KASEYA

CYBERSECURITY SURVEY REPORT

2024

NAVIGATING THE NEW FRONTIER OF CYBER CHALLENGES

IDAGENT
A Kaseya COMPANY

The velocity and volume of cybersecurity attacks continues to shape business and IT strategies, as the cost and consequences of data breaches rise.

The widespread adoption of artificial intelligence (AI) by both threat actors and defenders is arguably one of the most significant industry game-changers. At the same time, IT professionals face a myriad of challenges, ranging from budget pressures to digital transformation initiatives, further fueling the need to future-proof IT and cybersecurity investments and infrastructure.

IT professionals face a new frontier as they balance cybersecurity needs against hybrid workforces and accelerated dependencies on cloud-based applications and services, The Kaseya Cybersecurity Survey Report for 2024 sheds new light on these challenges, while providing IT professionals insights so they can safely navigate today's dynamic IT landscape.

EXECUTIVE SUMMARY

These key themes sum up of the most illuminating insights from this year's data.

1. Fewer companies are paying ransomware demands. Only 11% of victims claimed to have done so, which aligns with data suggesting that the impact of attacks is less severe, likely due to increased investment in backup and recovery technologies.

2. The percentage of organizations facing supply chain attacks has significantly decreased. In 2023, 61% of respondents reported experiencing such attacks, but this figure fell sharply to 19% in 2024.

3. The human element continues to be the weakest link in cybersecurity. An alarming 80% of respondents named a lack of training or bad user behavior as one of the biggest causes of cybersecurity challenges.

4. Cybersecurity maturity levels continue to rise, as evidenced by the increased investments in advanced security tools and services, such as EDR and MDR, which correlates to a reduction in incident costs and downtime.

5. Opinions on the impact and usefulness of AI in cybersecurity are decidedly mixed, with approximately one-third of survey respondents reserving judgement on the benefits of AI for defenders, which indicates skepticism remains around this emerging technology.

IT SECURITY BUDGETS ARE STABLE

Even in a time of strained budgets, survey respondents said they expect their organizations will continue to make investments in cybersecurity. Over 80% of our respondents said that they believe their IT security budget will remain the same or even grow in the next 12 months. Of those anticipating increases, a rise of up to 25% is the most common expectation. Continued investment in cybersecurity, even in challenging times, reflects the business world's recognition of the importance of cybersecurity for a company's continued success.

Do you expect your company's IT security budget to increase, stay the same or decrease in the next 12 months?

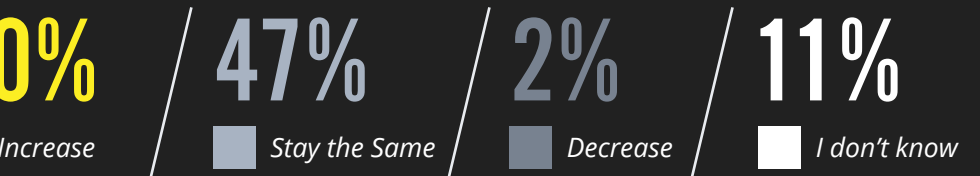


Figure 3

How much do you expect the budget for IT security to decrease in the next 12 months?

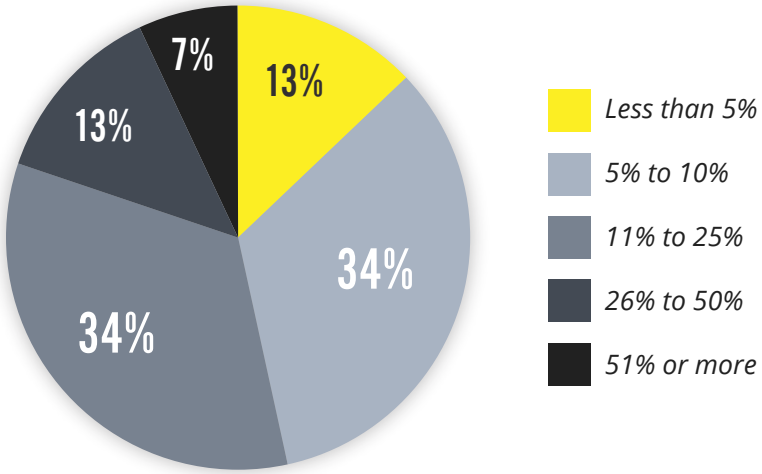


Figure 1

How much do you expect the budget for IT security to increase in the next 12 months?

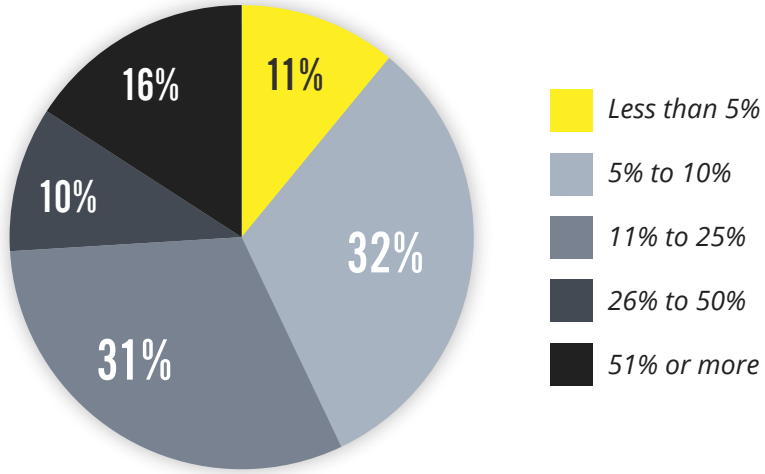


Figure 2

THE CHALLENGES BUSINESSES FACE IN THE DIGITAL BATTLEGROUND

IT professionals are tasked with the increasingly difficult prospect of securing networks, devices and data, while contending with the myriad of challenges involving user behavior and cyberattacks.

LEADING CYBERSECURITY ISSUES IMPACTING BUSINESS

A look at historical data gives us insight into which cybersecurity issues remain constant concerns and which are getting better – or worse.

Phishing remains the top issue for businesses, both historically (58%) and in the past 12 months (50%). IT professionals hold no illusions that phishing will be less of a problem in the future, as indicated in Figure 27. While we see some indications that businesses have experienced fewer issues in the past 12 months, it's important to note that some issues are evergreen and require ongoing vigilance.

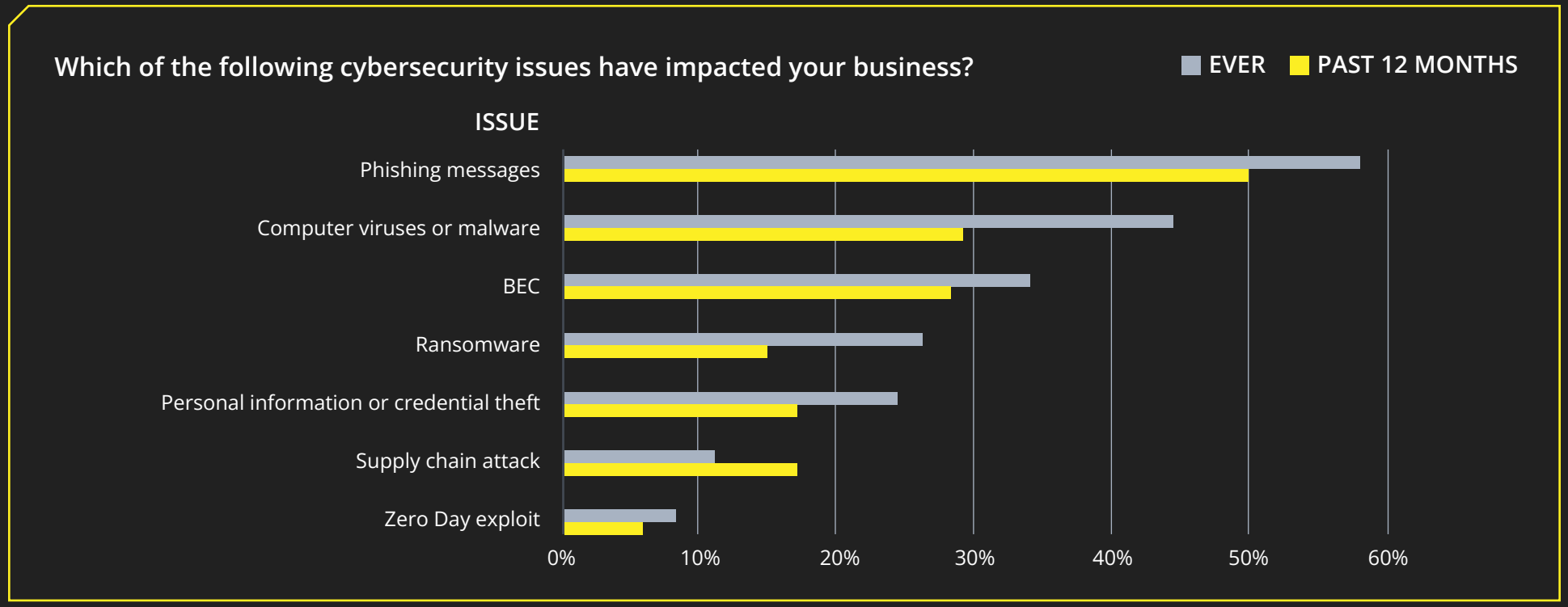


Figure 4

TOP THREE ROOT CAUSES OF CYBERSECURITY ISSUES

User-related security issues are the biggest causes of distress for IT professionals. The percentage of organizations citing lack of end-user or cybersecurity training as a root cause has increased by 16 percentage points from 28% in 2023 to 44% in 2024. Nearly half of the respondents also pointed to poor user practices or gullibility as a top cause of trouble, tripling from 15% in 2023 to 45% in 2024. Regardless of whether this is true, the perception of IT professionals is that users are the root of most cybersecurity trouble. This trend looks to continue in 2025, as seen in **Figure 28**.

What are the top three root causes of your cybersecurity issues?

