EXTRAHOP

2024

Global Cyber Confidence Index

Table of Contents

Executive Summary

In the second half of 2023, one story dominated the cybersecurity leadership community: the U.S. Securities and Exchange Commission (SEC) formally charged SolarWinds and its CISO with fraud and internal control failures related to a 2019 cyberattack.

The indictment sent a stern warning to security leaders, suggesting that they could be held criminally or civilly liable for cyberattacks that take place on their watch. It also highlighted a fundamental challenge for the CISO role: that while CISOs are responsible for raising risks to their senior leadership teams and board of directors, they rarely have the final say in how those risks should be managed or remediated. Additionally, the indictment raised broader questions about CISOs' confidence levels in their organizations' cyber risk management and governance practices.

We had this context—a cyber climate where scrutiny from the SEC in the U.S. is increasing and regulations around the globe are calling for more accountability—in mind when we conducted the survey for our third annual Global Cyber Confidence Index. In previous years, we asked security and IT decision-makers about their overall confidence in their organization's cybersecurity postures. This year, we asked specifically about their confidence in their organization's ability to effectively manage cyber risk. We also asked them about their organizations' cyber risk management practices, cybersecurity budgets, experiences with ransomware, planned investments in security technology, and more. Read on for highlights from the report.

Leaders May Be Overconfident

An overwhelming majority of respondents (88%) say they're confident in their organization's ability to handle cyber risk, yet their responses to questions about their experiences with ransomware attacks, their budgetary needs, and cyber hygiene indicate that perhaps they should be more cautious.

RANSOMWARE

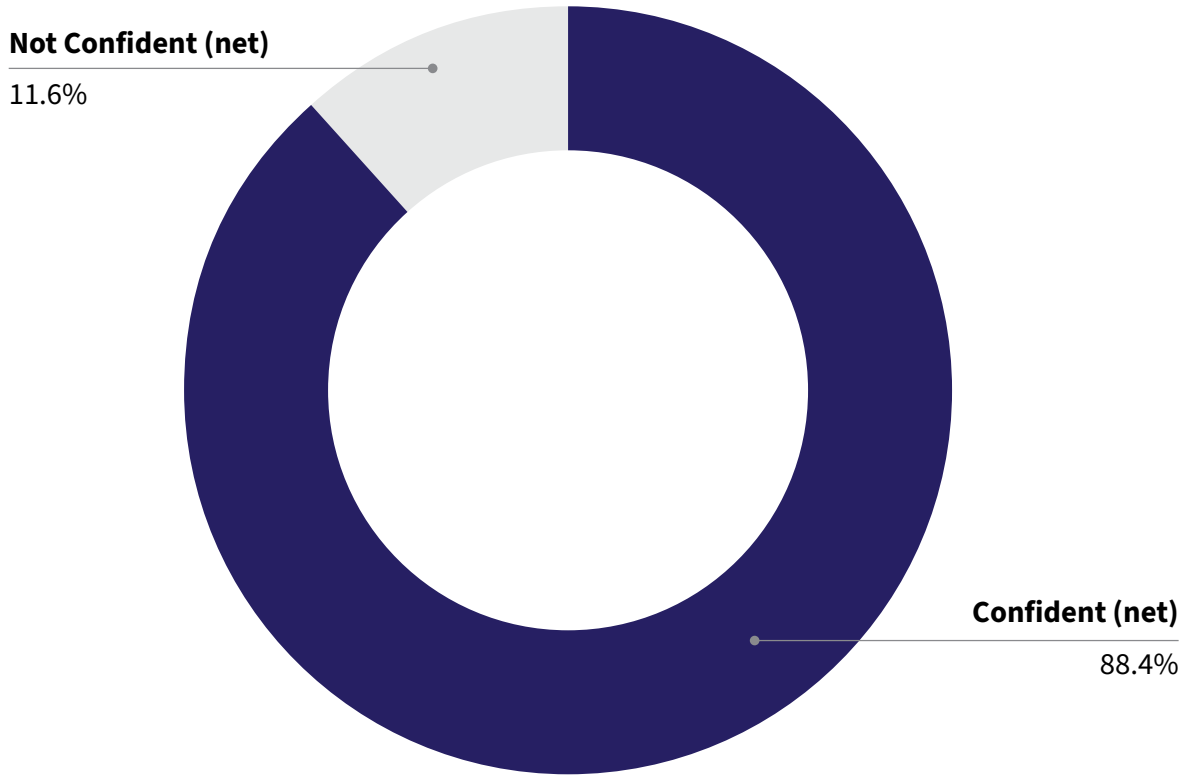
Organizations are experiencing more ransomware attacks than they've reported in previous years, and they're increasingly likely to pay the ransom. The $22 million payment a health insurer allegedly made in response to a February 2024 attack on one of their subsidiaries is a cautionary tale as these worrying trends suggest that many organizations remain unprepared for ransomware, which exposes them to significant risk.

> 58% of respondents experienced 6 or more ransomware attacks in the 12 months prior to the survey

> 91% of respondents paid at least one ransom over the same period

> The number of respondents who never pay the ransom is plummeting year over year, with just 8% saying they never pay

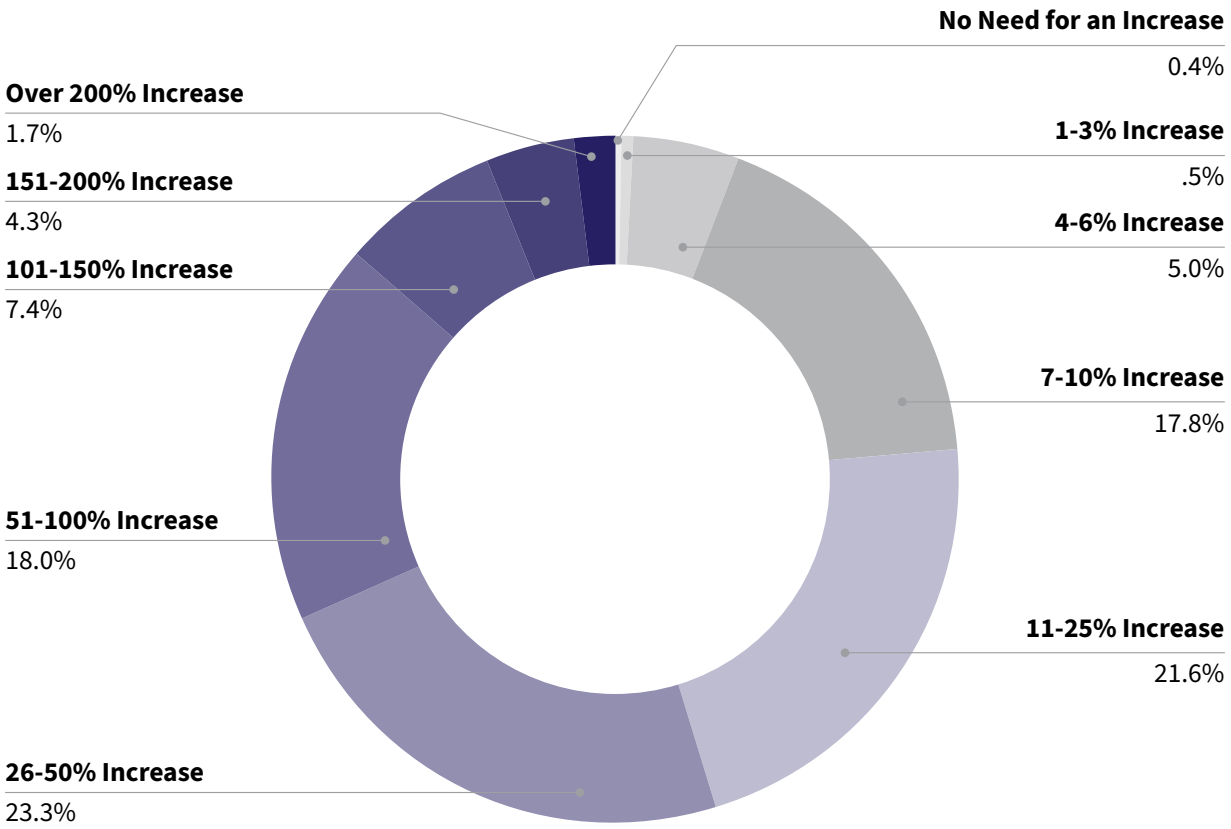
How confident are you, if at all, that your organization is effectively managing cyber risk?



CYBERSECURITY BUDGETS

Perhaps not surprisingly, most cyber and IT leaders want more budget. 31% of respondents say they need more than a 50% budget increase to effectively manage and mitigate cyber risk. This conflicts with the high levels of confidence they reported.

Required Increase in Budget for Effective Cyber Risk Management



CYBER HYGIENE

Leaders' responses to questions about cyber hygiene show cracks in the foundation of cyber confidence.

- Nearly 1 in 2 respondents' organizations are still running at least one insecure network protocol that threat actors are known to exploit in ransomware and other cyberattacks
- 51% of respondents say more than half of the cybersecurity incidents at their organization are related to poor cyber hygiene

SECURITY RESPONSE AND RESILIENCE

Respondents' answers to questions about incident downtime and response times to critical vulnerabilities were mixed. While there's certainly room for improvement, there are also positive signs.

