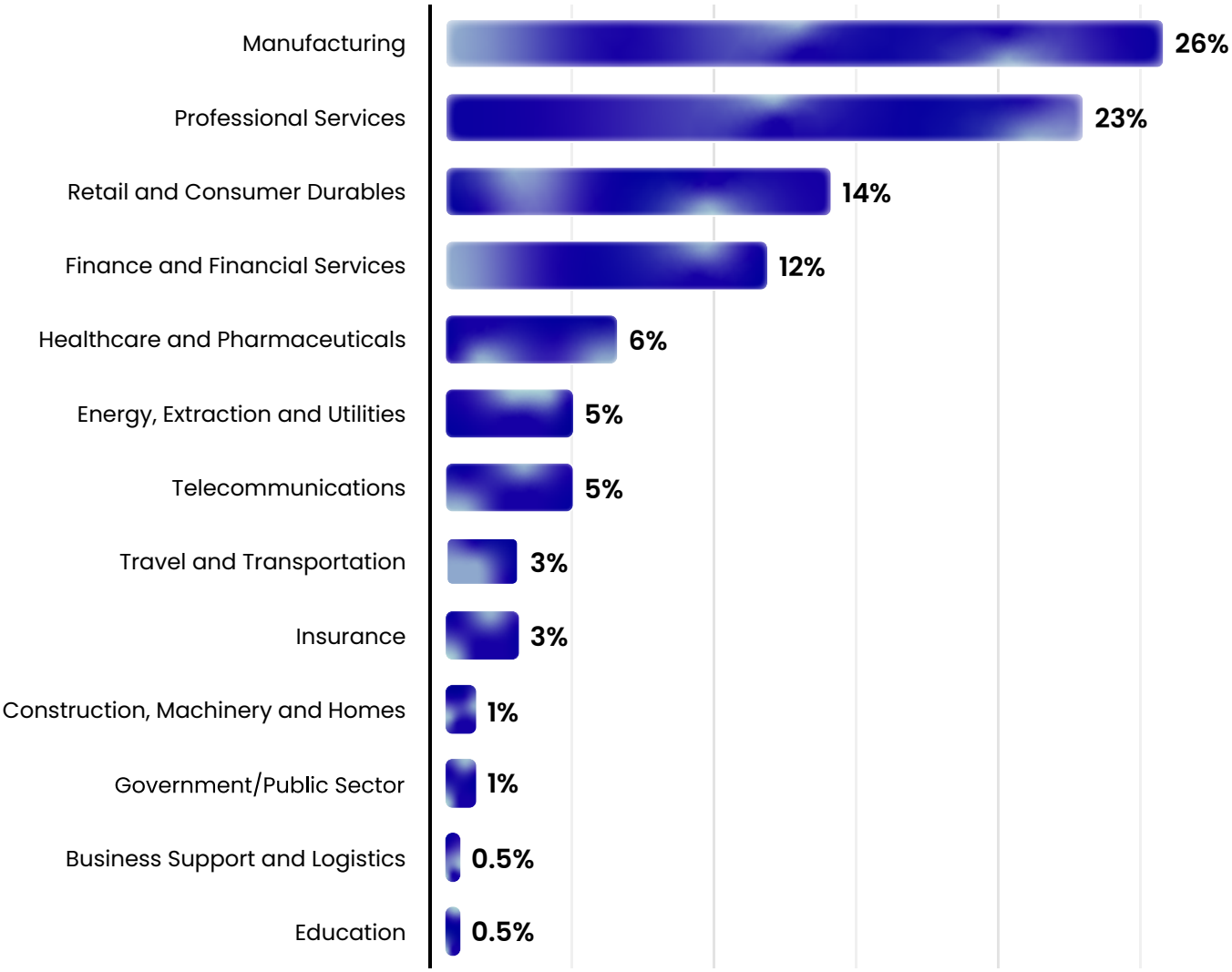


72% United States

21% Western Europe

7% Australia

Participants by Industry Sector



Key Findings

Introduction

The job of the CISO has never been more challenging. Between the steady increase in ransomware attacks, the rise of geopolitical tensions and nation-state sponsored espionage, and the acceleration of trends like cloud migration, there is a LOT on the CISO's plate.

With so many challenging headwinds, how do CISOs hold it together to protect both their assets and their teams' wellbeing at the same time?

It starts with understanding the key issues we are facing in cybersecurity today. To learn more about the massive challenges CISOs are currently tackling, we surveyed security leaders in the US, Europe, and Australia to get first-hand insights. Read on for our high-level findings.

Key Findings

The threat outlook is not improving.

All of our survey respondents reported that the cyber threat landscape is worse than the previous year. In fact, almost all respondents experienced at least one cyberattack and over half experienced between two and five. There was increased awareness of the amount and sophistication of attacks, especially attributed to conversations with their peers. Almost none said that a decrease in their own security budget contributed to this perception. It seems to be common knowledge and discourse in the industry.

The breadth of connected assets is largely unknown.

Over half of respondents said a better understanding their entire attack surface is their top priority for the next twelve months. Most respondents currently have poor visibility into the range of digital assets connecting to their network—28% discover connected assets manually, and only 22% use an automated tool. Clearly, organizations still have a long way to go. And, even though it is well known that people are the weakest link in cyber risks, security leaders' efforts to control connected personal assets and workers' online behaviors aren't as strict as they likely should be.

Geopolitics matter.

58% took defensive actions resulting from increased global tensions. With the war in Ukraine, today's divisive political landscape, and the ubiquity of globally distributed devices, nation-state actors are quickly taking advantage of this evolving paradigm. Additionally, the White House recently released their Cyber Security strategy, which stresses the importance of taking more vigilant action across both the public and private sectors.

Cyber investment protection is mixed.

Most respondents said their budgets for cyber spending are up, but spending is focused on sustaining what they already have in place rather than investing in new tools. Carrying cyber insurance has become a must, yet we question whether security leaders are really ready to meet all of their policy's terms.

Security teams may be close to hitting the wall.

