KASEYA 2023 CYBERSECURITY SURVEY:

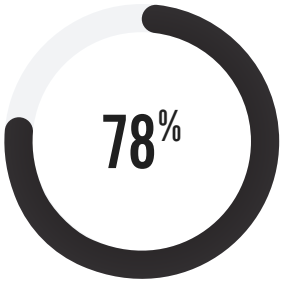
FACING A LANDSCAPE OF EVOLVING CHALLENGES

IDAGENT
A Kaseya COMPANY

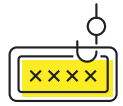
In today's rapidly evolving cybersecurity landscape, keeping businesses safe and secure can be a daunting task. The complications that IT teams face from a challenging economy and the IT talent shortage don't make things easier either.

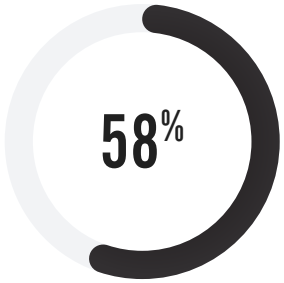
Our 2023 Kaseya Cybersecurity Survey polled 3,066 IT professionals from around the world to find out what their biggest cybersecurity challenges are right now and what they expect them to be in the next year. Although the results indicate that organizations are taking cybersecurity seriously, they still have weaknesses in their security buildout that could lead to trouble. Cybersecurity moves fast, and every company can benefit by making sure they are resilient enough to handle today's challenges and the challenges of tomorrow.

5 STATISTICS THAT SPEAK TO TODAY'S CYBERSECURITY CHALLENGES



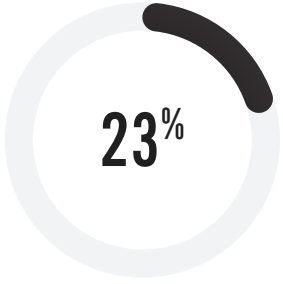
78% of respondents said they believe they'll be hit by phishing in the next year



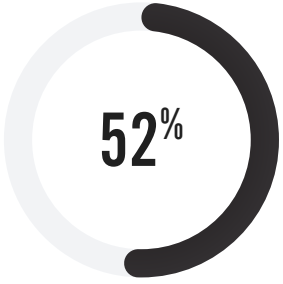


58% of respondents think it's likely they'll be hit by ransomware in the next 12 months

92% of respondents support a remote workforce



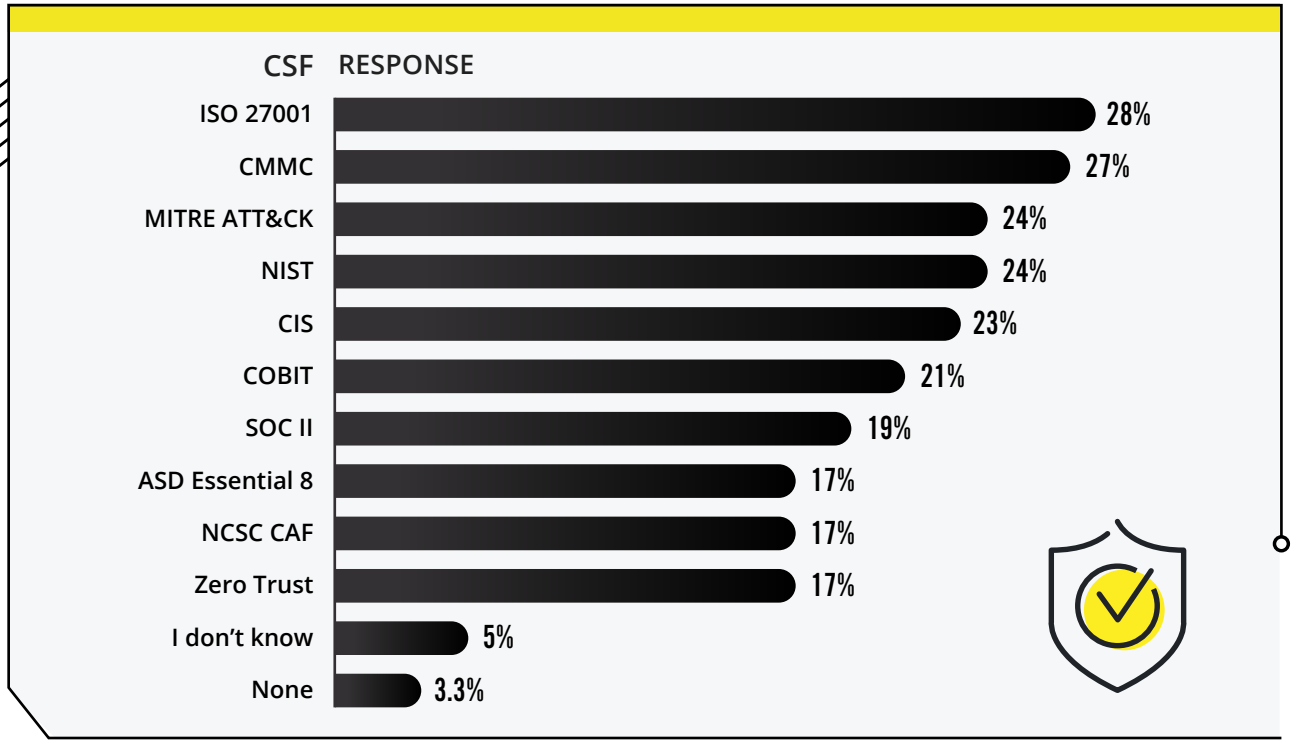
23% of respondents do not have an incident response plan