- Average incident downtime is 56 hours, more than two full days
- However, 65% of respondents say their organization takes less than a week to respond to critical vulnerabilities, well within CISA guidelines

THE STATE OF CYBER RISK MANAGEMENT

There's no clear front-runner when it comes to the barriers organizations face to effectively manage cyber risk or the approaches they use to assess it. High executive involvement suggests, however, that organizations take cyber risk seriously.

- 50% of organizations say their biggest barrier to effective cyber risk management is due to either people, processes, or technology
- Organizations employ a variety of methods to assess cyber risk, including regular executive management team meetings, regular penetration testing or red teaming exercises, and threat modeling assessments
- 59% of respondents say their organization's leadership teams are moderately or very involved in cyber risk governance

A Hopeful Outlook

Despite the challenges and issues our survey uncovered, organizations are making positive strides in the way they manage cyber risk that give reason to be hopeful about the future. Our results suggest that cyber risk management is a maturing discipline, and organizations are increasingly looking to AI to help manage and mitigate cyber risk. Respondents are employing diverse practices to assess their cyber risk exposure, from red teaming and threat modeling to third-party assessments, and C-level involvement in cyber risk management is high. Altogether, this suggests that organizations are increasingly recognizing that cyber risk is business risk and are acting accordingly.

Ransomware

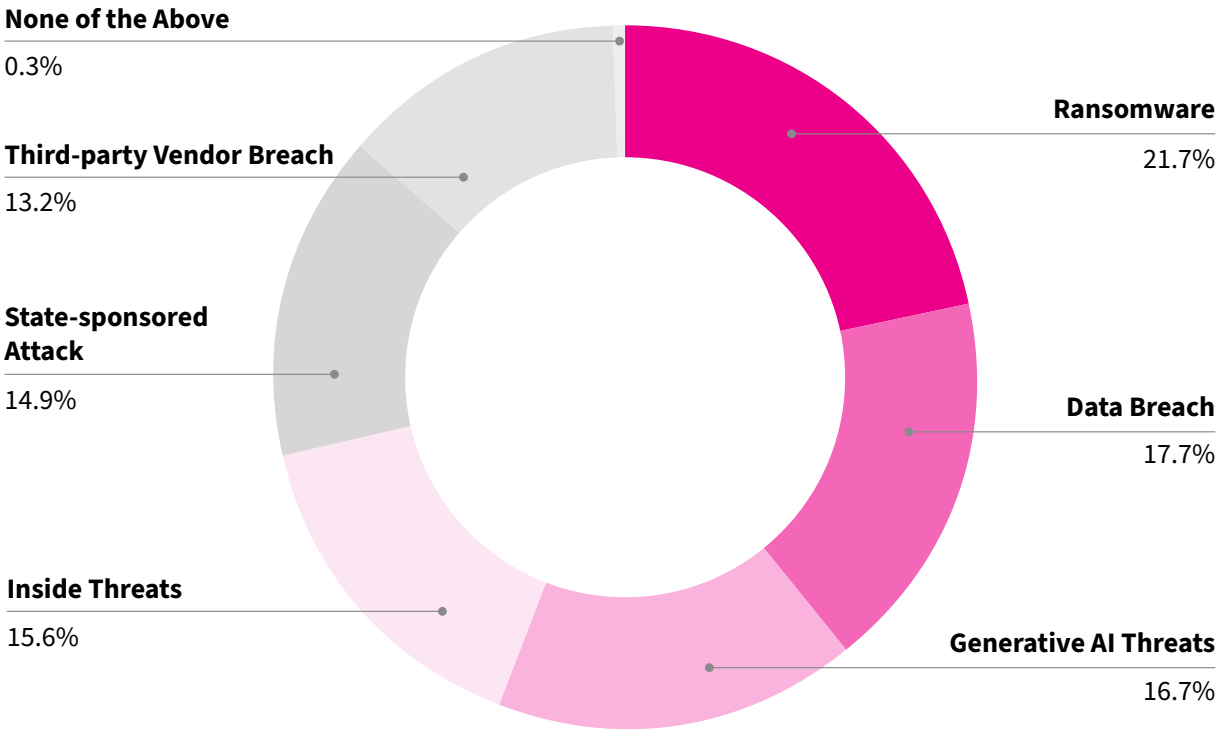
Organizations' responses to questions about ransomware suggest they may be ill-prepared for these incidents, and therefore, that they may be overly confident in their organization's ability to manage and mitigate cyber risk. Their responses also strongly suggest that they lack the network visibility required to detect and stop ransomware attacks in their early stages, before threat actors can achieve their objectives.

Ransomware is one of the largest challenges organizations identified. When asked to choose **which scenario posed the biggest risk to their organization, nearly 22% selected ransomware**, more than any other response.

Our data shows that ransomware is on the rise: **58% of organizations experienced 6 or more incidents[1] in 2023**, up 32% year over year.

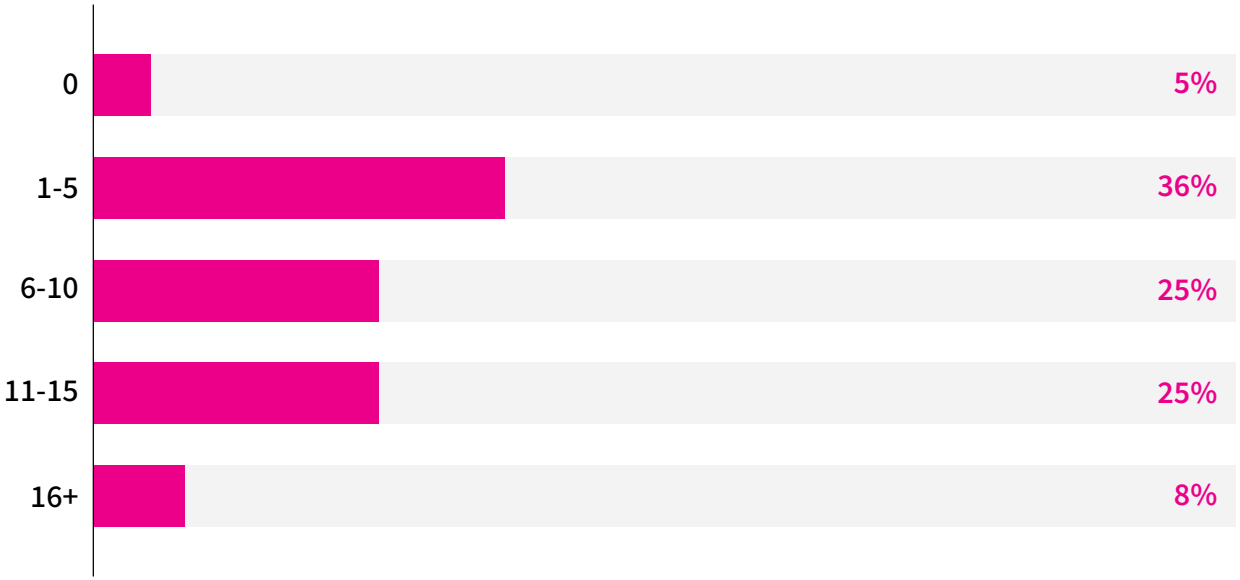
Ransomware is growing increasingly inevitable as the number of organizations stating they've experienced zero ransomware incidents has dropped—9% rebuffed ransomware in the 2023 survey results, compared to 5% in 2024. **On average, respondents experienced nearly 8 ransomware incidents**, including both successful and unsuccessful attacks, in the last year.

Which scenario poses the biggest risk to your organization?