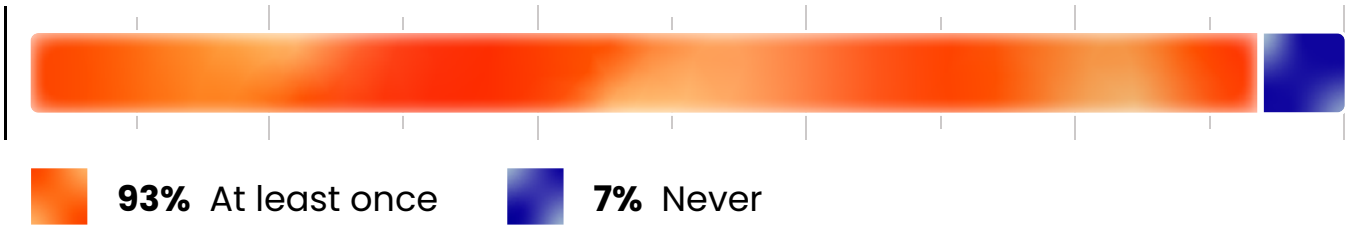
Respondents indicated significant concerns about the talent shortage and the resulting toll on current staff. With 65% citing the lack of qualified resources to fill their needs as their highest personnel worry, it is not surprising that over 60% of security leaders are reporting high levels of mental and physical burnout.

Detailed Findings

Damage Caused by Cyber Attacks is Accelerating

While organizations continue to bolster their defenses and invest in cybersecurity initiatives, respondents are clearly still feeling the cyber pain as the barrage of threats accelerate. **In our survey, an alarming 93% of respondents reported having suffered at least one successful cyberattack over the past 12 months that caused material impact.** And, even more concerning, 53% were successfully attacked between two and five times. With only 7% being 'safe' (for now), it is clear that experiencing a significant cyberattack has become the norm for most organizations.

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



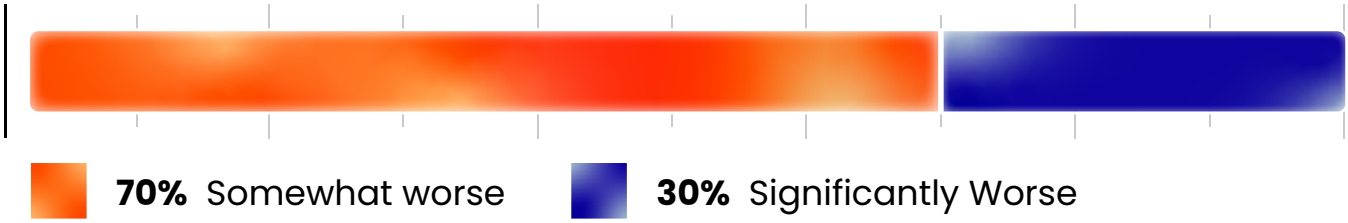
Enterprise Organizations Experience More Attacks

- 82% of companies with 5,000-9,999 employees reported being attacked materially 2-5 times.
- 53% of companies with 10,000-25,000 employees were materially attacked more than 5 times.

The Cyber Threat Landscape is Significantly Worse

All respondents perceive the current threat landscape as worse than one year ago, with 70% believing it is significantly worse. **Not one respondent reported that the cyber threat landscape had improved or remained the same from one year ago.** Fortunately, that perception was not linked to economic belt-tightening, as barely any respondents reported a decrease in budget in the past year.

Compared to one year ago, what is your perception of the level of threats currently facing your organization?



70% Somewhat worse

30% Significantly Worse

The Perception of the Threat Landscape is Worse in Manufacturing

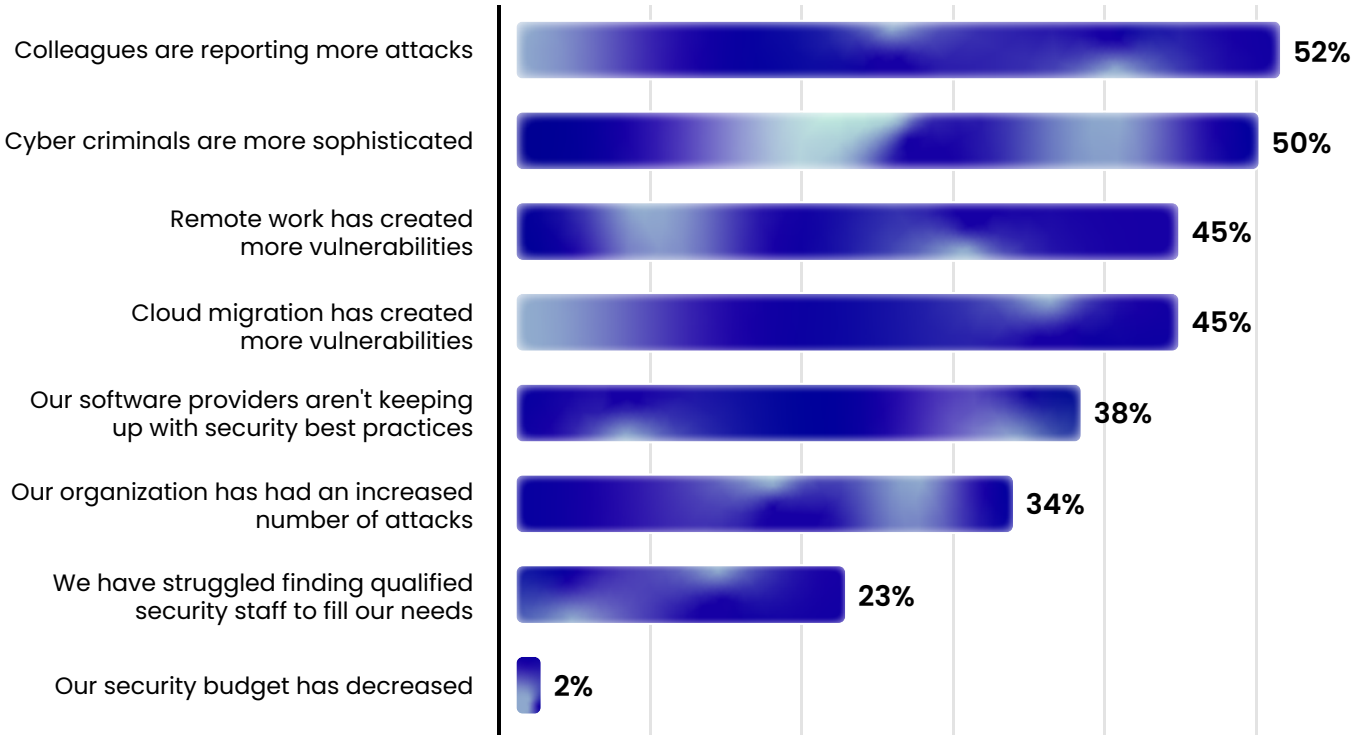
54.3% of those working in Manufacturing saw the threat landscape as:

- Somewhat Worse (24.1%) or,
- Significantly Worse (30.2%).