ISSUE	2024	2023
Poor user practices/gullibility	*45%*	*15%*
Lack of end-user cybersecurity training	*44%*	*28%*
Lack of funding for IT security solutions	*33%*	*21%*
Insufficient security support for different types of user devices	*29%*	*26%*
Weak passwords or access management	*25%*	*10%*
Lack of executive buy-in for adopting security solutions	*23%*	*22%*
Lack of administrator cybersecurity training	*22%*	*25%*
Outdated security patches	*19%*	*13%*
Lack of defense solutions (antivirus)	*15%*	*28%*
Open Remote Desktop Protocol (RDP) access	*14%*	*13%*

Figure 5

TWO-THIRDS OF RESPONDENTS POINT TO LACK OF END-USER OR ADMINISTRATOR TRAINING AS A TOP SECURITY WOE.

IMPROVED CYBERSECURITY INCIDENT DOWNTIME

Downtime from cybersecurity incidents appears to be going down, with only 8% of respondent seeing two to three day downtimes in 2024, and only 7% of respondents being down for a full day. More than one-quarter of respondents didn't experience any downtime, and one in five didn't experience a cybersecurity incident at all.

This impressive time to recovery data speaks to an increased investment in incident response and backup solutions, as can be seen in **Figure 17** facilitating a faster, smoother recovery.

If you've experienced a cybersecurity incident, what was your total downtime?

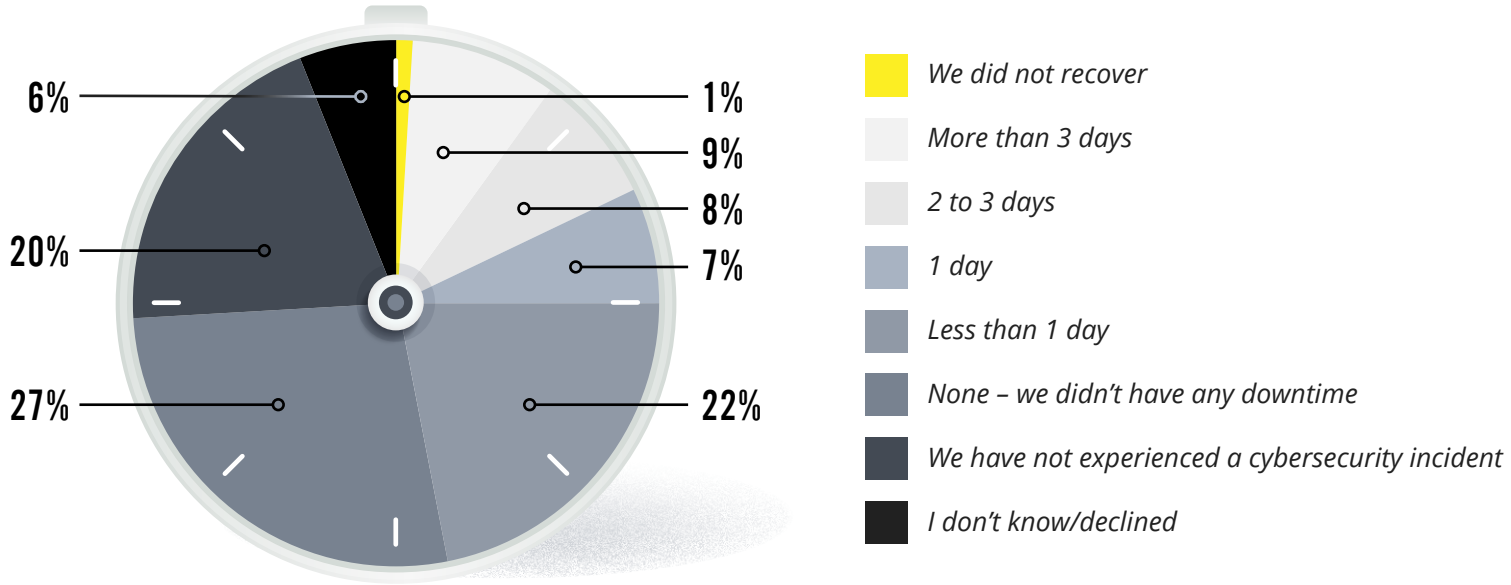


Figure 6

COST OF A CYBERSECURITY INCIDENTS

In 2024, businesses experienced fewer high-cost cybersecurity incidents compared to 2023. It is important to note that in 2024, we had a significant uptick in survey responses from larger organizations, which may reflect fast growth in the industry. The percentage of responses from companies with more than 3,000 employees more than doubled, increasing from 7% in 2023 to 17% in 2024. (Figure 31).

The investments that businesses are making in cybersecurity and incident response are paying off. The percentage of businesses reporting high-cost incidents ($250,000 to $500,000) dropped from 25% in 2023 to just 5% in 2024. This sharp decline could indicate that businesses are experiencing less severe attacks and have implemented better incident response controls to limit financial damage. Additionally, 35% of organizations reported no incidents in 2024, a significant improvement from 9% in 2023.

If you've experienced a cybersecurity incident, what was the total cost to the business, including lost revenue, lost productivity and recovery?

TOTAL COST OF A CYBERSECURITY INCIDENT	2024	2023
Less than $10,000	*22%*	*16%*
$10,000 to less than $50,000	*7%*	*17%*
$50,000 to less than $100,000	*10%*	*17%*
$100,000 to less than $250,000	*8%*	*18%*
$250,000 or more or less than $500,000	*5%*	*25%*
I don't know	*13%*	*4%*
We have not experienced a cybersecurity incident	*35%*	*9%*

Figure 7

IMPROVEMENTS IN RANSOMWARE RESILIENCE

Increased investments in cybersecurity are yielding positive results as evidenced by the reduced frequency and impact of ransomware attacks. By enhancing defenses with advanced tools and strategies, businesses are better equipped to prevent breaches and mitigate damage when they do occur.

RANSOMWARE PAYMENT

In a spot of good news, 56% of this year's survey respondents have not experienced a ransomware attack. However, that left 44% of respondents' companies facing a difficult choice: to pay or not to pay.

Many organizations have absorbed the message from experts and law enforcement that paying off cyber extortionists is a bad idea. Only 11% of survey respondents paid a ransom after an attack; 26% refused, indicating a shift toward alternative recovery methods. This growing resistance, driven by high costs and ethical concerns, reflects a broader focus on preventative measures and non-payment strategies. IT professionals also know they must remain vigilant about ransomware in the future.

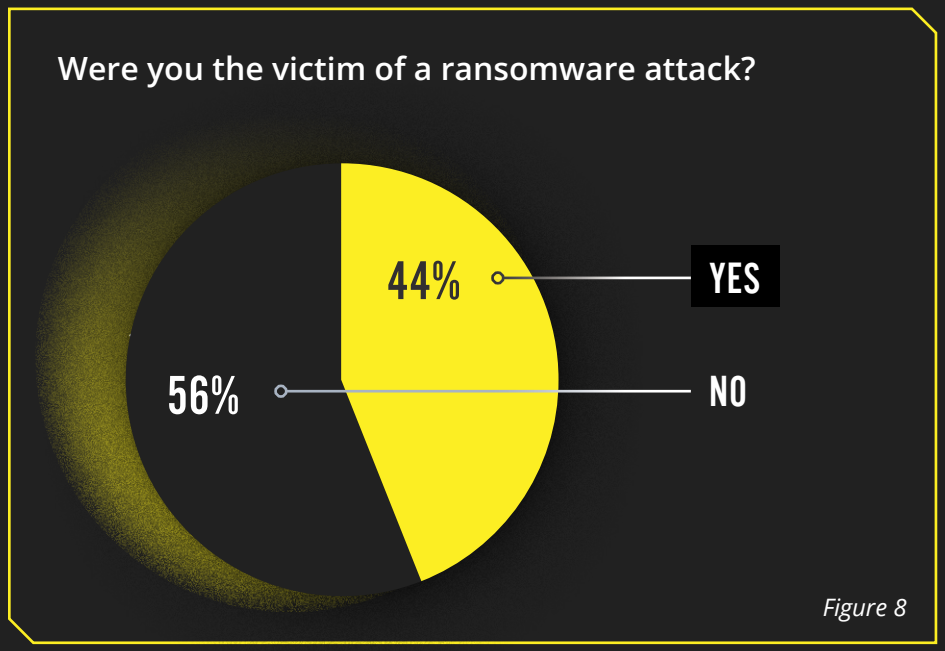


Figure 8

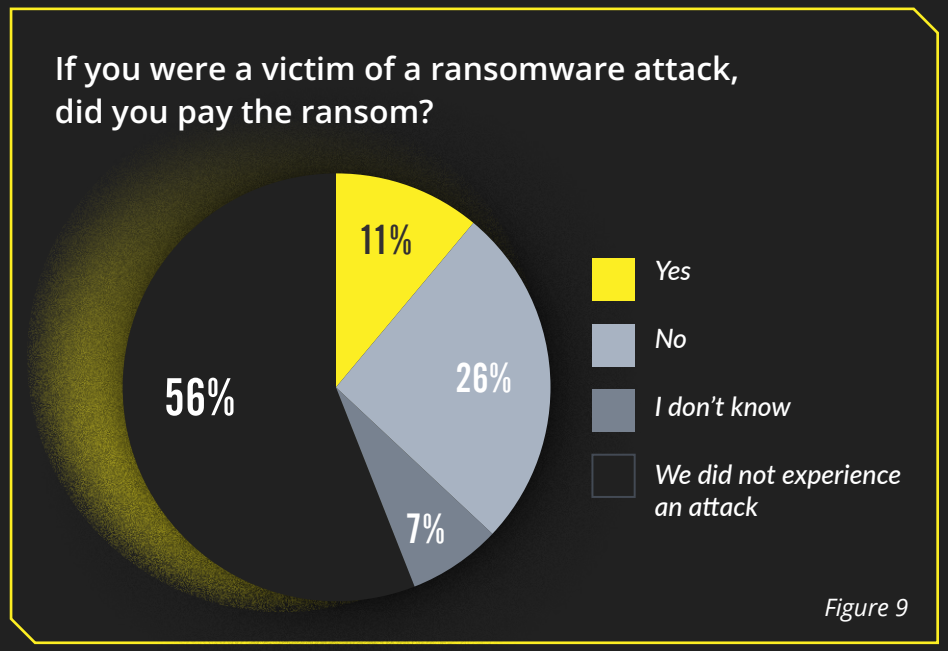


Figure 9

INCREASED RANSOM PAYMENTS

Organizations that chose to pay the ransom paid much more this year than they would have in 2023. There was a sharp increase in respondents indicating that their organization paid a ransom of $50,000. The decline in smaller ransom payments suggests that attackers are looking to increase their income by increasing their ransom demands.