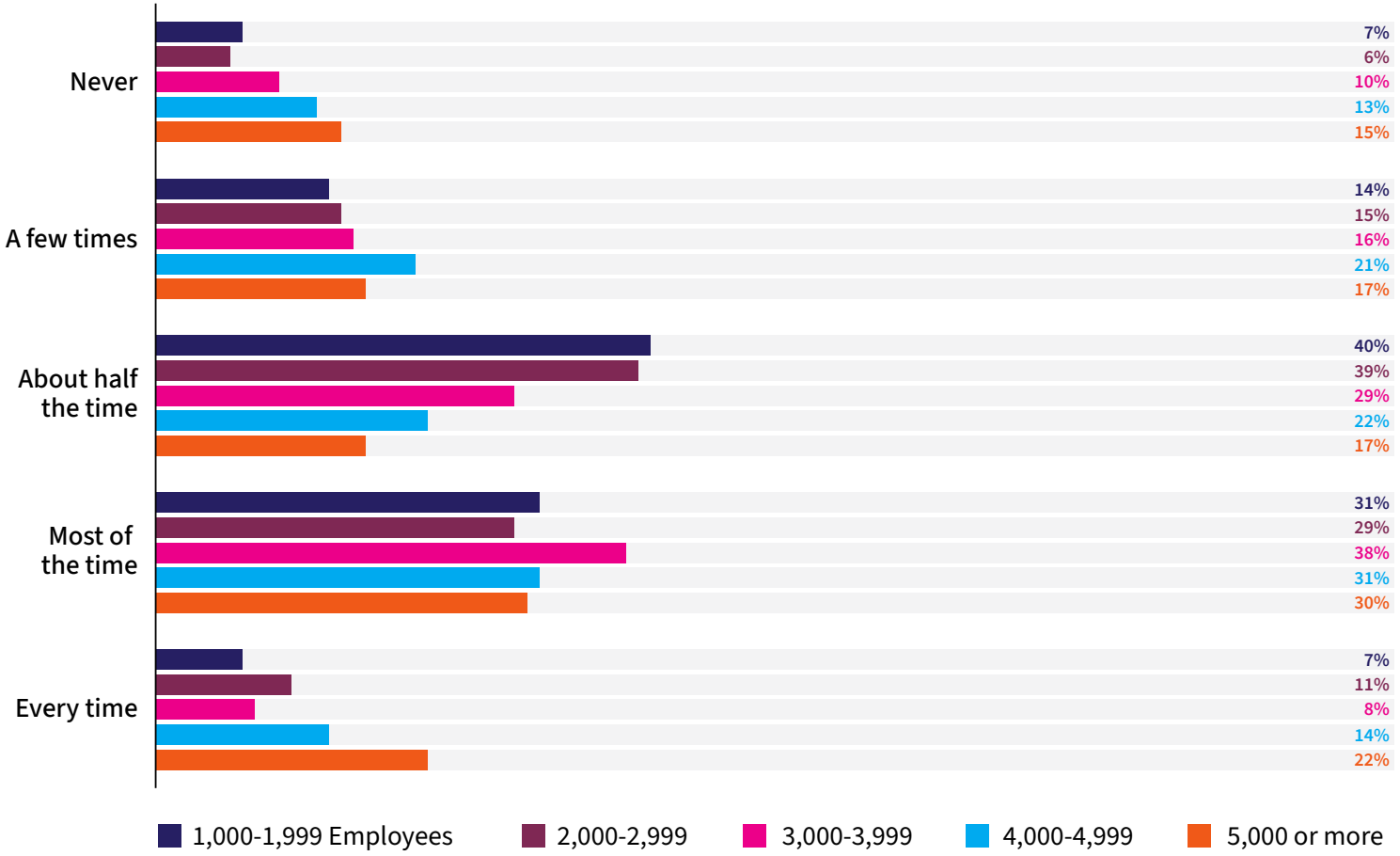
1. While the survey didn't define an incident as a successful ransomware attack, based on the numbers reported by survey respondents, we take "incident" to mean an attempted ransomware attack.

Number of Ransomware Incidents Experienced in the Last 12 Months



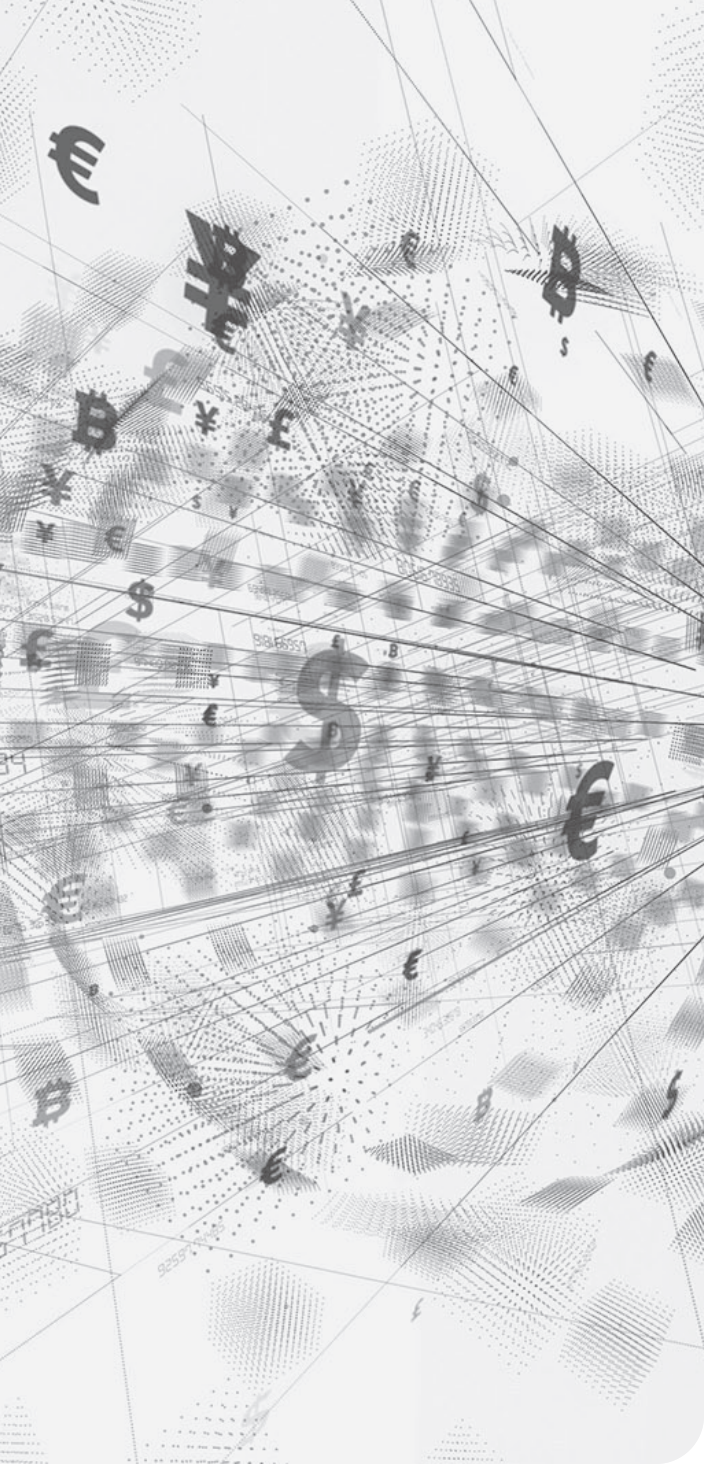
In another worrying trend, ransom payments are becoming larger and more frequent despite government and industry efforts to discourage them. Nearly every organization we surveyed paid at least one ransom last year (91%) and 75% of respondents say they paid more than half the time. The number of organizations never having paid a ransom has significantly decreased in a shocking downward trend—in the 2022 survey results, 28% of respondents never paid the ransom, compared to 17% in 2023 and 9% in 2024.

How often did your organization pay the ransom?



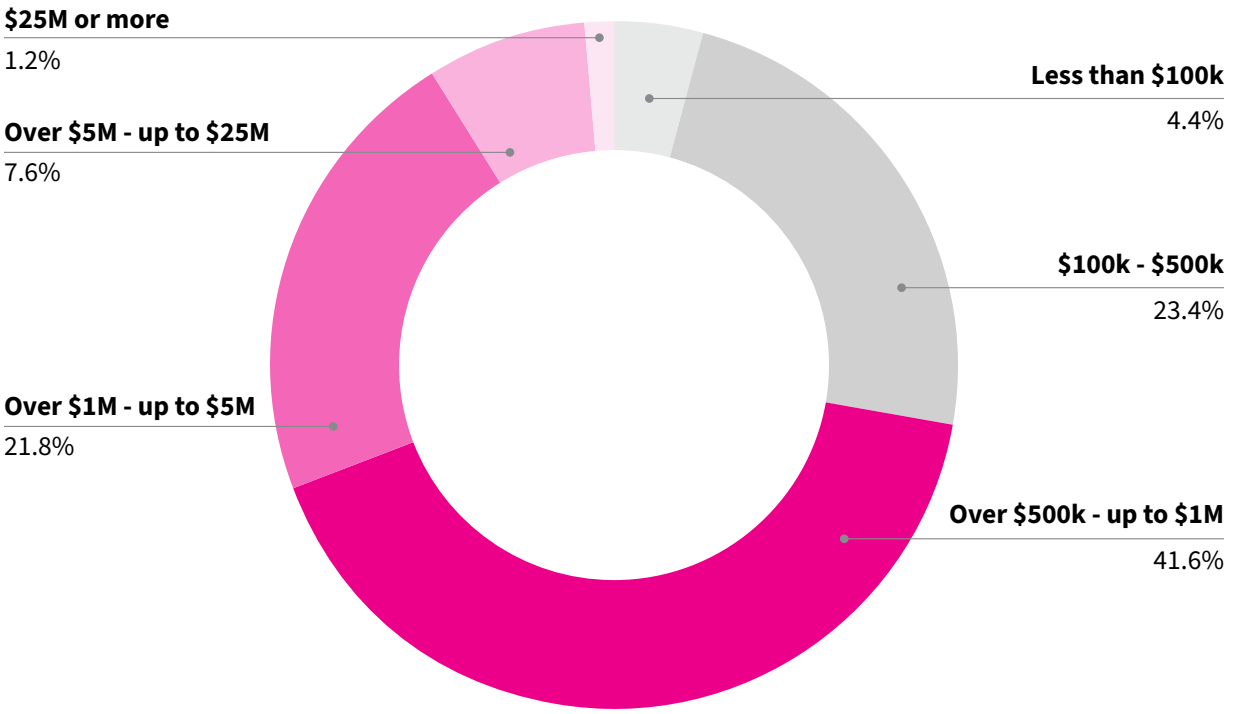
We suspect more organizations are paying ransoms because they can't afford not to pay. This could be due to a variety of factors. For one, they may lack the business and operational resilience to weather a ransomware attack. So they pay the ransom out of desperation or necessity, believing that paying the ransom provides them with the quickest path back to restored business operations. And when people's health or lives are at stake, some organizations have no choice but to pay.