The reasons respondents did have that perception vary. About half reported their perceptions came from peer-level input and the increased sophistication of attackers. Security leaders implicitly trust the opinions and experiences of their peers, so it is not surprising that this is the number one reason for their unfavorable perceptions of the landscape.

The second most concerning group were external factors such as remote work, cloud computing, and supply chain partner practices that complicate the risk environment and increase vulnerabilities. Still, well under 50% identified remote work and the move to the cloud as part of their rationale, perhaps signifying that some of the biggest problems in the earlier part of the COVID-19 pandemic are easing, and respondents may have more of a handle on them.

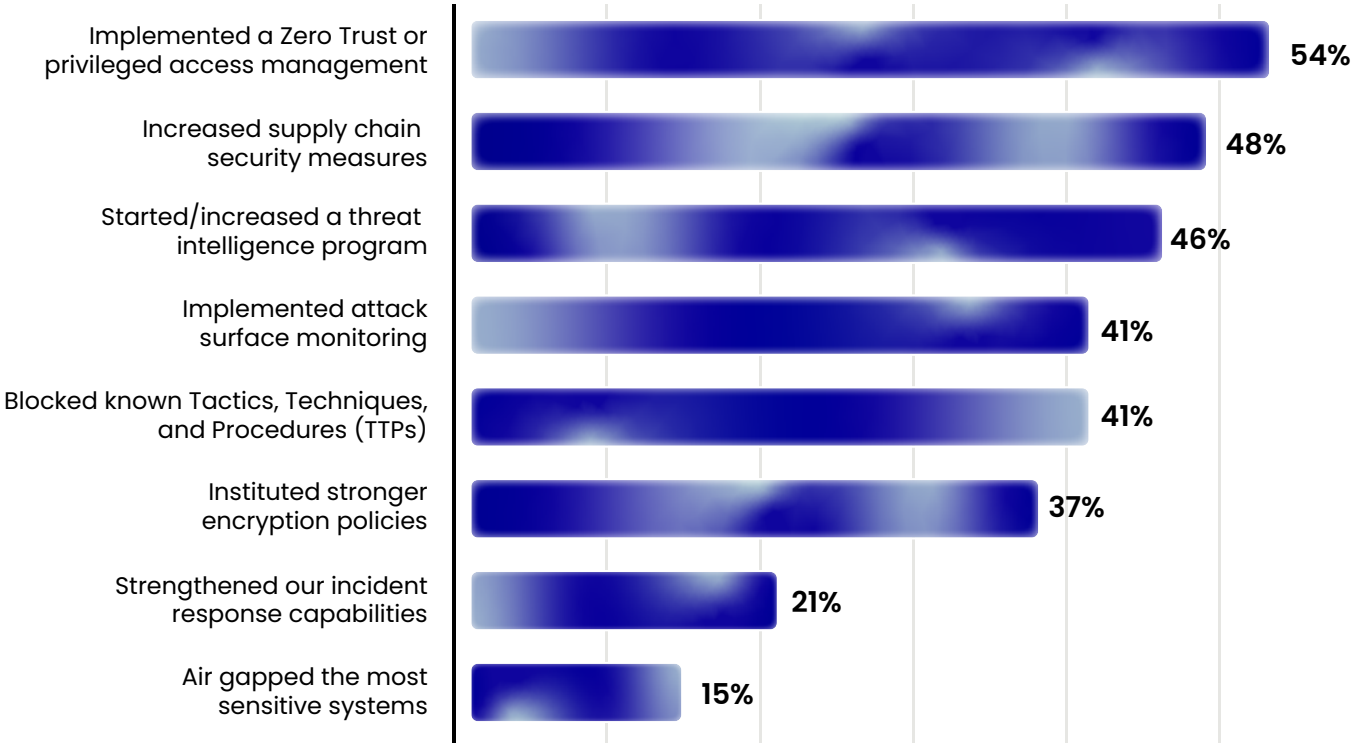
Why do you perceive the level of cyber threats currently facing your organization as worse than a year ago?



Geopolitical Tensions Have Caused Organizations to Take Action

Respondents have taken multiple actions toward improving their cyber defenses. Given the amount of attention paid to Zero Trust in the last two years, it is not surprising that implementing a Zero Trust architecture and privileged access management topped the list. Bolstering supply chain security was the second most common action taken, followed by beefing up threat intelligence. These steps demonstrate that security leaders are prioritizing a strategic approach to cyber security.

In the last 12 months, has your organization taken any of the following cybersecurity actions?



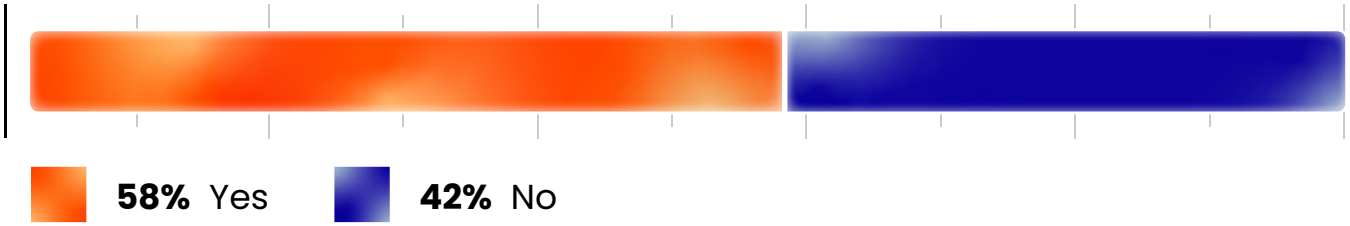
Of organizations with 5,000-9,999 employees:

- 73% increased supply chain security measures
- 70% implemented attack surface monitoring techniques
- 68% started or increased a threat intelligence effort
- 69% said they accelerated their security measures because of increased geopolitical tensions

These are significant steps for companies of this size to take.