Thinking about the ransomware attack you experienced, what was the cost of the ransom?

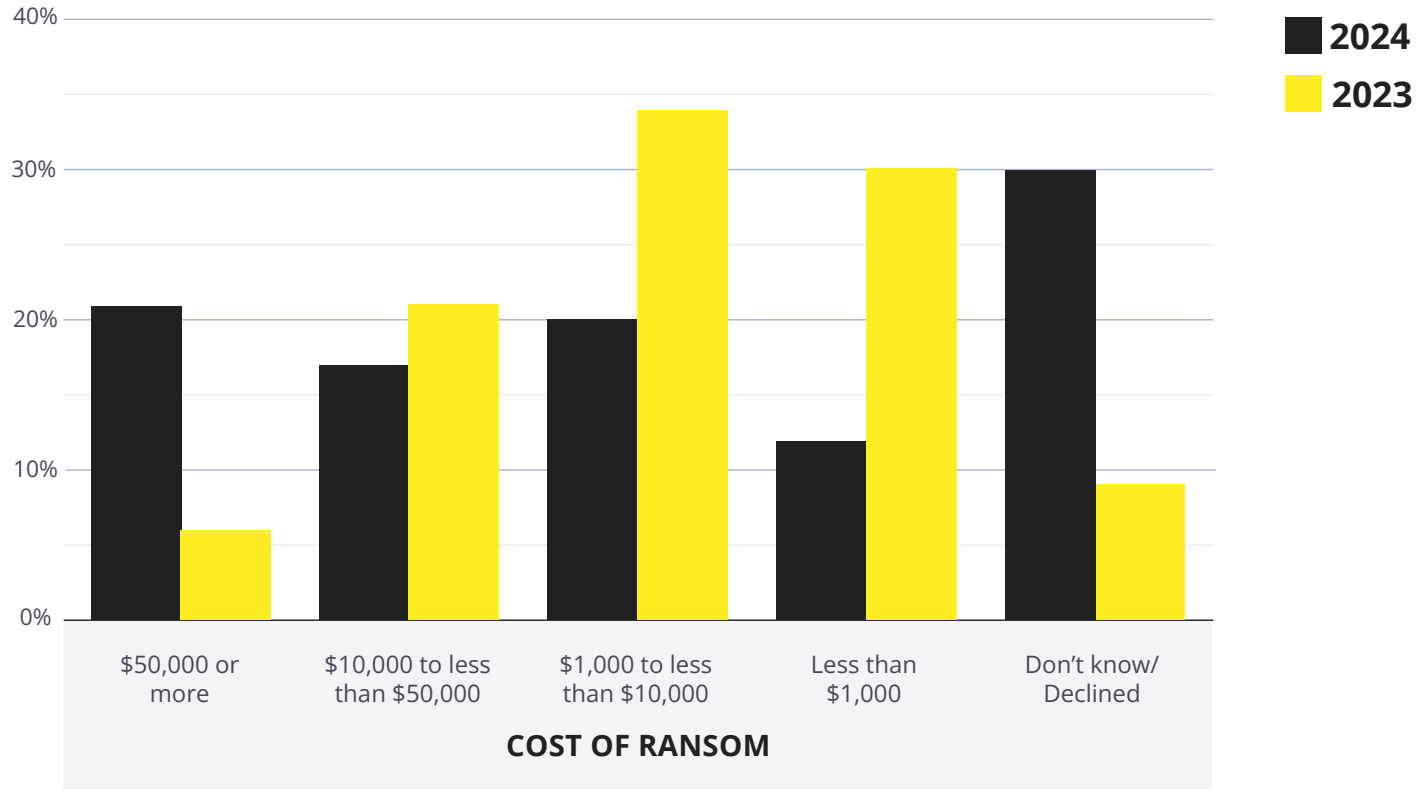


Figure 10

POST-RANSOM ACTIONS

Some encouraging news: Most organizations that experienced ransomware attacks were able to recover their data. More than two-thirds (69%) of survey respondents said their organizations were able to successfully decrypt their data after paying the ransom or by using other recovery methods.

Data loss remains a real possibility. Just over one-quarter of IT professionals said that their organizations decrypted only some of their data.

Which of the following best describes the actions you took after paying the ransom?

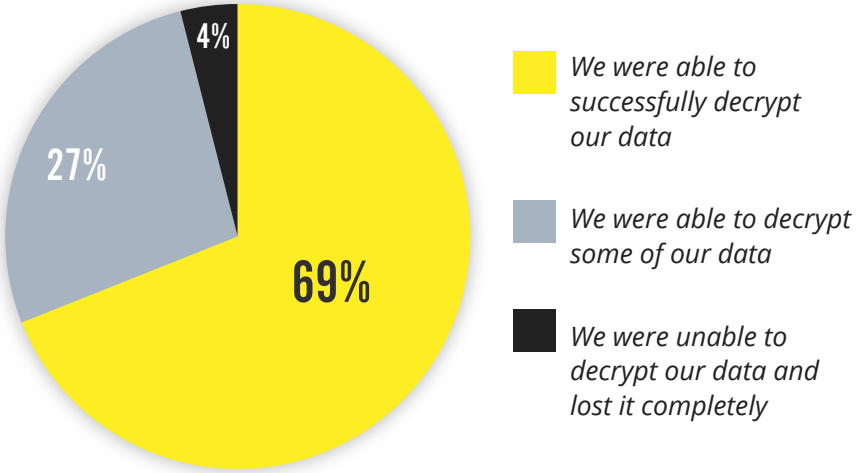


Figure 11

Companies that chose not to pay the ransom took various paths to recovery. Most respondents were able to perform a full recovery. This reflects a growing trend toward robust backup and recovery strategies, implying increased investment in comprehensive backup solutions to mitigate ransomware impact.

Which of the following best describes the actions you took after declining to pay the ransom?

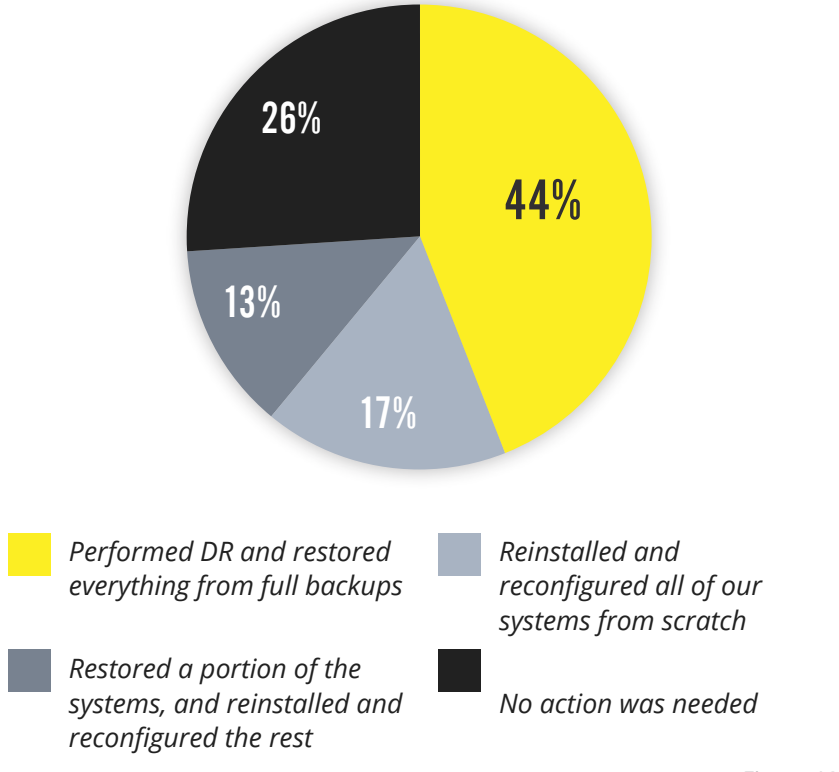


Figure 12

RANSOMWARE PREPAREDNESS

The good news: The impact of a ransomware attack has decreased. Only 7% of 2024 respondents said they believe a ransomware attack would have an extreme impact on their organization. This is a marked reduction from 2023. Those expecting only a "minimal impact" rose from 28% to 33%.

Overall, this suggests increased confidence in ransomware preparedness, with more organizations banking on their incident response and recovery plans to ensure less severe consequences if an attack occurs.

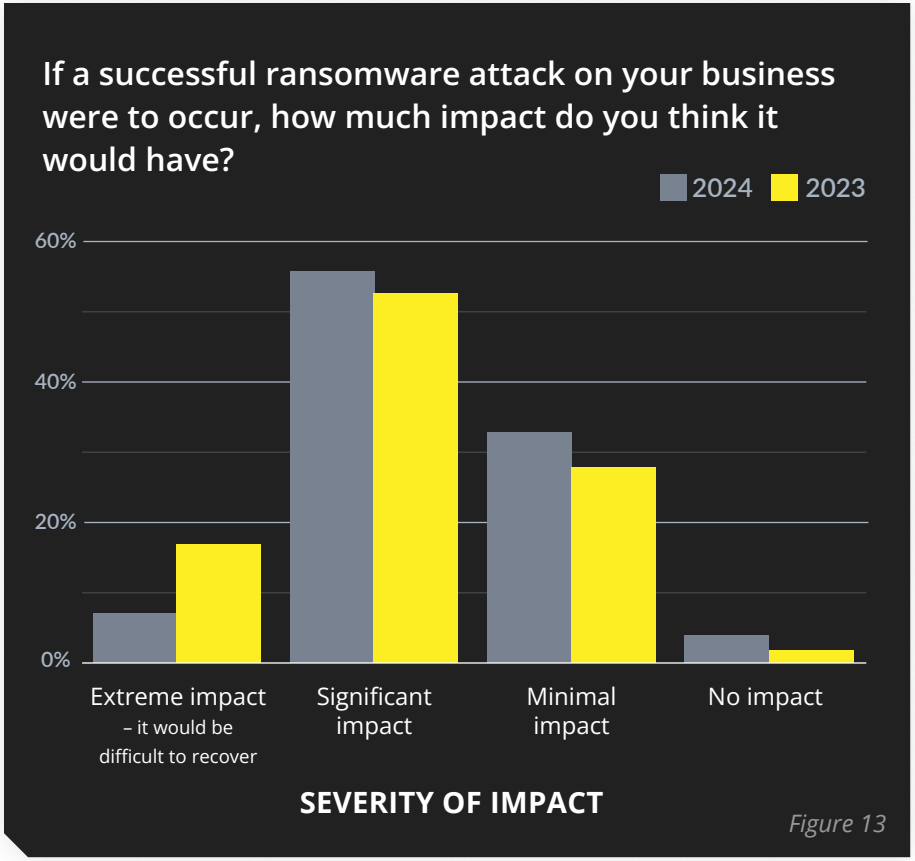


Figure 13

SUPPLY CHAIN ATTACKS

Businesses are getting a handle on supply chain risk, and it shows. The percentage of organizations experiencing supply chain attacks dropped dramatically. Last year, 61% of respondents said that their organizations had experienced a supply chain attack. That percentage plummeted to 19% this year. Respondents also do not anticipate supply chain risk to be a major attack vector in the next 12 months, as reflected in Figure 27. This dramatic decrease suggests a greater awareness of this risk and tracks with the increased investment in security illustrated throughout this survey.