But this strategy is likely to backfire: Paying the ransom doesn't guarantee an organization will get its data back. Moreover, research shows that organizations that have fallen victim to a ransomware attack are six times more likely to be targeted again over the next three months. Our survey data backs this up, with 90% of respondents experiencing at least two ransomware incidents in the last year.



And repeat ransom payments add up: On average, respondents paid nearly $2.5 million in ransom payments in 2023.

Total Ransomware Payments in 2023



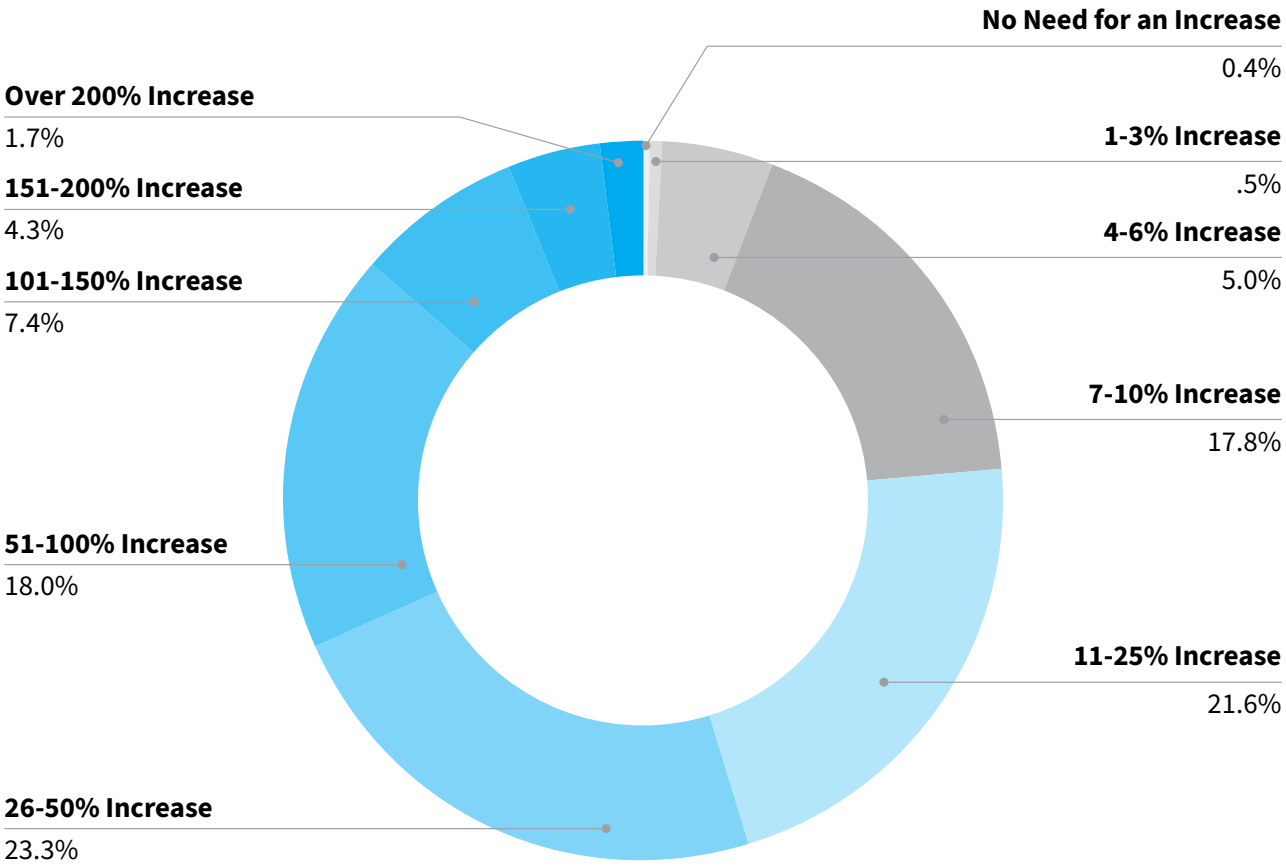
Paying the ransom only gets you the decryption key (and there's no guarantee of that); you'll still need to cover the cost of incident response and remediation, customer notifications and credit/identity theft monitoring (if certain personal or payment card data was compromised), and any potential regulatory fines and legal fees, which can add significantly more to the total cost of the breach.

It's likely that ransomware attacks will increase over the remainder of 2024 and into 2025, as threat actors tied to nation-states use ransom payments to finance military operations or further political goals. These groups are highly sophisticated: They target specific organizations and know how large of a payment their victims can afford.

Cybersecurity Budgets

On average, respondents say they need a 48% increase to their cybersecurity budget to effectively manage and mitigate cyber risk. Nearly a third (31%) would like more than a 50% increase.

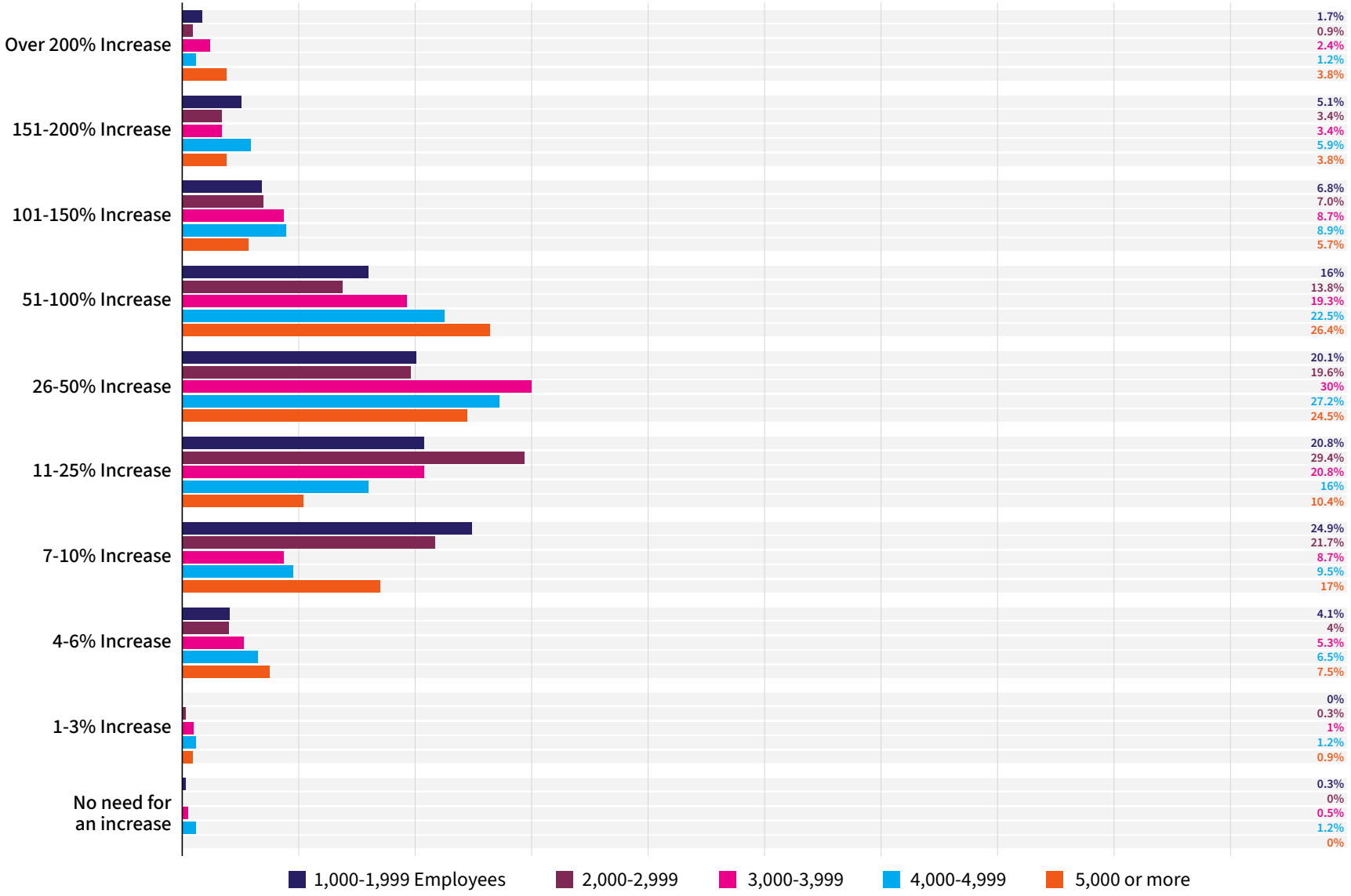
Required Increase in Budget for Effective Cyber Risk Management



The fact that so many respondents say they need significant increases to their budgets undercuts their claims about their confidence levels.

The larger the organization, the more their security or IT leaders would like to increase their budget. Larger organizations typically carry more risk, as they have a bigger attack surface to protect and often must comply with more regulatory requirements.

Required Increase in Budget for Effective Cyber Risk Management



INDUSTRY VERTICALS

When we examine industry verticals, a few interesting trends emerge.

Respondents in the agricultural industry seek the most aggressive budget increases: **44% want more than a 50% increase and 27% want to more than double their budget.** This is a highly regulated industry—disruptions to food production can have disastrous consequences—and many organizations are transitioning to operational technology (OT) and internet of things (IoT) devices on the factory floor.