Interestingly, current geopolitical events certainly had an impact, with well over half of respondents saying they increased their security efforts due to political tensions such as the conflict in Ukraine and challenges with China. Malicious nation-state actors' common usage of the Dark Web no doubt contributed to the greater interest in threat intelligence, indicating a potential paradigm shift in how security leaders need to assess today's threat landscape.

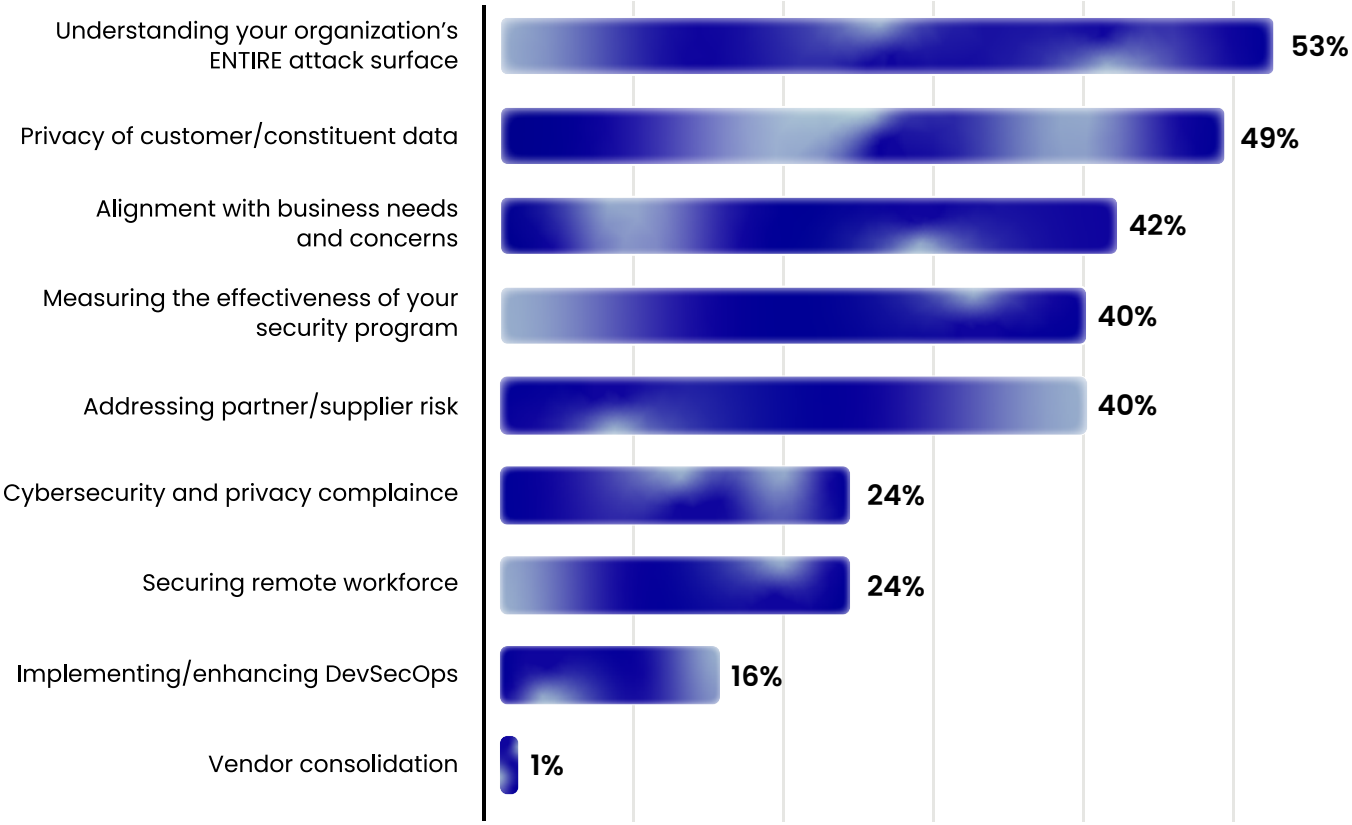
Did you take any of the actions listed above due to increased geopolitical tensions?



Securing the Attack Surface is the Number One Priority for the Next 12 Months

Respondents' forward-looking priorities indicated the need to uplevel cyber efforts to be more comprehensive and more strategic. Over half of respondents said they need to better understand their entire attack surface, revealing that they currently do not have a handle on everything that is touching their network. This underscores the rapid rise of External Attack Surface Management (EASM) platforms as a critical and foundational element to securing global organizations and preventing attacks.