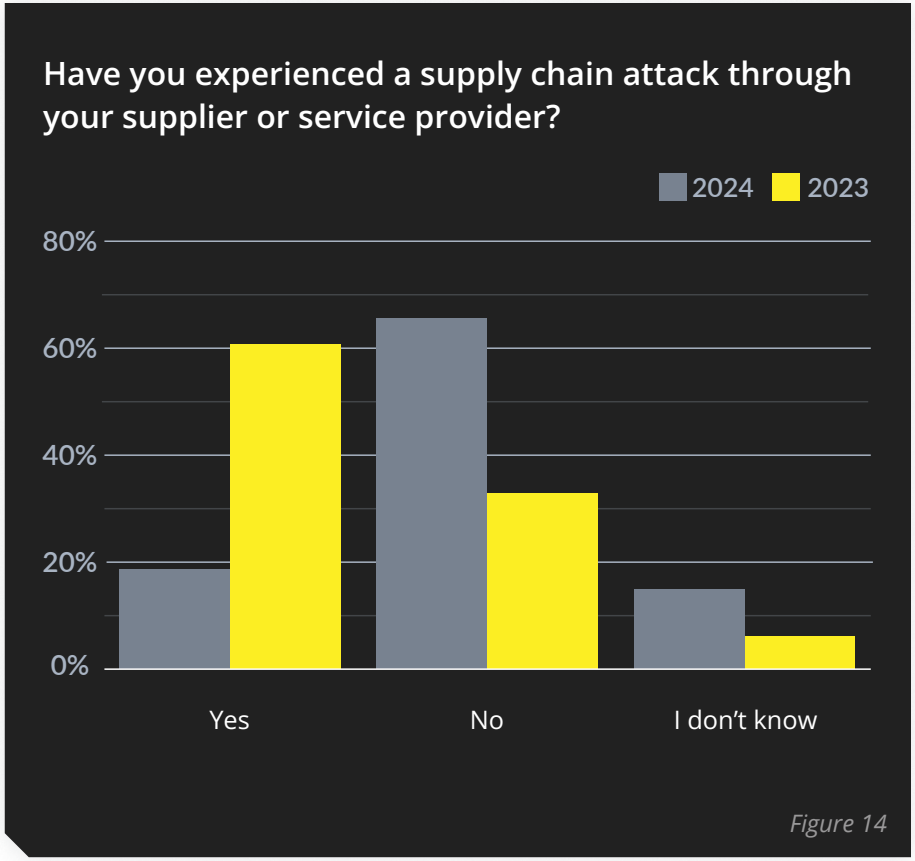


Figure 14

IS AI THE NEW FRONTLINE IN CYBERSECURITY OR JUST HYPE?

The AI revolution is here. Cybercriminals are all-in, leveraging advances in AI technology to mount more sophisticated cyberattacks at a faster pace than ever before.

AI's role in cybersecurity is a hotly debated topic. While advocates call it a game-changer for detecting threats faster and more accurately, critics question if its potential is overhyped, given its current limitations and evolving cybercriminal tactics. As cybercriminals increasingly use AI for more sophisticated attacks, the question remains: Are defenders ready to step into a new AI-driven future?

AI DEPLOYED FOR LAWFUL GOOD

As with any hot topic, IT professionals have widely varying opinions on the expected impact of AI on cybersecurity. Our survey respondents showed a generally positive outlook toward the role of AI in enhancing business security, with more than half of the respondents saying they believe that AI will help them be more secure.

However, doubt remains. Almost one-third of the IT professionals surveyed said they are uncertain about the impact that AI may have on their company's security. This split in perspectives highlights the need for more education and clarity around the benefits and limitations of AI in cybersecurity.

Do you believe AI will help you be more secure?

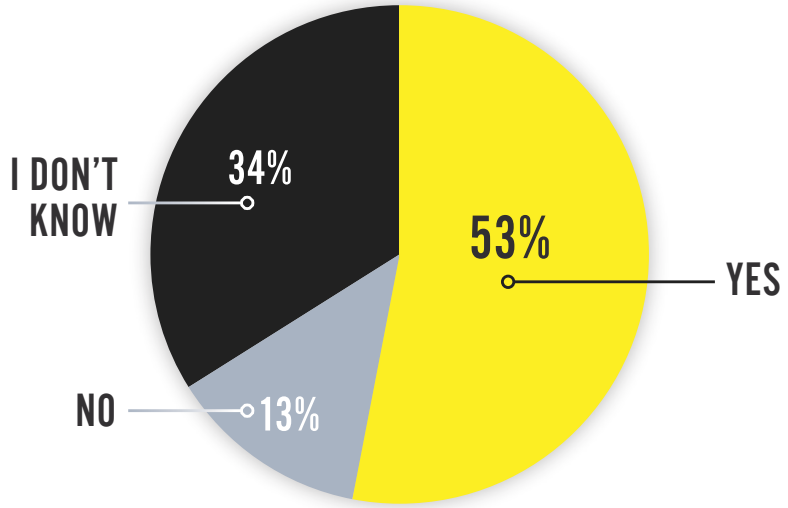


Figure 15

We gave respondents the opportunity to voice their sentiment about the impact of AI. Here are their answers.

What impact do you believe AI will have on your organization?

- AI helps improve productivity.
- AI can provide quicker accurate data analysis.
- Our antimalware solution uses predictive AI to evaluate threats.
- It will reduce human error.
- AI can offer better threat detection by analyzing successful attacks on our peers and determining if we have similar vulnerabilities.

How do you believe AI will benefit bad actors?

- AI helps make more believable phishing emails.
- It can be used to automate cyberattacks, making them more difficult to detect and respond to.
- Hackers can use AI to find vulnerabilities in systems or personalize phishing attacks.
- AI will provide more of the target's data and at a quicker pace. This will help them orchestrate a more robust and convincing attack.
- It will open more doors to social engineering attacks and make them seem even more realistic.

HOW BUSINESSES MANAGE THE THREAT LANDSCAPE

Today's quickly shifting threat landscape calls for a proactive approach to risk management through a smart array of defensive and diagnostic solutions. sophisticated attacks, the question remains: Are defenders ready to step into a new AI-driven future?

CYBERSECURITY FRAMEWORKS DEPLOYED

Cybersecurity frameworks provide a structured approach to identifying, managing and mitigating risks, ensuring that an organization can effectively protect its assets and respond to threats. NIST (40%) and Zero Trust (36%) are currently the most widely adopted cybersecurity frameworks among respondents.

THE MOST WIDELY USED FRAMEWORK IS NIST

Which of the following cybersecurity frameworks do you currently utilize?

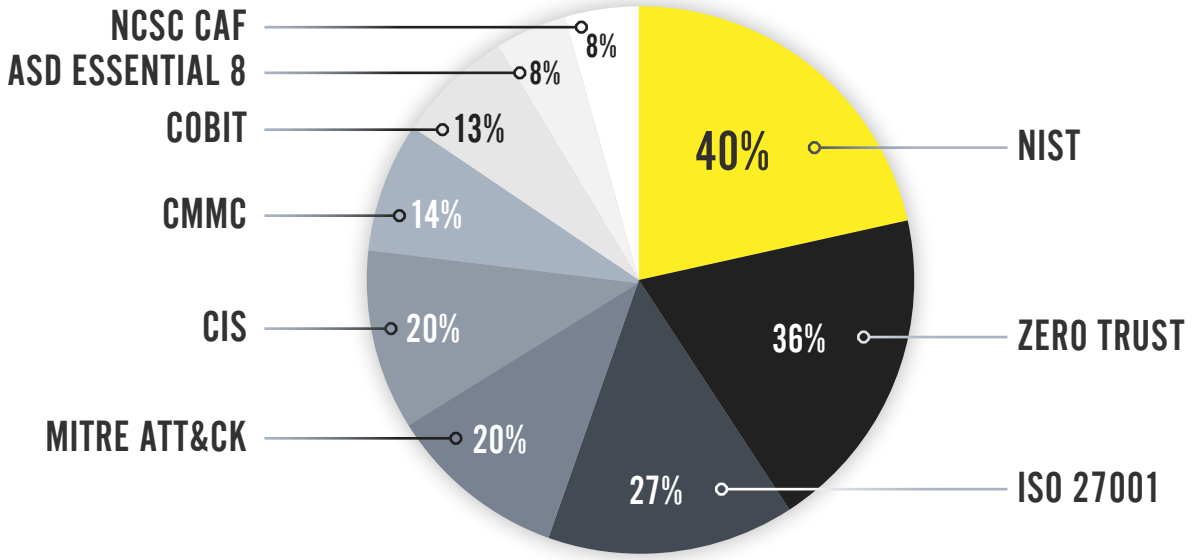


Figure 16

SECURITY SOLUTIONS IMPLEMENTED

Our survey respondents have been busy beefing up their defenses, a fact that is corroborated by the decreases in supply chain attacks and ransomware expenses seen earlier in this report. It's no surprise that antivirus software is ubiquitous. Perennial problems with phishing have resulted in more than three-quarters of respondents ramping up email security. Overall, businesses seem to be committed to investing in advanced cybersecurity solutions. This trend shows a rising security maturity that is likely a response to increasingly sophisticated threats. Figure 25 indicates that trend is set to continue.