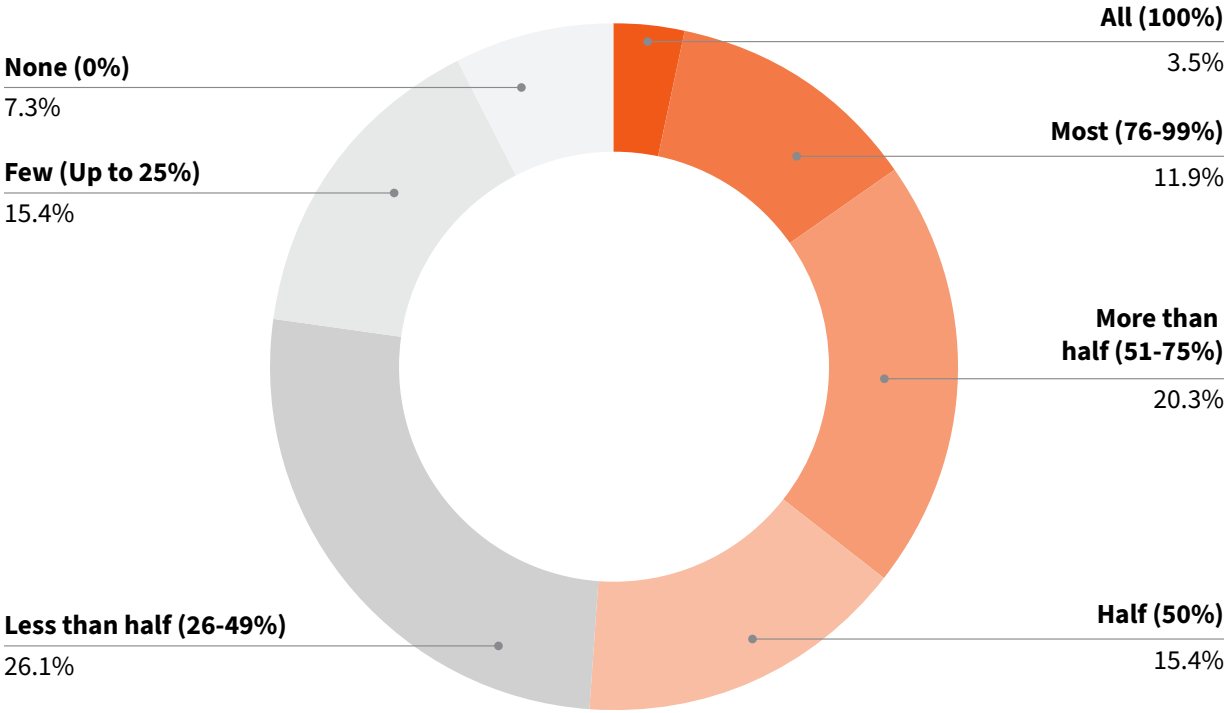
Governmental organizations follow closely behind, as **41% seek more than a 50% increase in budget and 6% (the greatest proportion by industry) want to triple their budget.** These organizations must comply with security mandates, like the Federal Zero Trust Strategy in the United States.

Conversely, respondents in manufacturing, construction, and utilities seek the smallest budget increases: **42% want no more than a 10% increase.** This seems surprising because this industry includes critical infrastructure and complex OT environments. However, these organizations tend to have relatively high security maturity, as indicated by their responses to questions about security hygiene.

Cyber Hygiene

While cyber hygiene is improving, survey data shows that this area remains a significant source of risk exposure, particularly in the agriculture, education, and government sectors.

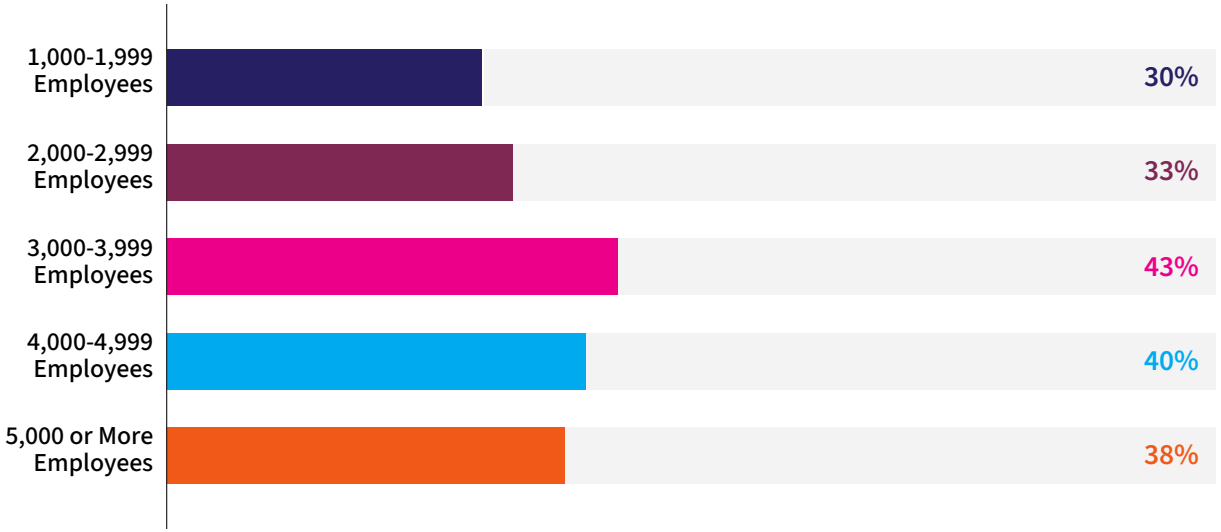
Proportion of Cybersecurity Incidents Related to Poor Cyber Hygiene Practices



Just over half (51%) of respondents say more than half of cybersecurity incidents at their organization are due to poor cyber hygiene, though our survey data shows this figure trending downwards over the past three years. Cyber hygiene seems to follow a bell-shaped curve when plotted against organizational size, with smaller organizations performing the best and midsize organizations lagging behind.

Cyber hygiene seems to follow a bell-shaped curve when plotted against organizational size, with smaller organizations performing the best and midsize organizations lagging behind.

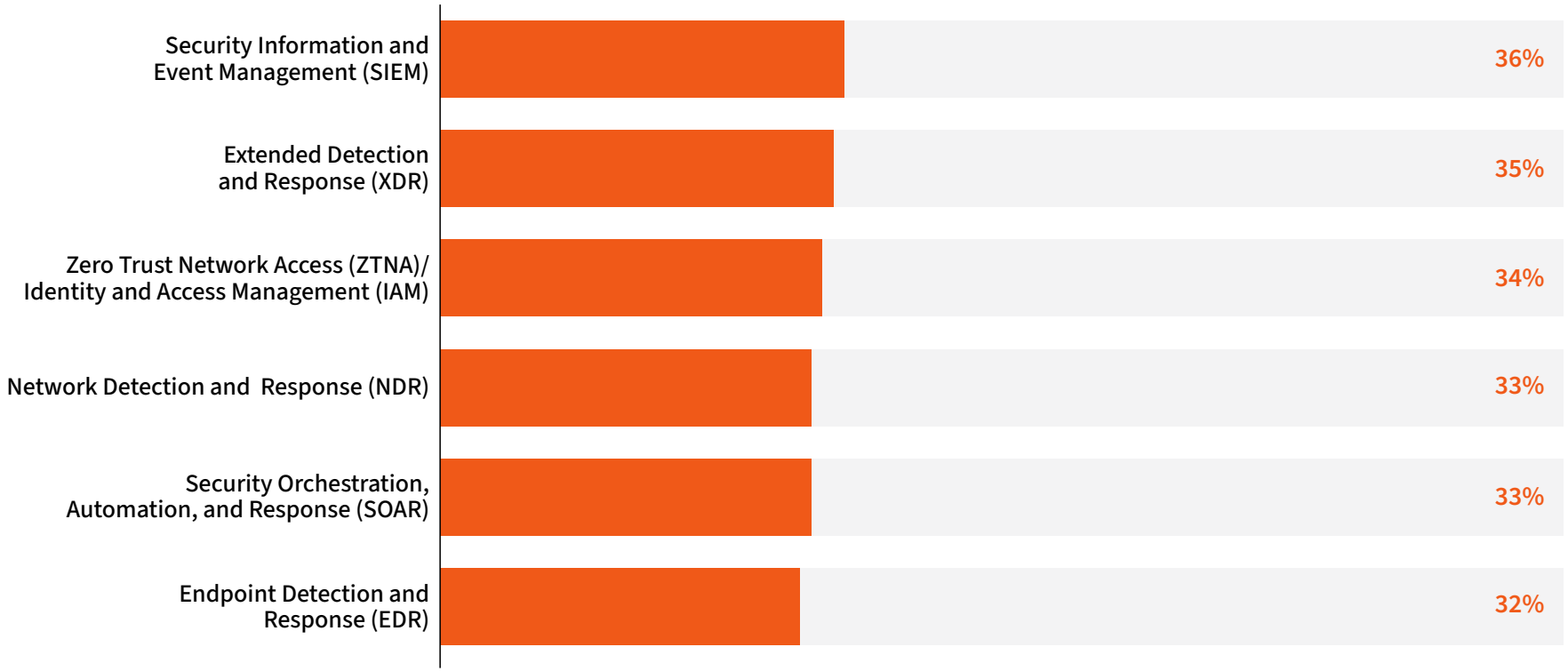
Percent of Organizations Where More Than Half of Cybersecurity Incidents Are Related to Poor Cyber Hygiene



Examining the results by industry shows that cyber hygiene issues are lightly correlated with the size of budget increases an organization seeks. In the agriculture sector, 51% of respondents say more than half of cybersecurity incidents stem from poor hygiene. A similar proportion (48%) from the government and education sectors say the same. While agricultural and government organizations seek to reconcile this with large budget increases, educational organizations are asking for less—only 31% seek more than a 50% increase. Those in manufacturing, construction, and utilities, on the other hand, seem to have their cyber hygiene under control—only 17% say more than half of incidents are linked to poor hygiene.