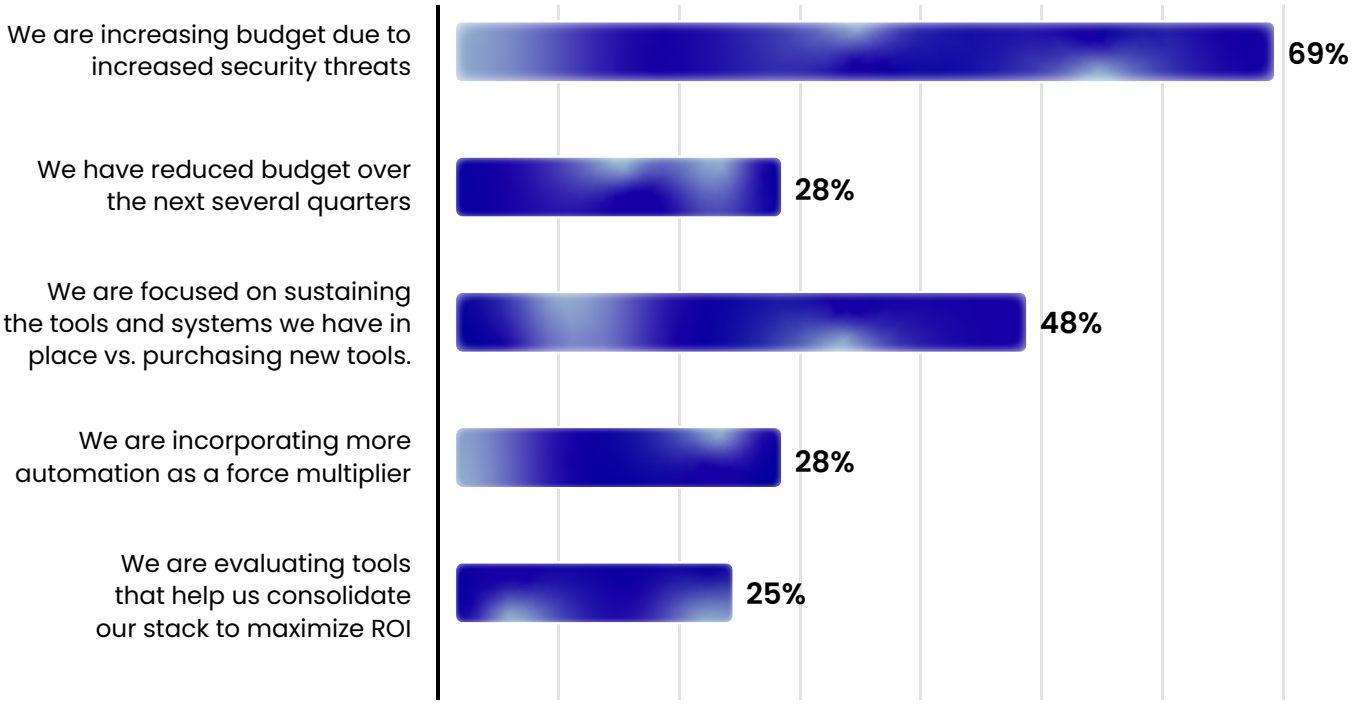
Which of the following reflect your top priorities for improving your organization's cybersecurity over the next 12 months?



About half of respondents recognized the need to better protect customer and/or constituent data privacy, although doing so for compliance reasons was a lesser concern (only 24%). Today's customers are demanding more privacy and security from the organizations they conduct business with, and as a result, security leaders are prioritizing these efforts. So while there are compliance reasons to protect data, businesses are realizing that their security practices (or lack thereof) can have an impact on revenue.

Another initiative that surfaced for our respondents is the need for executive level and cross-functional prioritization. Over 40% of respondents are prioritizing security's alignment with business needs and concerns. With the increase in threats and the catastrophic impact a breach can have on an organization, security strategy needs to be prioritized across all functions in the business. This has been further accelerated by the proliferation of cloud sprawl and shadow IT that goes outside of the organization's technical functions.

Is current economic uncertainty influencing your budget for cybersecurity investments?

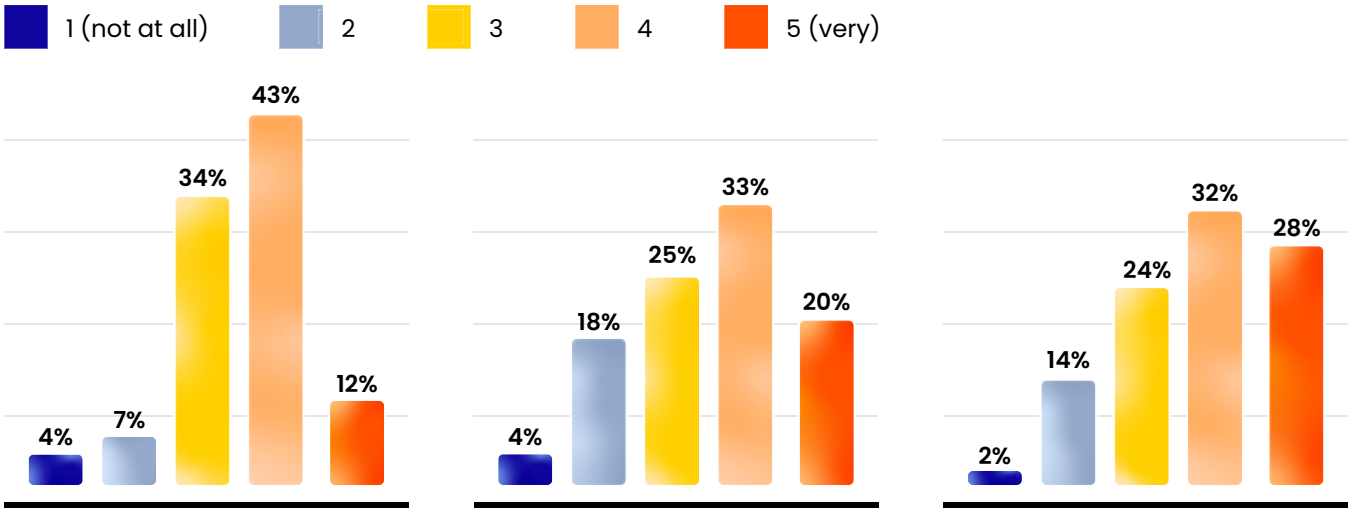


How are security leaders planning to support these priorities? A large percentage of respondents are increasing their cyber budgets in response to increased threats. However, spending reflects a more conservative approach, as nearly half will use their spend to sustain what is already in place rather than introduce new technologies. Only 28% are turning to automation as a force multiplier. So while economic uncertainty continues to loom, security leaders are continuing to hold on to their budgets. Again, this is another indicator that the cost of a breach is simply too high to risk unnecessary exposure, regardless of economic headwinds.

Mental Health and Burnout is a Significant Concern

With so many challenges facing security leaders today, we wanted to investigate how issues like burnout, the talent gap, and mental health are impacting teams.