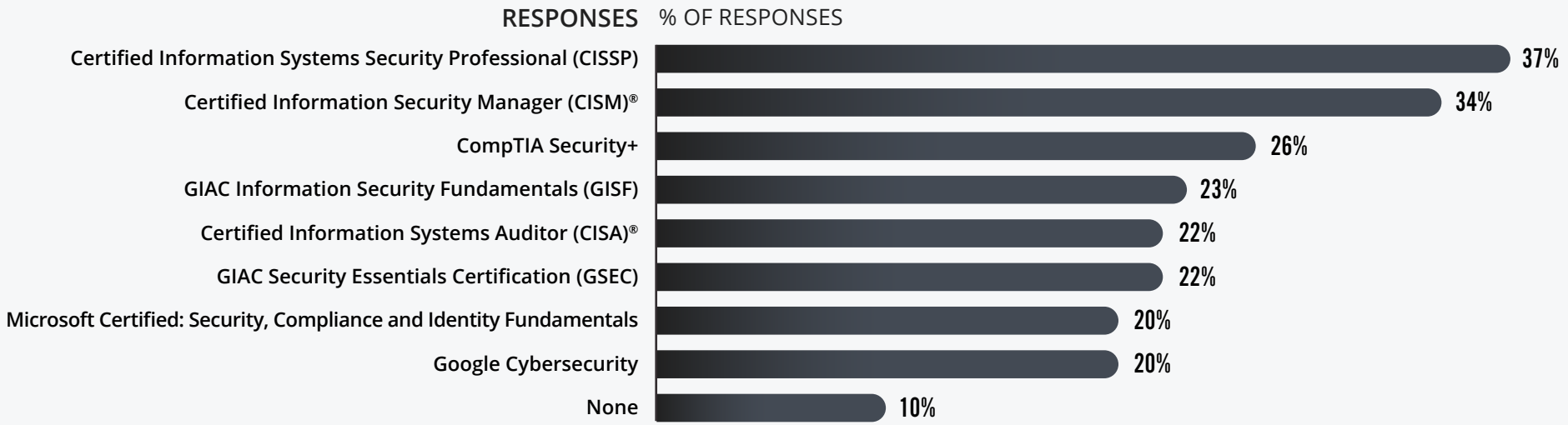
52% of respondents cite a lack of cybersecurity training as a top problem

HOW BUSINESSES ARE UNDERTAKING CYBERSECURITY MANAGEMENT

The cybersecurity framework a company chooses is an important indicator of its security focus and security concerns. In this year's survey, the top framework was ISO 27001, with more than one-quarter of respondents (28%) indicating that their organization uses it. CMMC wasn't far behind, with 27% of respondents indicating it as their company's top choice. MITRE ATT&CK and NIST tied for third place (24%).