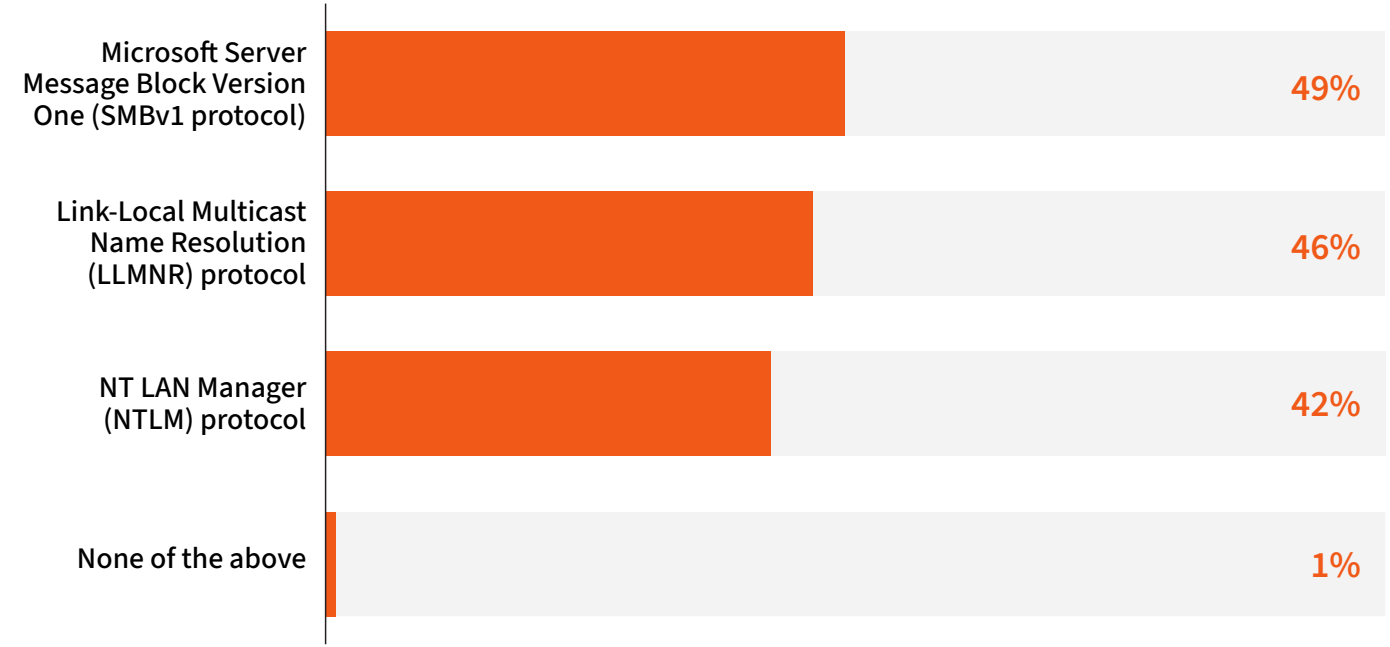
Other survey questions corroborate a trend of improving hygiene, albeit with room for improvement. Security technology adoption is growing, though only around a third of respondents currently have deployed or plan to deploy any individual solution. The second-most popular solution was extended detection and response (XDR), which brings together the capabilities of best-of-breed endpoint detection and response (EDR), network detection and response (NDR), SIEM, and SOAR solutions. Zero trust network access and identity and access management, which placed third, also rely on NDR to reach their full security potential, making NDR an essential investment for organizations planning to implement a range of solutions.

Which of the following solutions do you currently have deployed or plan to deploy within 12 months?



Respondents are also relying less on certain insecure network protocols, but their use still remains somewhat common.

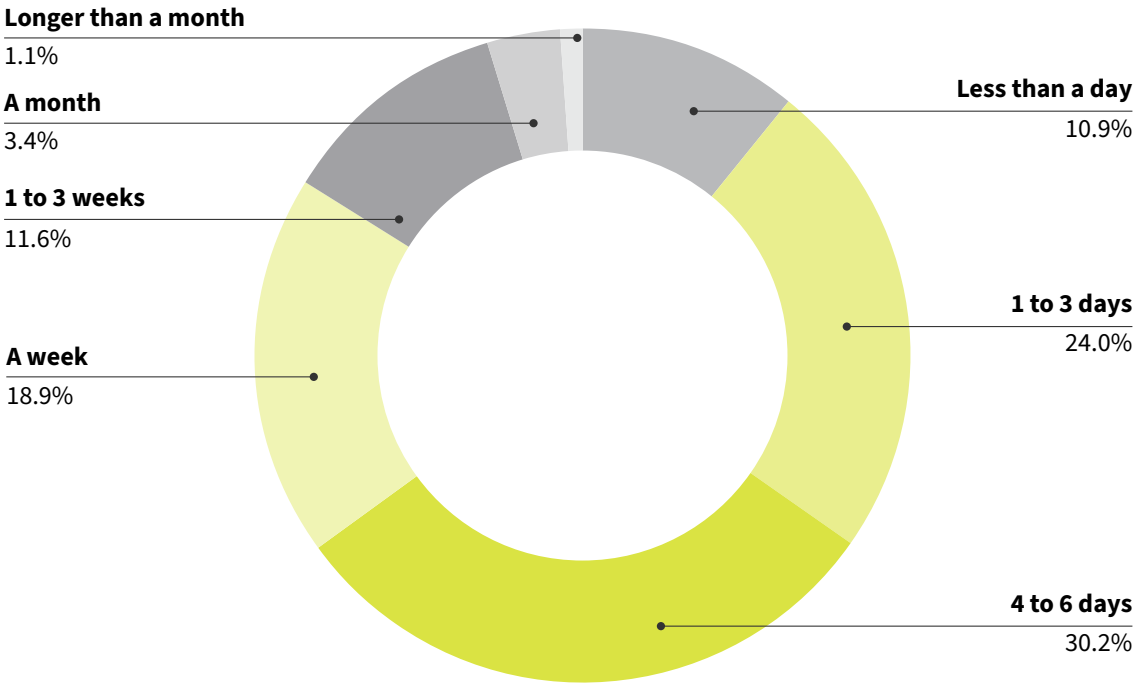
Percent of Organizations with Instances of Insecure Protocols



Security Response and Operational Resilience

Response times to critical vulnerabilities were noteworthy. The number of respondents who take longer than a month to respond to vulnerabilities is trending downwards from past years, and 65% of respondents take action in less than a week, well within the CISA recommended time frame of 15 days.

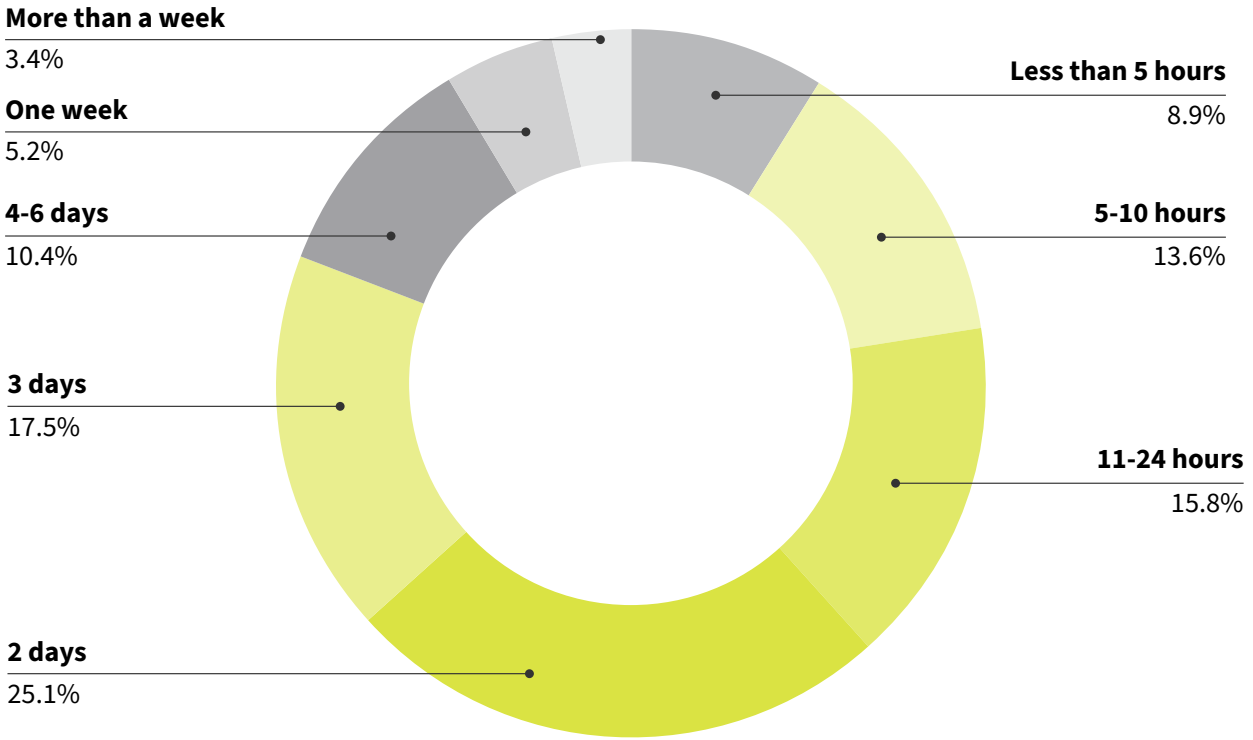
Response Times to Critical Vulnerabilities



Based on respondents' answers to questions about the average amount of downtime their organizations have experienced per cybersecurity event and the amount of time it takes them to respond to critical vulnerabilities, we believe many organizations continue to be hampered by a lack of visibility. This is despite investments in vulnerability management, endpoint detection and response (EDR), and security information and event management (SIEM) tools. The challenge many organizations face is a lack of adequate network visibility. If you can't see what's happening on your network, it's much harder to identify and remediate vulnerabilities, which increases organizations' exposure to cyberattacks and the disruption they cause.