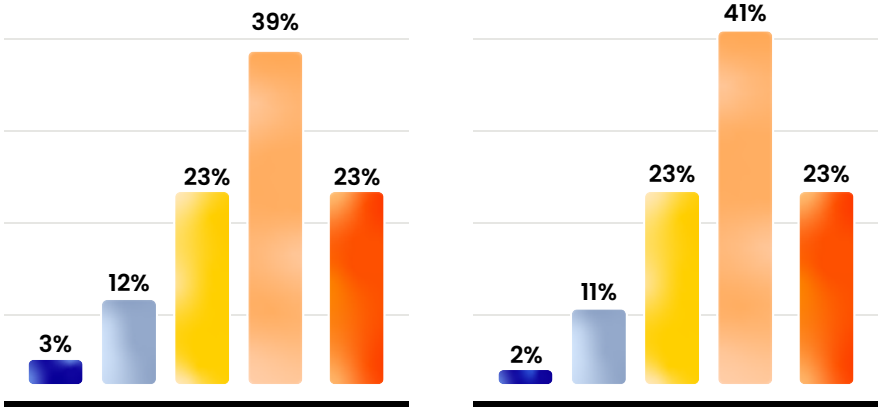
On a scale of 1 (lowest) to 5 (highest), please rate your level of concern regarding the following cybersecurity personnel issues:



Insufficient external talent pool available to fill your hiring needs

Limited/no skills growth for internal cybersecurity staff

Mental/physical burnout of internal cybersecurity staff



Mental/physical burnout of you personally

Insufficient qualified resources to meet the cybersecurity requirements of your organization

For security teams to effectively grapple with the evolving threat and compliance landscape, they need qualified resources to fill talent gaps. However, 43% of respondents reported that the lack of a skilled talent pool to meet hiring needs was a major challenge, and 33% reported that there was limited or no skills growth for their own internal cybersecurity staff. Unfortunately, this is a very real consequence of the current security talent gap—there are simply not enough trained resources available to fill all of the open roles.

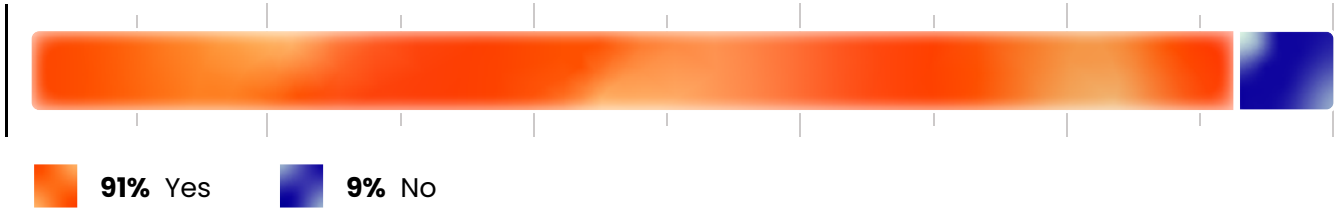
Perhaps not having the right resources for critical roles is one of the reasons that we saw mental health impacts and burnout coming in as the second most prominent people-related concern. 39% of respondents reported significant concerns around their own mental health and physical burnout, and 32% reported concerns about their staff's mental health and physical burnout.

It is interesting to point out that our respondents reported concern over their own mental health slightly higher than concerns over their staff's mental health. As cyber practitioners benefit from more tools that can help with rote tasks and reducing false positives, their jobs might be becoming a little bit easier, while the senior leaders still bear the greater responsibility of protecting the business. Might more collaboration or trusted delegation be needed?

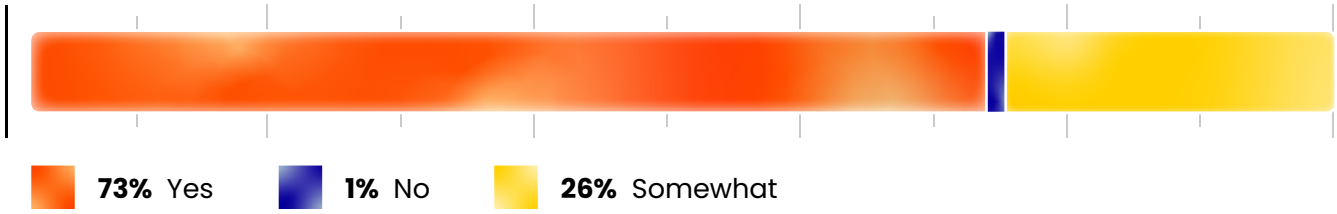
Cyber Insurance is Table Stakes

In addition to sustaining budgets for cyber protection, cyber insurance has become a must-have. Almost all respondents said their organizations carry a cyber policy. That is a significant increase from even a few years ago. However, among those who do, over a quarter said they are not aware of or fully prepared to meet all of the obligations of their policy. Even those respondents claiming they are fully aware of the terms and obligations of their cyber insurance policy may be overly confident.

Does your organization carry cyber insurance?



(If yes) Are you aware of the FULL terms and obligations of your organization's cyber insurance policy?



The uncertainty is likely due to the pace of change in the cyber insurance space. Given the high number of claims over the last several years, cyber insurance policies have become far more expensive, strict, and detailed, as underwriters get more into the cyber-weeds.

For instance, one of the main requirements of a cyber policy is having an asset inventory. That can't be correctly done if an organization does not know all of its assets. This may be a contributing factor to respondents rating the need to get a better understanding of their entire attack surface as their top priority for the next 12 months. In fact, many cyber insurance providers today have implemented their own Attack Surface Management platforms in order to monitor the companies they insure. However, businesses should not rely on a provider's attack surface monitoring to inform their business' strategy.