Which of the following security solutions has your organization implemented?

87%

Antivirus software

79%

Email/spam protection

70%

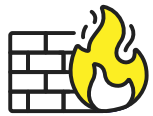
File backup

69%

Security awareness training

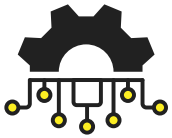
65%

Endpoint detection and response (EDR)



65%

Managed firewall



57%

Automated software patching

48%

Business continuity and disaster recovery (BCDR)

47%

Identity and access management

44%

Incident response

40%

Penetration testing

35%

Security operations center

Figure 17

INCIDENT RESPONSE PLANNING SLACKED OFF

There is significant room for improvement in incident response preparation. The good news is nearly three out of five respondents have an incident response (IR) plan in place. The less good news is the follow-through: Only 37% of respondents report that they confirm the efficacy of their plan with periodic drills, down from 46% in 2023. Meanwhile, 30% have security solutions but lack a formal IR plan, an increase from 23% last year.

It should go without saying that companies looking to minimize downtime and damage from a cyber incident must step up their commitment to incident response planning.

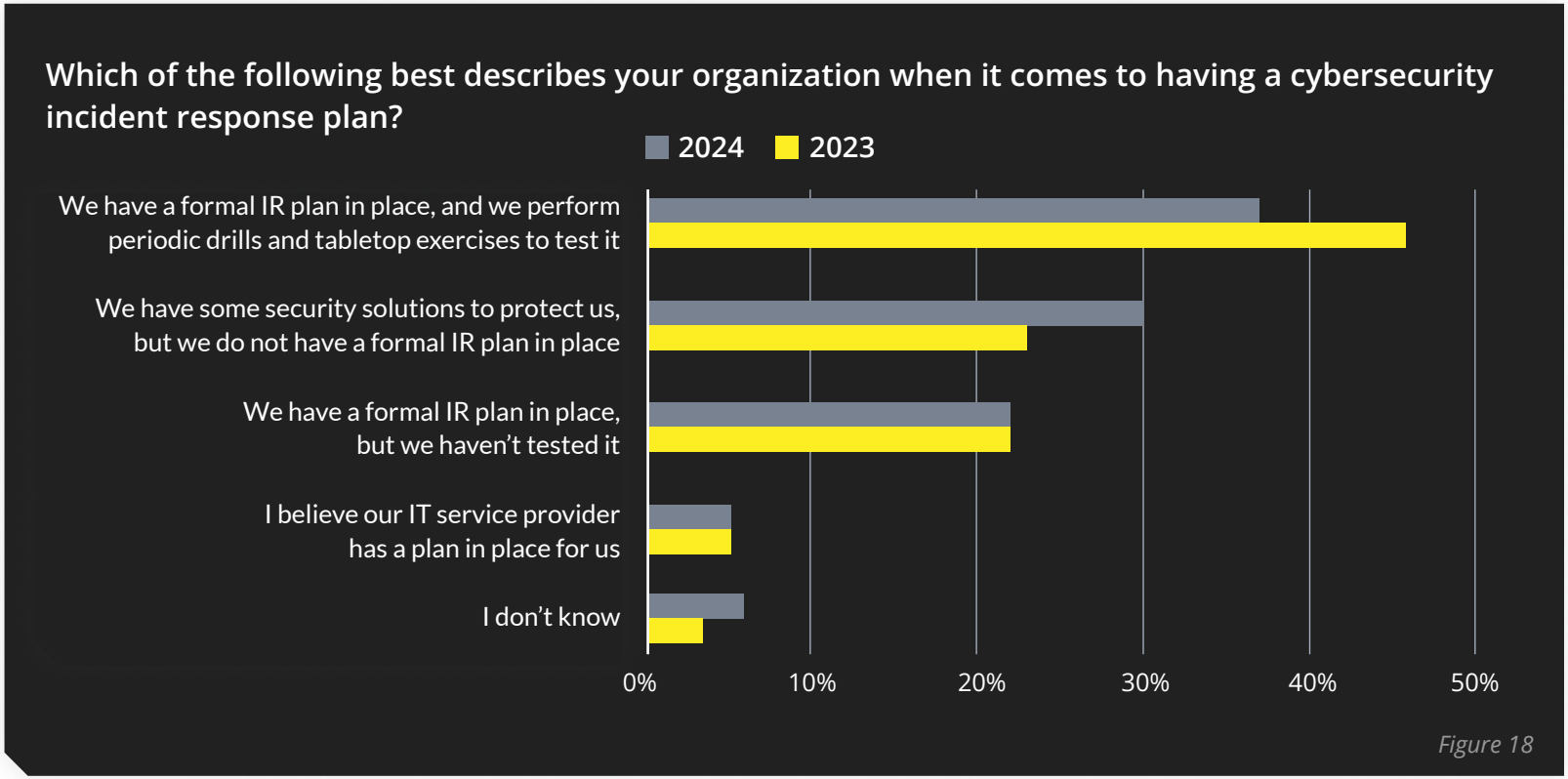


Figure 18

LESS THAN TWO-THIRDS OF RESPONDENTS HAVE AN INCIDENT RESPONSE PLAN.

VULNERABILITY ASSESSMENT FREQUENCY ON THE RISE

The frequency of vulnerability assessments has increased, with 24% of organizations conducting them more than four times per year in 2024, up from 15% in 2023. Conversely, biannual assessments have decreased from 29% to 18%, while annual assessments remain steady at 18%. This shift highlights a growing emphasis on more frequent and regular security evaluations as regulations tighten in a turbulent cybersecurity landscape.

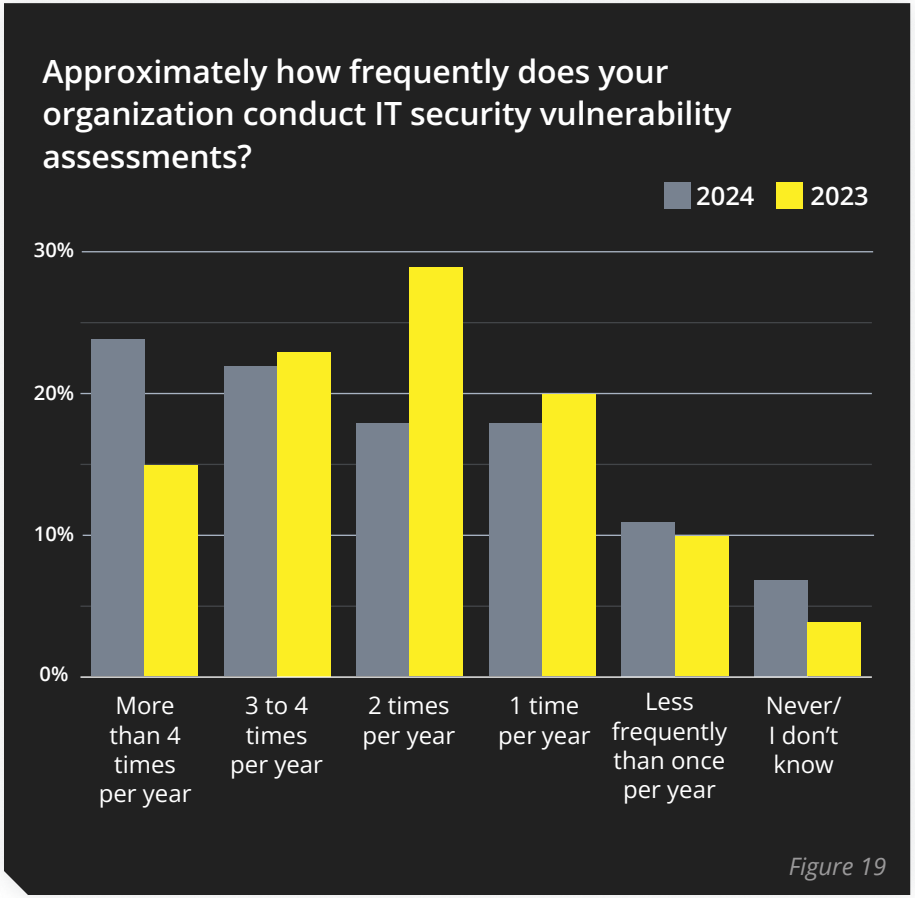


Figure 19

PENETRATION TESTING GOES MAINSTREAM

Most organizations conduct IT penetration testing, or pentesting, regularly. More than two-thirds of respondents test at least twice per year, and more than one-third test at least three times each year. Nearly all organizations engage in some form of penetration testing annually, reflecting a trend toward more frequent and thorough security evaluations — a smart move for maintaining a robust security posture in a volatile threat atmosphere.