However, these improvements are hobbled by long downtimes: The average amount of downtime organizations experienced from security incidents was 56 hours. Data describing the cost of downtime varies, but it won't be cheap: Research from the Uptime Institute in 2022 shows that "over 60% of failures result in at least $100,000 in total losses," while the share of outages that cost upwards of $1 million increased from 11% to 15% between 2019 and 2022. A survey conducted by ABB in 2023 puts the median cost of downtime at nearly $125,000 per hour—a total of $7 million for a 56 hour outage.

Average Downtime per Incident in 2023



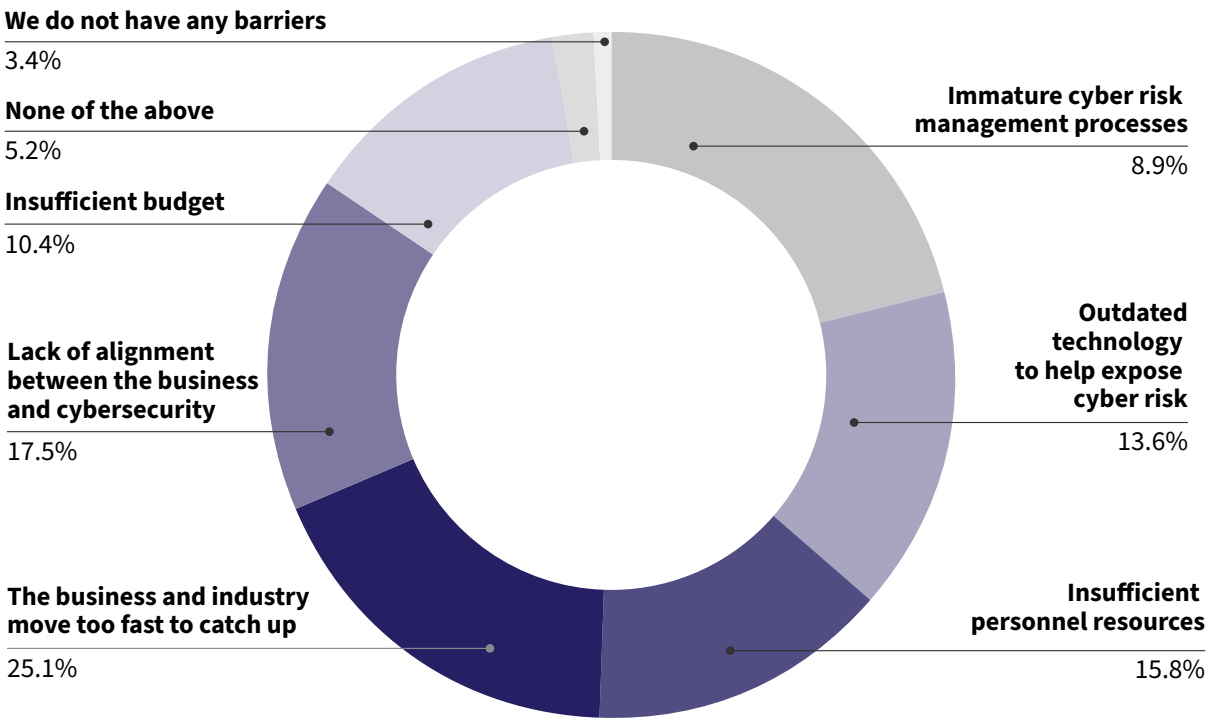
The State of Cyber Risk Management Practices

Every organization is unique, and the risks they face are, too. Organizations are divided on what their largest barrier to effective cyber risk management is, but there's room for optimism as organizations use a variety of methods to assess risk and the majority of executives are moderately or very involved in cyber risk governance processes. Respondents are also looking to AI to help lift the burden on their teams.

Just over 50% of respondents say their biggest barrier is related to either insufficient people, immature processes, or outdated technology. Conversely, 47% of respondents say their largest barrier is business-related.

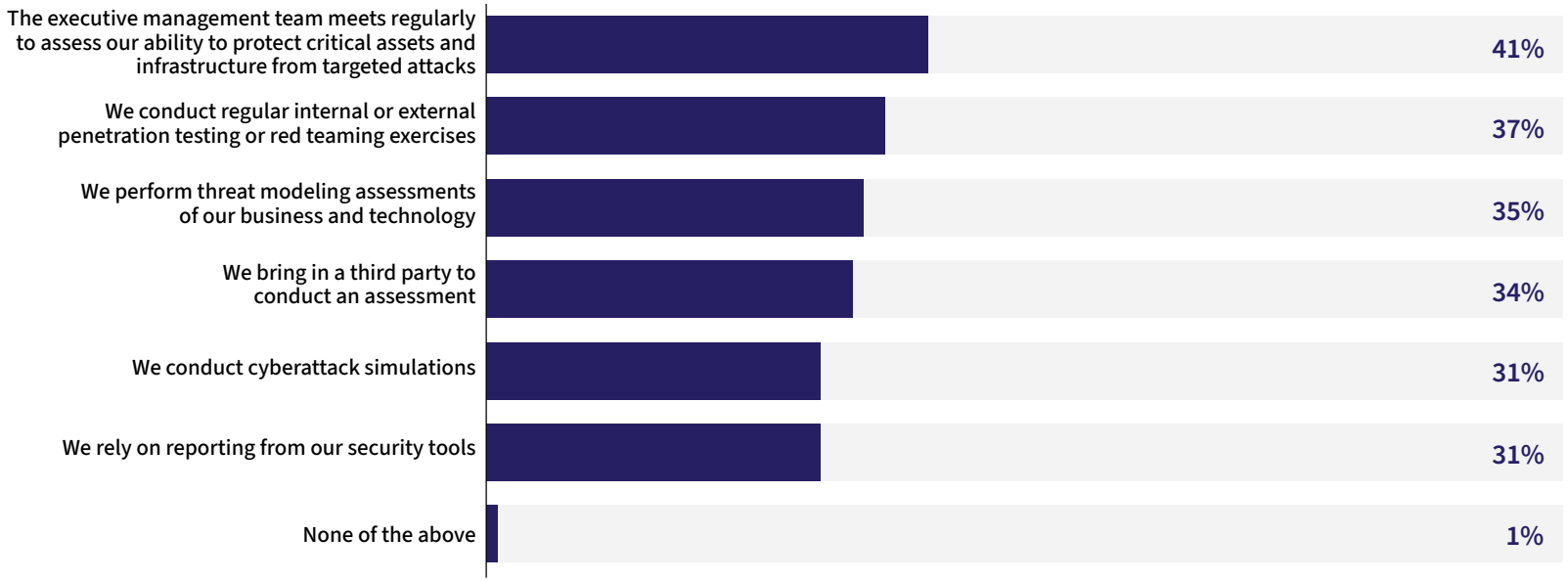
Despite the fact that, on average, respondents seek a **48% increase in their cybersecurity budget**, insufficient budget is cited as the largest barrier to effective cyber risk management by only 13% of respondents. This goes to show that budget is not the magic bullet for cybersecurity woes. More money can always be made available if you can show how it will help, but it's just as important to fix broken practices.