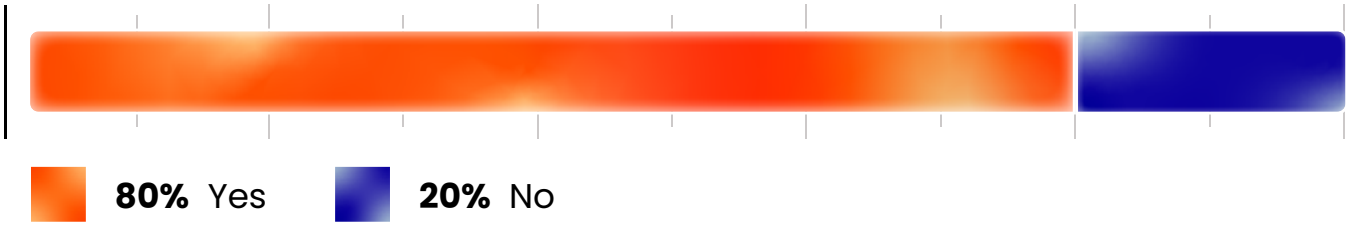
Policies and Capabilities

Over half of respondents are making concerted efforts to keep employees' personal assets separate from job-related technology and networks. 55% said they actively block unauthorized connections, and 38% actively monitor employees' online behaviors. Considering it is widely known that people are the weakest link in cyber-attacks, these numbers seem somewhat low. Still, 80% found their policies adequate for meeting the risks posed by modern technology employees use, again possibly suggesting over-confidence.

Data exposures via misconfiguration remain a serious problem. In Censys' 2023 State of the Internet Report, we identified over 8,000 servers on the internet hosting potentially sensitive information, including possible credentials, database backups, and configuration files. This suggests that perhaps policies aren't working the way security leaders had hoped, and there is likely a disconnect between what they want to work and what actually does work to prevent misconfigurations and data exposures effectively.

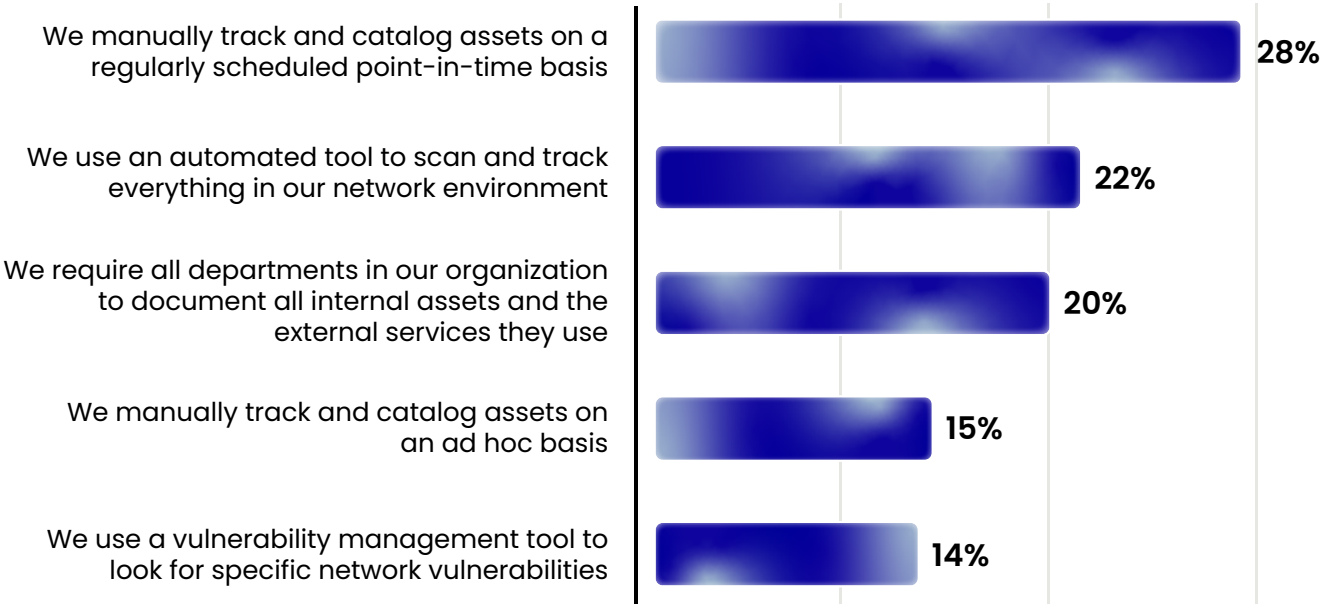
Does your organization maintain policies around employees' personal use of applications and other technologies on employer-owned assets?

Is your policy stringent enough to address risks from current technology at workers' disposal?



Even with the best policies, mistakes happen. Social engineering happens. Also, sometimes people make choices to go outside of policies to support a preferred work practice. An example might be a developer setting up unauthorized external sandboxes for tinkering with code and then leaving those sites orphaned. Typically, those sites are cloud instances, and because each cloud provider has a different configuration scheme, it's easy for a developer to unintentionally set up a cloud environment that is exposed to the internet. If that developer then leaves the company, there is no way to track down the properties they had set up. Risky behaviors like this - and more - are difficult to police, and likely should not be left to trust. This reinforces the need for better awareness of all (even very remote) corners of the attack surface.

Which of the following best describes how you discover and gain visibility into digital assets that need protecting?

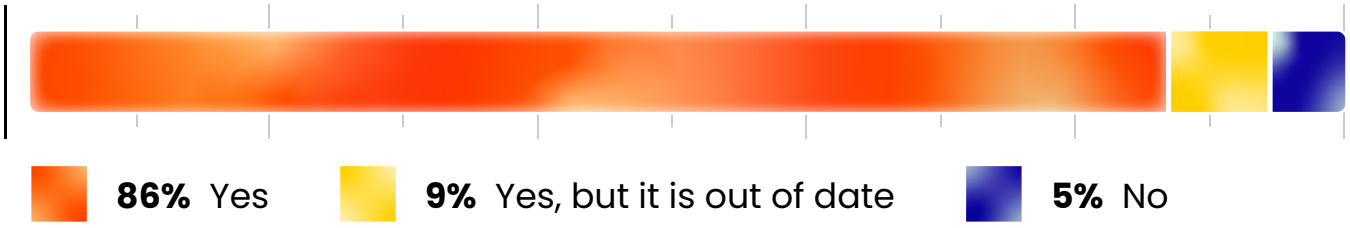


Professional Services Manually Tracking the Most Assets

Professional Services was the top industry sector for manually tracking and cataloging digital assets on a regularly scheduled basis (34.5%); but this sector also tops the list for tracking and cataloging ad hoc (31.3%). While this sector may be most disciplined about tracking, too many are still relying on manual, error-prone methods.