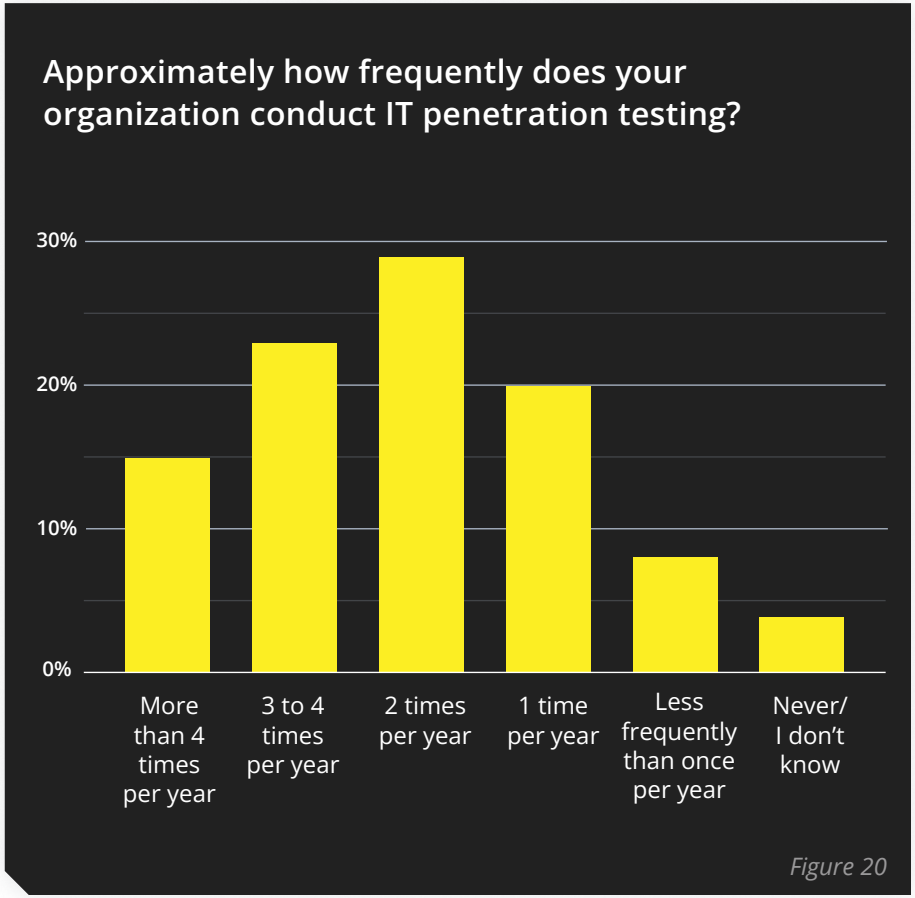


Figure 20

PENTEST ADOPTION CHALLENGES

Cost, specifically budget constraints, is the primary roadblock to pentest adoption (58%). Resource limitations (18%) and IT staffing issues (12%) also play a role, albeit less significantly. Addressing budget and resource issues, along with leveraging automation to reduce costs, has the potential to improve penetration testing adoption.

What challenges prevent you from adopting penetration testing?

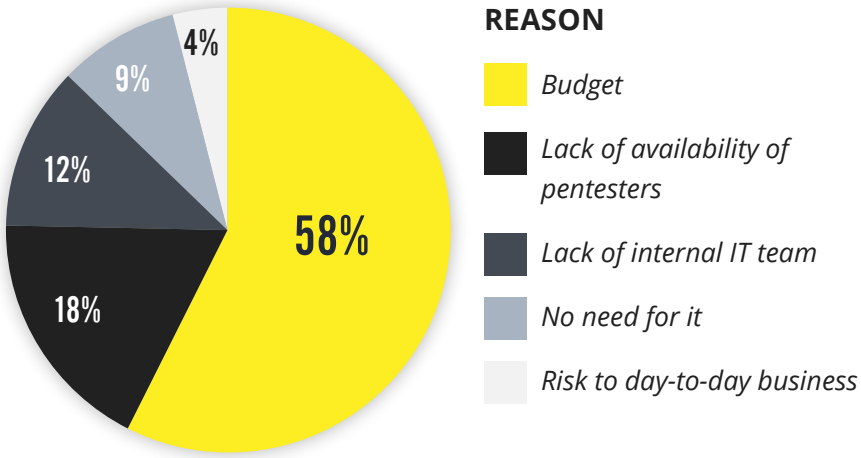


Figure 21

PENTEST ADOPTION DRIVERS NOT ALL ABOUT SECURITY

Unfortunately, too many businesses overlook the tremendous security benefits of pentesting, opting instead to see it as a way to check a box for compliance with insurance or legal requirements. Cybersecurity control and validation (34%) are the main drivers for penetration testing, followed by regulatory compliance (19%) and cyber insurance requirements (15%). Businesses have not yet fully grasped the benefits of pentesting to improve their cyber resilience. evaluations — a smart move for maintaining a robust security posture in a volatile threat atmosphere.

What drives your current pentesting practices?

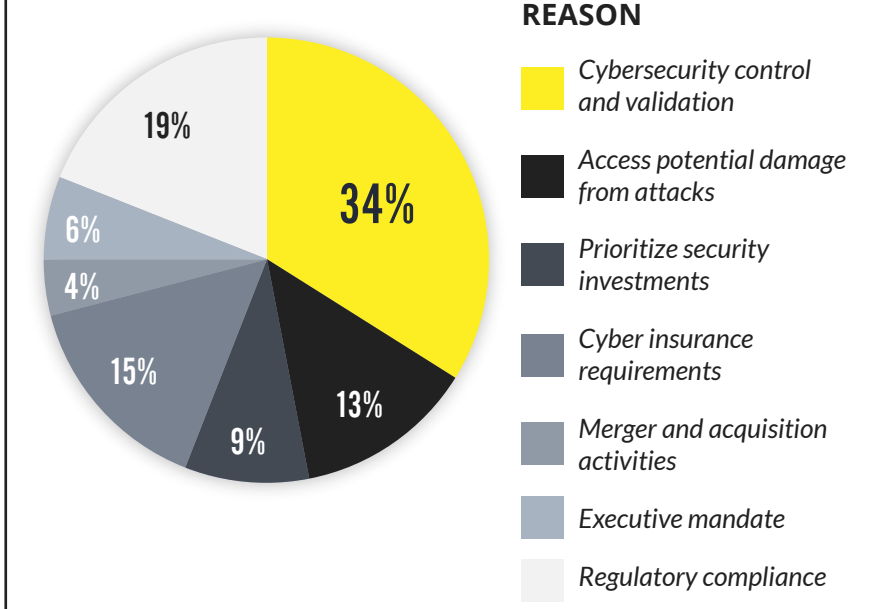


Figure 22

LOOKING AHEAD

As we approach 2025, IT professionals remain deeply concerned about human-related cybersecurity threats. Despite advancements in technology and security measures, the difficult-to-quantify human element that IT professionals face in securing businesses continues to pose significant challenges.

DEFENSE TACTICS MITIGATE FEAR OF PHISHING AND RANSOMWARE ATTACKS

We suspect IT professionals are feeling good about the defenses they've put in place. Phishing and ransomware are viewed as moderate risks by respondents, with 43% considering phishing "somewhat likely" to take place in the next 12 months, and 36% viewing ransomware the same way. This suggests not only awareness of these threats but also confidence in current security measures, leading to a lower perceived likelihood of successful attacks. Overall, while confidence in security measures is high, vigilance remains crucial.

What do you believe is the likelihood that your organization will experience a successful phishing attack in the next 12 months?

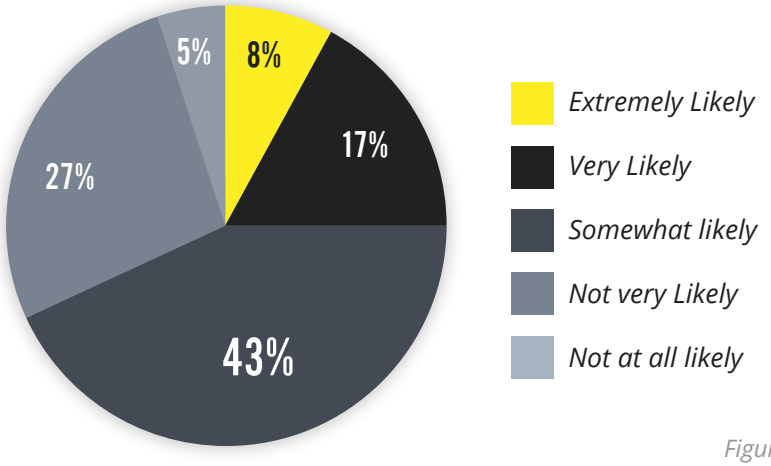


Figure 23

What do you believe is the likelihood your organization will experience a successful ransomware attack in the next 12 months?

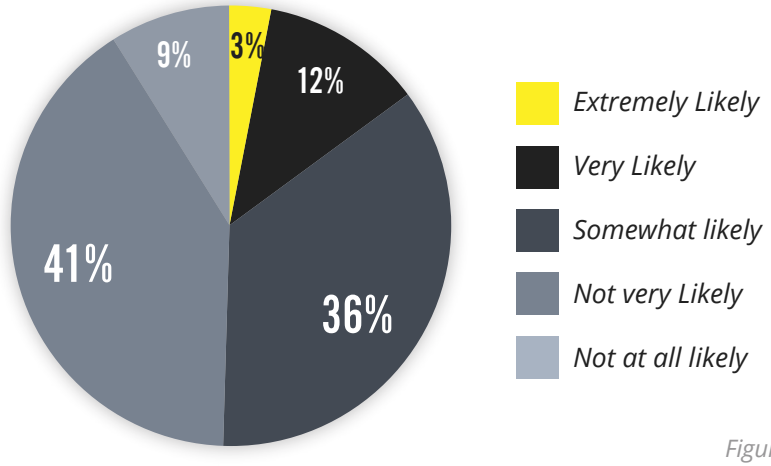


Figure 24

68% OF RESPONDENTS BELIEVE THEY MAY ENCOUNTER A PHISHING ATTACK IN THE NEXT 12 MONTHS.

ANTICIPATED CYBERSECURITY INVESTMENTS

As security maturity reaches a plateau for many businesses, organizations are increasingly focusing on proactive cybersecurity measures, with notable rises in planned investments for advanced solutions, like automated penetration testing. The most significant change is an anticipated increase in investment in a vulnerability assessment tool.