Barriers to Effective Cyber Risk Management



Numerous Approaches for Assessing Cyber Risk Exposure

Popularity of Assessment Methods for Cyber Risk Exposure

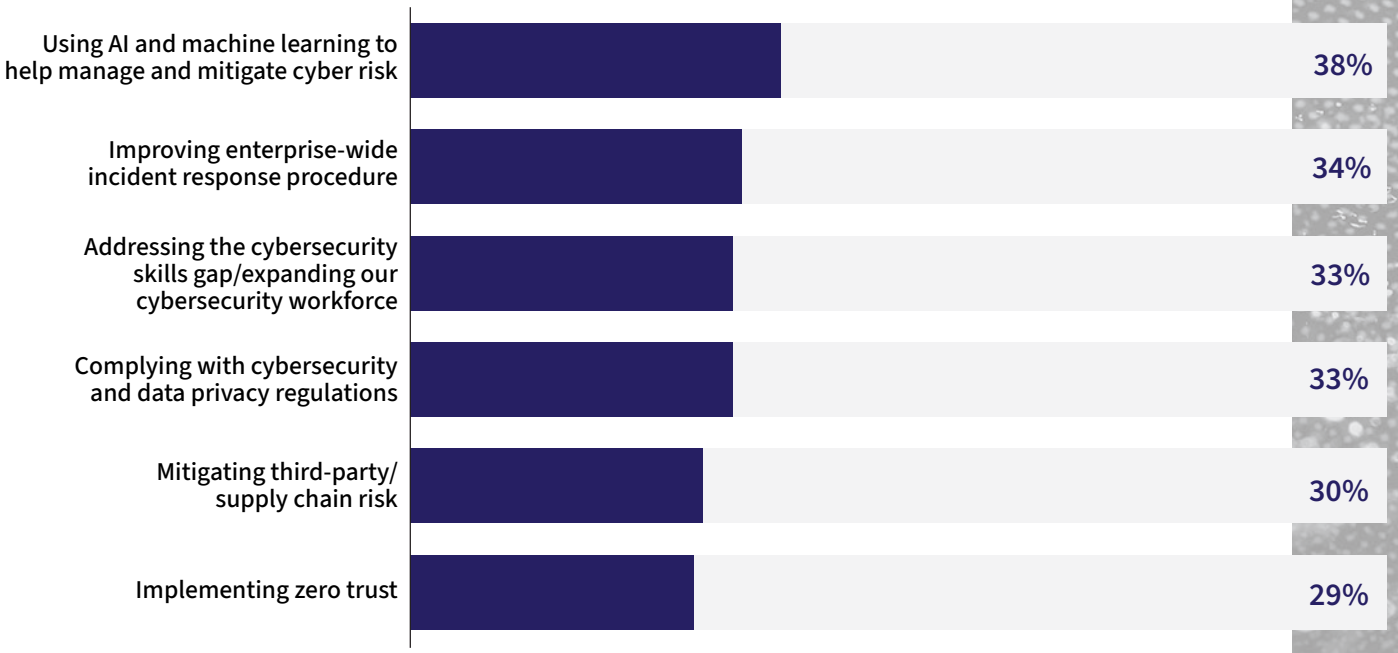


Organizations have many viable options when it comes to assessing cyber risk. Respondents could select all methods they use to assess their risk exposure, and results show fairly similar levels of adoption for each. Since each organization faces unique risks, it follows that their methods for assessing those risks will be, too.

The Role of AI

Organizations seem to realize that investments in AI-powered solutions can help lift the burden on understaffed teams. When asked to name their top three cybersecurity priorities for 2024, 38% of respondents chose “using AI and machine learning to help manage and mitigate cyber risk.” This corroborates our findings in The Generative AI Tipping Point report, which showed employees at 73% of surveyed organizations use AI tools with some regularity.

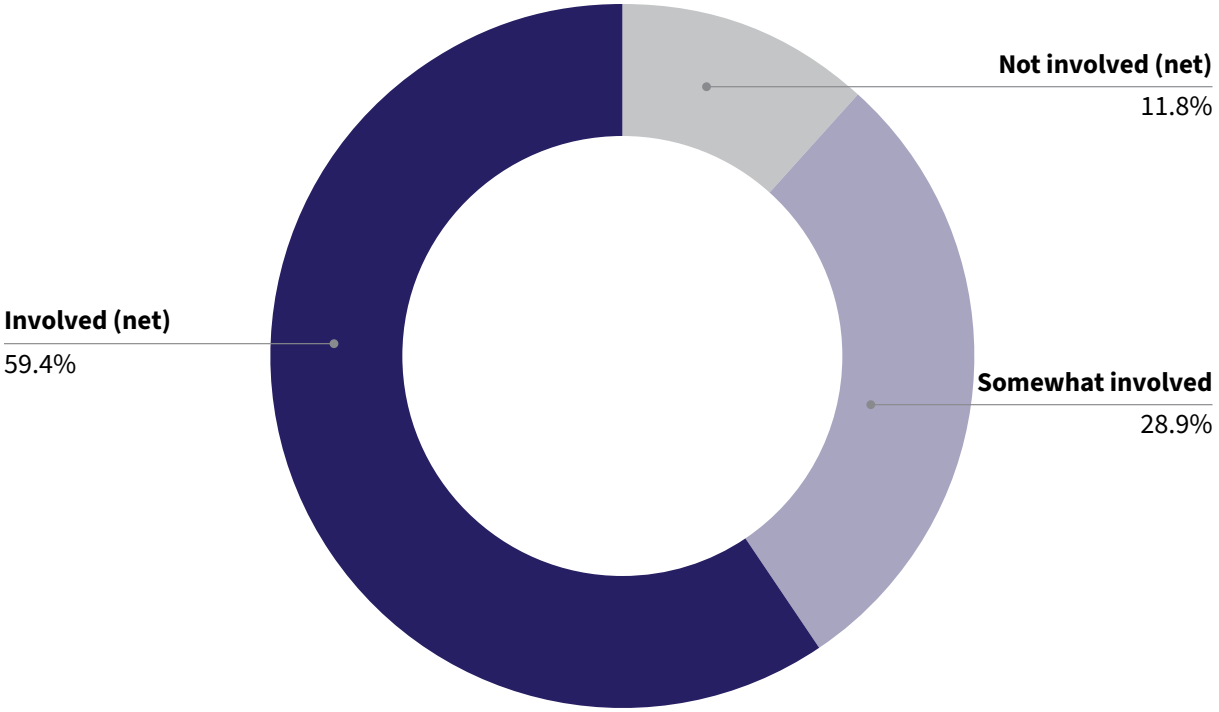
Top Cybersecurity Priorities for 2024



Executives Are Making Cyber Risk Their Business

Executives and board members increasingly recognize that cyber risk is business risk and their involvement in cyber risk governance shows in our data. The majority of respondents (59%) say their executives are moderately or very involved.

Executive Involvement in Cyber Risk Governance



Conclusion

While net confidence is high among respondents, most (53%) are only somewhat confident that their organization is effectively managing cyber risk. Our data shows that respondents should be cautiously optimistic about cyber risk, with cyber hygiene improving, increasing investments in security technology, and high levels of executive involvement.

But unchecked confidence is unwarranted as ransomware attacks—and payments—are growing and the average downtime per incident remains uncomfortably long.

We hope this data helps you benchmark your organization's cyber risk management practices and challenges against other organizations.

How RevealX Helps Buy Down Cyber Risk

At ExtraHop®, our mission is to help organizations reveal cyber risk and build resilience. We do that by leveraging the power of the network to give organizations broad risk visibility into the cyber threats, vulnerabilities, and network performance issues cropping up across their complex and rapidly expanding IT estates.

The network delivers a powerful source of truth, transparency, and history into cyber threats and performance issues across all assets in an enterprise—from cloud, to on-premises, to endpoints. The network is where adversaries first land, where they expand their reach, establish command and control communications, move laterally, and employ living off the land binaries and scripts to evade detection. The network sees everything, shows everything, and maintains a packet record of every place attackers try to hide. And unlike endpoint agents, logs, and other security tools, the network can't be evaded or disabled.

Network visibility is essential to cybersecurity and IT operations. Threat actors are turning to techniques that common cybersecurity controls can't catch. RevealX™ allows you to see into all of your traffic—north-south, east-west, even encrypted traffic—so you can quickly spot malicious activity before it creates massive risks for your organization. You can't get this level of visibility from any other security control.

A consistent theme across the results of this survey is that a lack of network visibility can lead to lost revenue from downtime and costly ransom payments. Organizations seeking to gain greater insight into activity on their network and buy down their cyber risk should strongly consider RevealX. RevealX sees all network traffic, including encrypted network traffic, and automatically discovers, classifies, and inventories all devices and cloud assets connecting to an organization's network, enabling security teams to spot vulnerable devices, insecure protocols, and unpatched software with ease.

RevealX leverages cutting-edge SSL and TLS 1.3 decryption, AI, and detections powered by machine learning to help lean teams investigate smarter and stop threats faster. Security and performance monitoring use cases enable teams to reduce downtime due to both security incidents and network performance issues. As a leading NDR solution, RevealX also enables SIEM, EDR, and zero trust implementations to reach their fullest potential and organizations to move at the speed of risk.

The complete network visibility provided by RevealX also helps address one of the largest challenges organizations identified in this survey: ransomware. RevealX offers dozens of detection capabilities that map to known ransomware TTPs across 12 categories of the MITRE ATT&CK framework, so you can stop attackers before they can cause damage.

Better visibility into threats and vulnerabilities leads to better decision-making and faster response times. And a clearer understanding of your organization's attack surface and risks leads to more effective controls to manage and buy down that risk. RevealX offers unmatched visibility to bolster your cyber confidence and doesn't come at the cost of a ransom payment.

Methodology

For the third edition of this report, ExtraHop® worked with Censuswide in early 2024 to conduct a survey of IT and security decision-makers from around the world. Censuswide selected 1,102 respondents at the director level or above who worked at organizations with greater than 1,000 employees and who provided input in their organization's security and IT decisions.

ExtraHop surveyed 251 decision-makers each from the United States and the United Kingdom, 150 decision-makers each from France and Germany, and 100 decision-makers each from Singapore, Australia, and the United Arab Emirates.

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at extrahop.com.

EXTRAHOP®