Respondents did feel they are in good shape when it comes to having a regularly updated and shared process for remediating common vulnerabilities and exposures (CVEs) that impact their network. CVEs are a very particular type of risk, formally tracked and published by the MITRE Corporation. Staying current on them should be part of every security team's ongoing practice. It seems these senior security leaders understand that and make it a regular part of their team's priorities.

Does your security organization maintain a formal remediation process to be implemented should a critical vulnerability exposure (CVE) impact your network?



However, as also demonstrated through findings in the Censys 2023 State of the Internet Report, vulnerability does not only refer to servers with outdated and exploitable software. Vulnerabilities can arise from various sources like misconfigurations, unknown assets, errors in judgment, and rushed work. While having a reliable CVE remediation process in place is certainly essential, it is not nearly enough to counter the breadth of exposure that exists.

The Cyber Evolution Continues

5 Recommendations for Today's Security Leaders

Top 5 Recommendations for Today's Security Leaders

As the cybersecurity landscape continues to evolve at breakneck speeds, security leaders will be asked to adapt. While there is no true definitive list of recommendations to help CISOs tackle all of the issues mentioned in this report, here, we offer some of Censys' recommended solutions based on our own expertise and the experience of our customers:

1. Ensure Leadership and Cross-Functional Alignment for Security Initiatives

40% of respondents to our survey are prioritizing security's alignment with business needs and concerns. With the increased occurrence of breaches (53% of survey respondents have been breached between 2-5 times over the past 12 months), security must become a critical element of every organization's strategy. Not only can a breach cost an organization a material amount of money, but it can also impact employees, productivity, customer revenue, and more. Plus, security is now interwoven with a large number of cross-functional compliance initiatives.

To ensure alignment with leadership, security leaders must develop easy-to-understand executive reports, clear ROI metrics around security investments, guidelines on cross-functional security frameworks, and robust employee training programs. It is imperative that security leaders bring these concerns and challenges directly to the C-suite to get buy-in for an organization-wide security strategy. Additionally, security leaders must make sure they and their teams understand the organization's business objectives and incorporate those priorities into the security roadmap.

2. Implement an External Attack Surface Management Platform to Identify and Monitor Internet-Facing Assets

In our survey we learned that understanding and securing the entire attack surface is the number one priority for organizations over the next 12 months. Clearly, with the rapid proliferation of assets, businesses simply can't catch up, and the lack of visibility can quickly leave you exposed.

The lack of transparency into internet-facing assets also showed up when we asked why respondents perceive the level of cyber threats worse than a year ago. 45% noted that remote work has created more vulnerabilities, 45% noted that the move to the cloud has created more vulnerabilities, and 38% were concerned that their software providers are not keeping up with security best practices.

By implementing an EASM platform like Censys, organizations are armed with the critical information they need to discover, monitor, and understand internet-facing assets in real-time. This information empowers security leaders and teams to automate the identification, prioritization, and remediation of advanced threats and exposures. Identifying assets manually is time consuming and inaccurate, and an EASM helps to automate that process.

3. Understand the Nuances of Your Cyber Insurance Policy

While 91% of our respondents do in fact carry a cyber insurance policy, 26% said that they were only somewhat aware of their policy obligations. While it is great that cyber insurance is now table stakes, organizations must be aware of the policy terms, which can be challenging due to the pace that the cyber insurance space has been moving.

Make sure that you are constantly up-to-date with all policy changes, no matter how small, to help better inform your business strategy. Don't simply read the policy once and assume that the terms and conditions will remain the same. Cyber insurance policies are continuing to raise the stakes.

Additionally, one of the main requirements of cyber insurance is having an asset inventory, so businesses must adopt tools like EASM platforms to know exactly what is going on with internal and external assets before an insurance provider dings you for having a critical vulnerability.

4. Take the Time to Understand Mental Health Impacts on You and Your Team

With so much going on in the world of cybersecurity, it is challenging to take the time to consider your own mental health or the mental health of your team. The seemingly never-ending talent gap, the increased sophistication of threat actors, and the rapid proliferation of tools mean mental health can quickly be put on the back burner. However, studies show that burnout can lead to a variety of critical issues, including inadvertently missing a potential vulnerability that leads to a breach.

While there is no hard and fast solution to this issue, a great first step is to encourage high-level conversations on your team that address burnout and mental health challenges. By normalizing these conversations, teams can feel more comfortable coming to their leaders when significant challenges arise.

Additionally, reducing cybersecurity tool sprawl and investing in automation can help increase the productivity of your team while making their jobs easier. The sheer amount of tools that many security professionals must monitor can be incredibly overwhelming. By investing in automation and consolidation, you can better leverage your resources and streamline tasks.

5. Prioritize Cyber Security Policies Across Your Organization

While 58% of our survey respondents said that they do train employees about cyber risks, 42% of our respondents do not. And what's even more concerning is that of those 58% that do, 20% do not think that training is stringent enough.

We know that the majority of exposures happen because of human error and misconfigurations, so it is critical that organizations develop and implement a regular training program that is easily understood and accessible to all employees.

Additionally, it is important to the success of a training program to have C-suite alignment and prioritization.

There are many tools out there that help you automate training programs and develop strict policies that your employees can follow. Make sure that you and your leadership team are in lock-step around the prioritization of these programs.

Conclusion

This research demonstrates the continual progression of a cybersecurity conundrum that has become an unfortunate but permanent part of the digital environment. Progress is being made, but new fronts open up and new challenges emerge in a seemingly endless cycle. As the need for security rises to a board level concern, cyber leaders are facing more strategic issues to defend against, even while ongoing threats persist. As those security leaders stand to meet the threats, it behooves organizational leaders to provide the support and resources necessary to help enable those they must count on to keep their enterprises safe.

censys

About Censys

Censys, Inc.™ is the leading Internet Intelligence Platform for Threat Hunting and Exposure Management. Founded in 2013 in Ann Arbor, Michigan, Censys gives organizations the world's most comprehensive real-time view of global networks and devices. Customers like Google, Cisco, Microsoft, Samsung, NATO, Swiss Armed Forces, the U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, and over 51% of the Fortune 500 rely on the company's Exposure Management solution for a real-time, contextualized view into their internet and cloud assets.

For more information, visit www.censys.io.