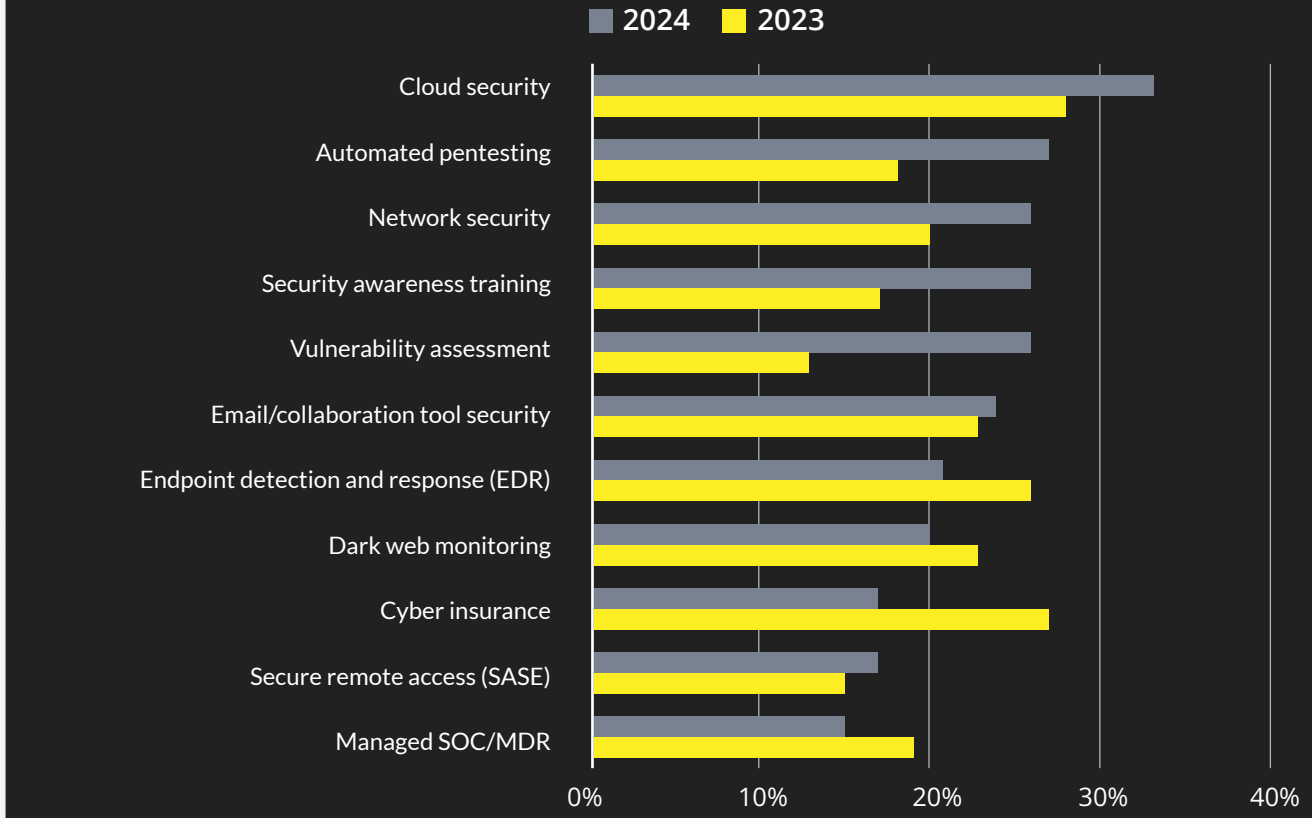


Figure 25

CYBER INSURANCE INVESTMENT PLANS

As the likelihood of cyberattacks has risen, so has the adoption of cyber insurance, with coverage now at 61% compared to 27% in 2023. Overall, more organizations already have cyber insurance, but fewer are expected to invest further in the coming year.

41% OF ORGANIZATIONS ARE PLANNING TO INVEST IN CYBER INSURANCE IN THE NEXT 12 MONTHS.

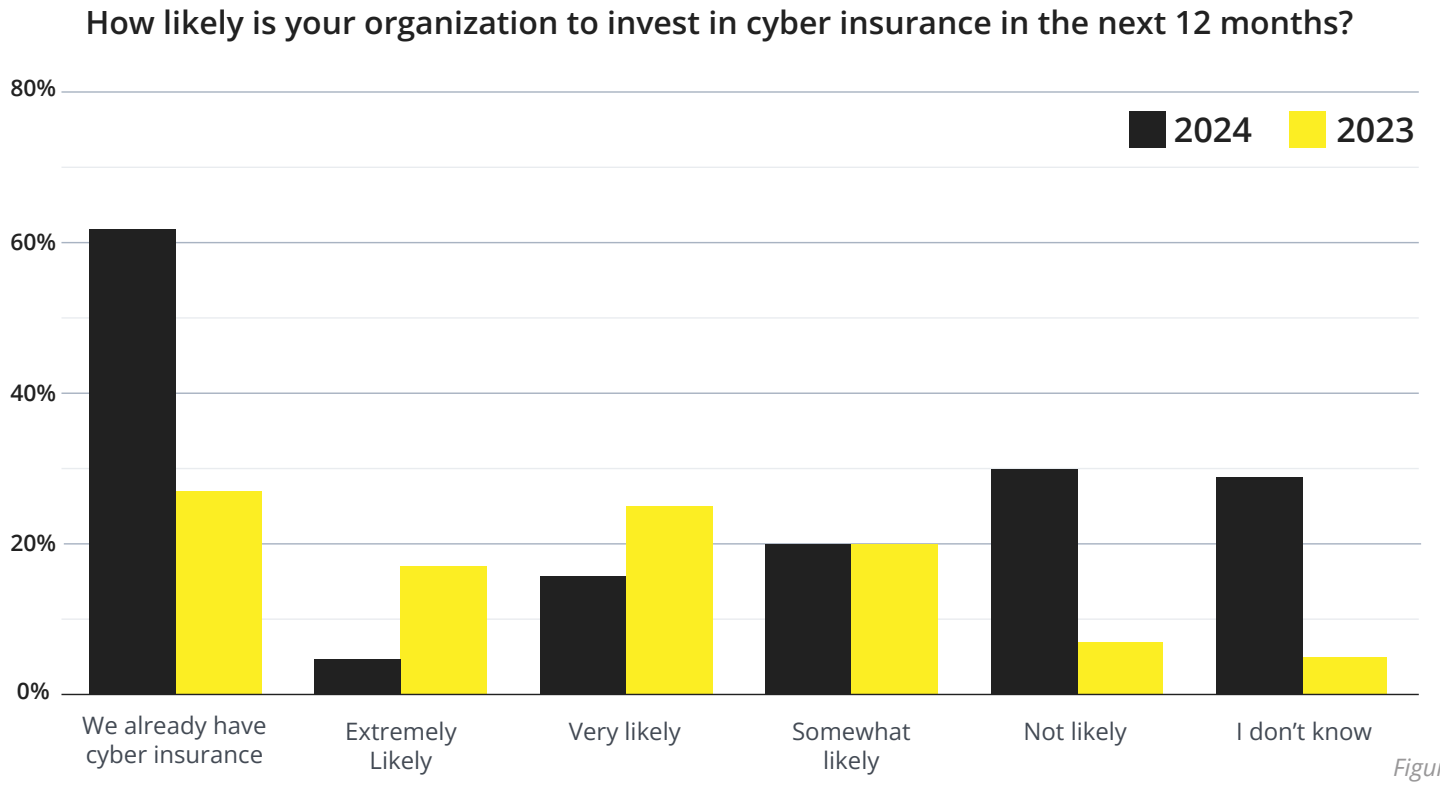


Figure 26

THREAT VECTORS OF PARAMOUNT CONCERN

As stated previously, there is a significant increase in concern over human error, which rose to 36% this year. This highlighting a growing awareness of social engineering and distraction as major threat vectors. Concerns about endpoint threats, including servers and laptops, have plummeted, with server concerns dropping from 12% to 4% and laptops from 11% to 6% Overall, the data suggests a shift in focus toward human error and cloud security, with a decrease in concern about traditional vectors like email and endpoint security.

Which of the following threat vectors are you most concerned about being the gateway to a successful attack in the next 12 months?

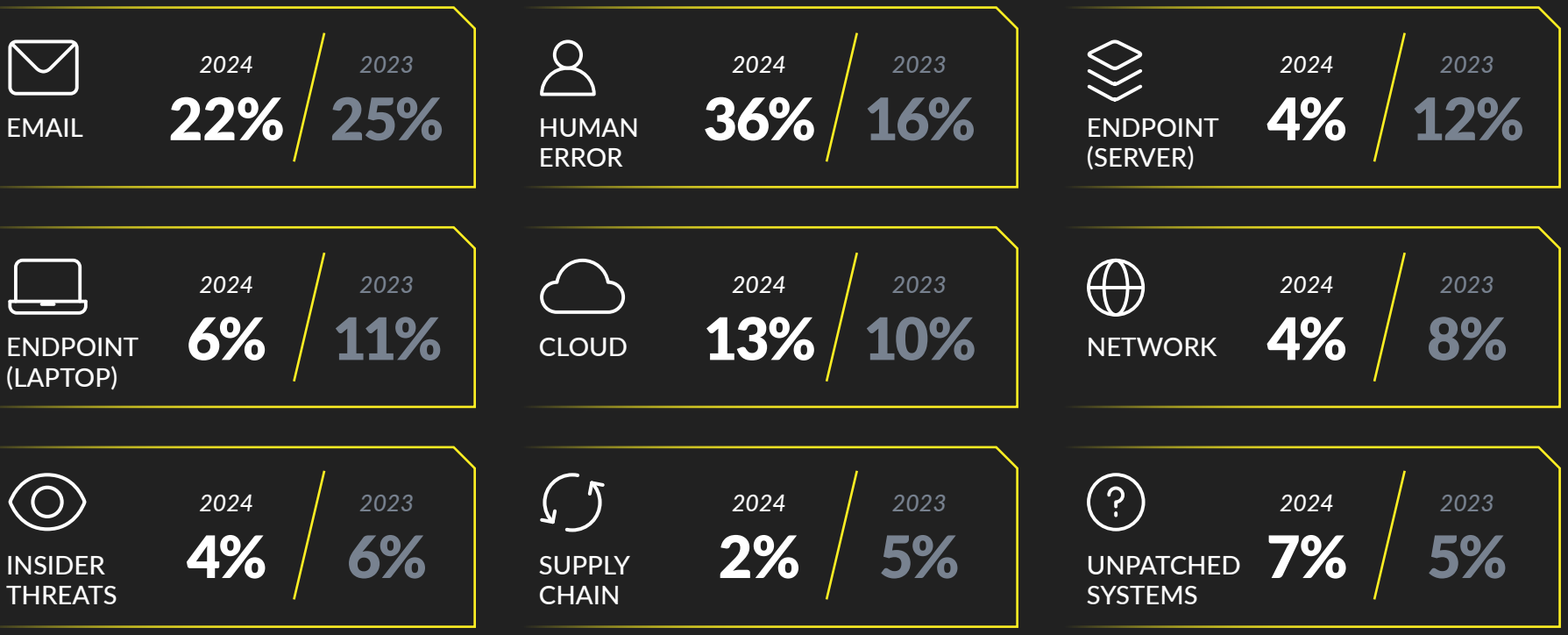


Figure 27

TOP SECURITY MANAGEMENT CHALLENGES

Respondents cited human error (19%) and budget constraints (16%), with significant focus also on IT and security skills (14%) and building a security culture (13%), as top security management challenges for the next 12 months.

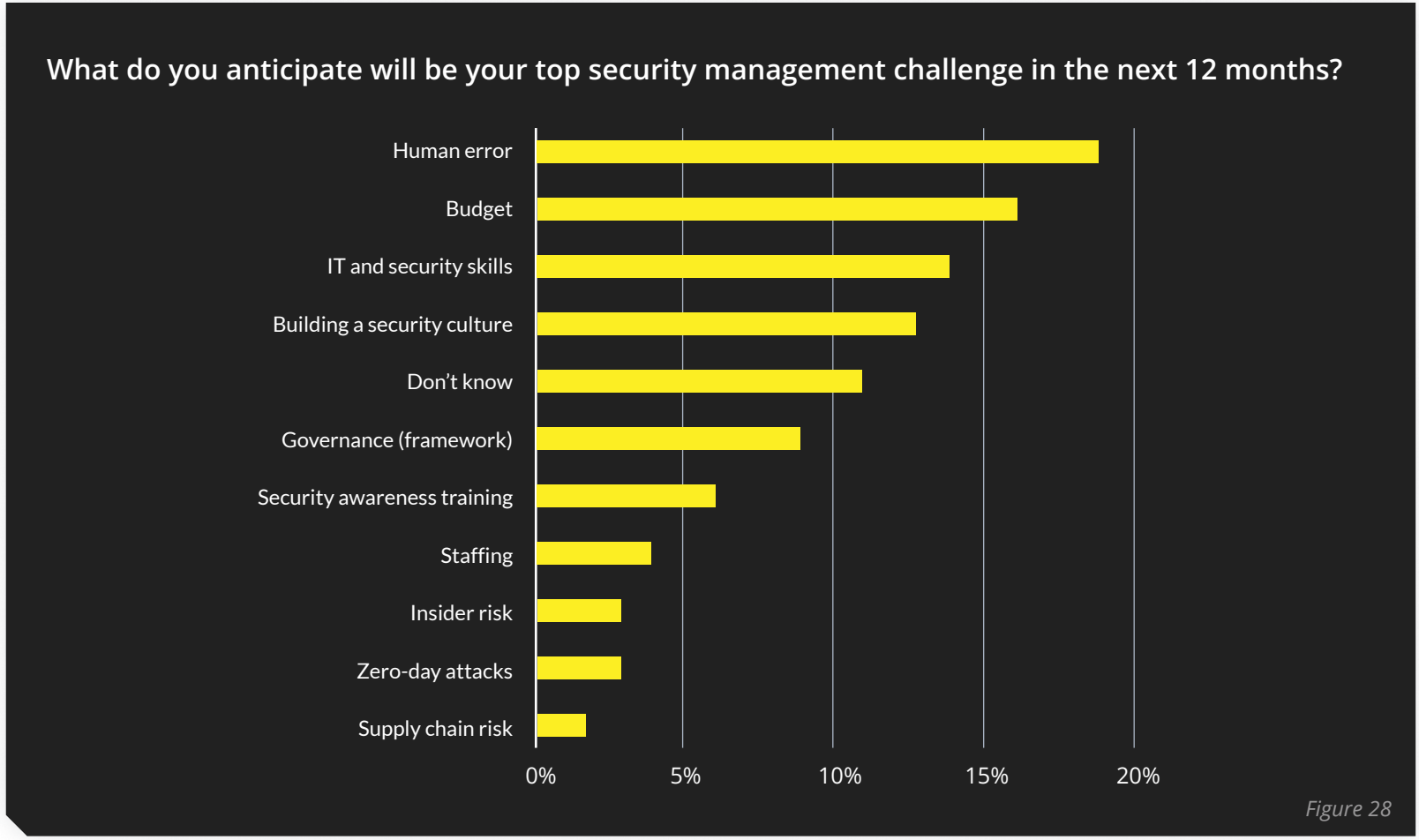


Figure 28

KEY TAKEAWAYS

Here are some key takeaways from this year's data as we look ahead to the evolution of cybersecurity in 2025.

- **Nearly one-third of surveyed IT professionals are unsure about the potential impact of AI on their company's security. This division in viewpoints underscores the need for greater education and clarity regarding AI's benefits and limitations in cybersecurity.**
- **This year saw a significant rise in respondents identifying user behavior as their biggest cybersecurity challenge, with over half citing it as the main issue now and in the future. This shift suggests IT professionals are more confident in their strategies, placing the blame for security issues on users.**
- **Companies will continue to make steady progress toward higher levels of security maturity in an effort to both fend off today's sophisticated cyberattacks and maintain a high level of readiness for growing challenges from sources like AI-enabled cyberattacks.**
- **While defenders feel confident in their abilities to defend against phishing and ransomware as well as minimize the impact of such attacks, they're under no illusions that ransomware and phishing will be less of a problem in the future.**

RISING TO THE CHALLENGE: SECURING TOMORROW'S DIGITAL WORLD

As IT professionals navigate this rapidly changing cybersecurity landscape, it's clear that the challenges are as dynamic as the technologies that are emerging. The integration of AI into both offensive and defensive strategies has fundamentally altered the playing field, demanding a proactive and adaptable approach from IT professionals.

However, with these challenges come opportunities. The drive to build a robust IT infrastructure is not just about staying ahead of today's threats. It is also about creating resilient, agile systems that can adapt to whatever comes next. As we stand on the frontier of cybersecurity, it is clear that a commitment to innovation, investments in next-gen solutions and increased preparedness for trouble will be the keys to securing a bright digital future.

RESPONDENT DEMOGRAPHICS

In which country is your corporate headquarters located?

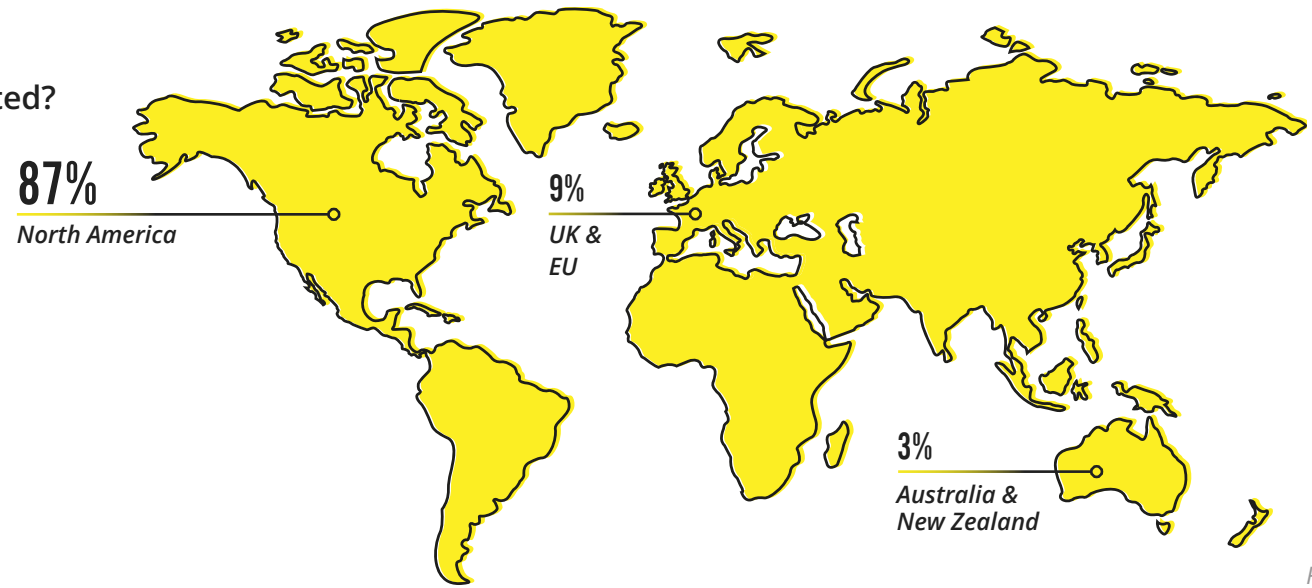


Figure 29

Which of the following ranges best describes your company's annual revenue?

ANNUAL REVENUE

Over $1 billion	9%
$500 million to $1 billion	7%
$100 million to $500 million	17%
$50 million to $100 million	13%
$10 million to $50 million	20%
$1 million to $10 million	21%
Less than $1 million	13%

Figure 30

What is the total number of employees in your company?

COMPANY SIZE

More than 3,000	17%
1,001 to 3,000	13%
501 to 1,000	11%
101 to 500	29%
51 to 100	13%
Less than 50	17%

Figure 31

How are your organization's IT needs managed?

We have a dedicated internal IT team	71%
We have a co-managed relationship with an IT service provider	26%
We outsource everything to an IT service provider	2%
I don't know	1%

Figure 32

LEARN MORE ABOUT HOW OUR SECURITY SOLUTIONS CAN PROTECT YOUR BUSINESS.

Dark Web Monitoring, Phishing Defense and Security Awareness Training

LEARN MORE

ID AGENT
A Kaseya COMPANY

ABOUT ID AGENT

ID Agent, a Kaseya company, provides the leading Dark Web monitoring, security awareness training and phishing simulation solutions worldwide. Its flagship product, Dark Web ID™, delivers validated intelligence to identify, analyze and monitor for compromised or stolen employee and customer data. The company's BullPhish ID™ product provides cybersecurity awareness training and phishing simulation geared to the non-technical end user, to enhance a company's overall cybersecurity and further safeguard corporate systems. To learn more, visit www.idagent.com.