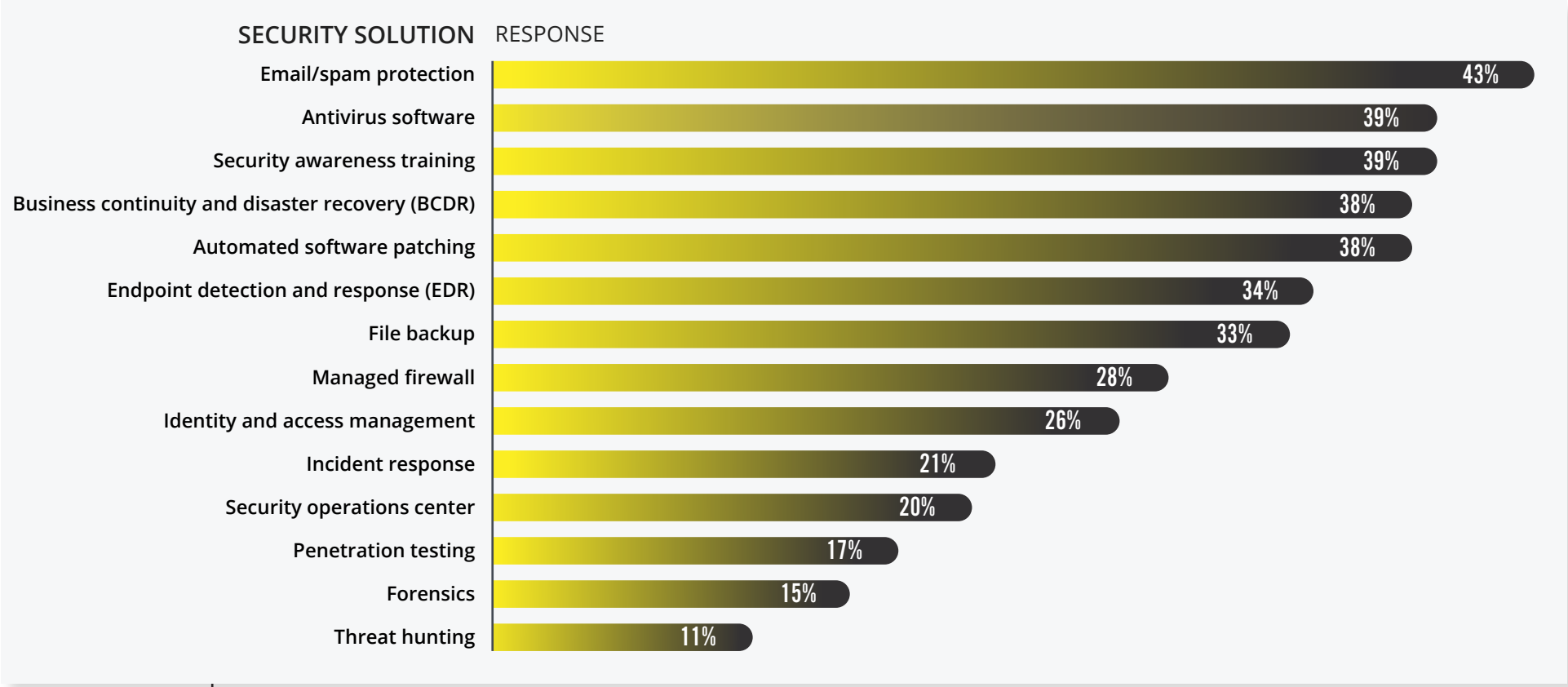
WHICH OF THE FOLLOWING CYBERSECURITY CERTIFICATIONS DO YOU HAVE OR ARE PURSUING IN THE NEXT 12 MONTHS?



Cybersecurity is a complex and ever-evolving field. That means that IT professionals need a solid foundation in education to keep up with today's demands and a commitment to continuing education to be ready for what's next. Among our survey respondents, the top certifications held or being pursued in the next year are Certified Information Systems Security Professional (37%) and Certified Information Security Manager® (34%).

Fewer than half of businesses surveyed have enhanced email security.

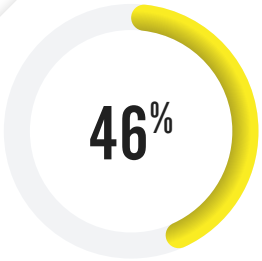
WHICH OF THE FOLLOWING SECURITY SOLUTIONS HAS YOUR ORGANIZATION IMPLEMENTED?



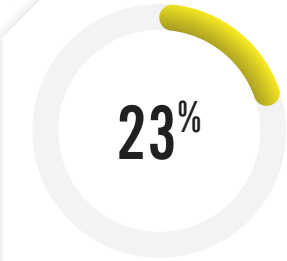
In response to the current fast-paced security threat landscape, most companies have deployed a wide array of security solutions to mitigate those threats. However, some significant gaps remain. Email continues to be a top threat vector, but only a little under half of our respondents have deployed an email security solution to secure it (43%), instead choosing to rely on native security in cloud email platforms like Microsoft 365. Antivirus software and security awareness training tied for the second most implemented solution (39%).

That's especially surprising in terms of cybersecurity training, a low upfront cost security measure that yields high returns. Only about one-third of respondents (38%) said that their organization has implemented automated software patching or a business continuity and disaster recovery (BCDR) solution. The survey respondents indicated that penetration testing (17%), forensics (15%) and threat hunting (11%) were the least adopted technologies.

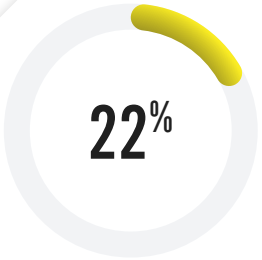
WHICH OF THE FOLLOWING BEST DESCRIBES YOUR ORGANIZATION WHEN IT COMES TO HAVING A CYBERSECURITY INCIDENT RESPONSE PLAN?



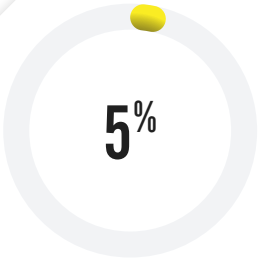
46% We have a formal IR plan in place, and we perform periodic drills and tabletop exercises to test it



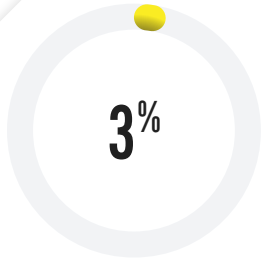
23% We have some security solutions to protect us but we do not have a formal IR plan in place



22% We have a formal IR plan in place but we haven't tested it



5% I believe our IT service provider has a plan in place for us

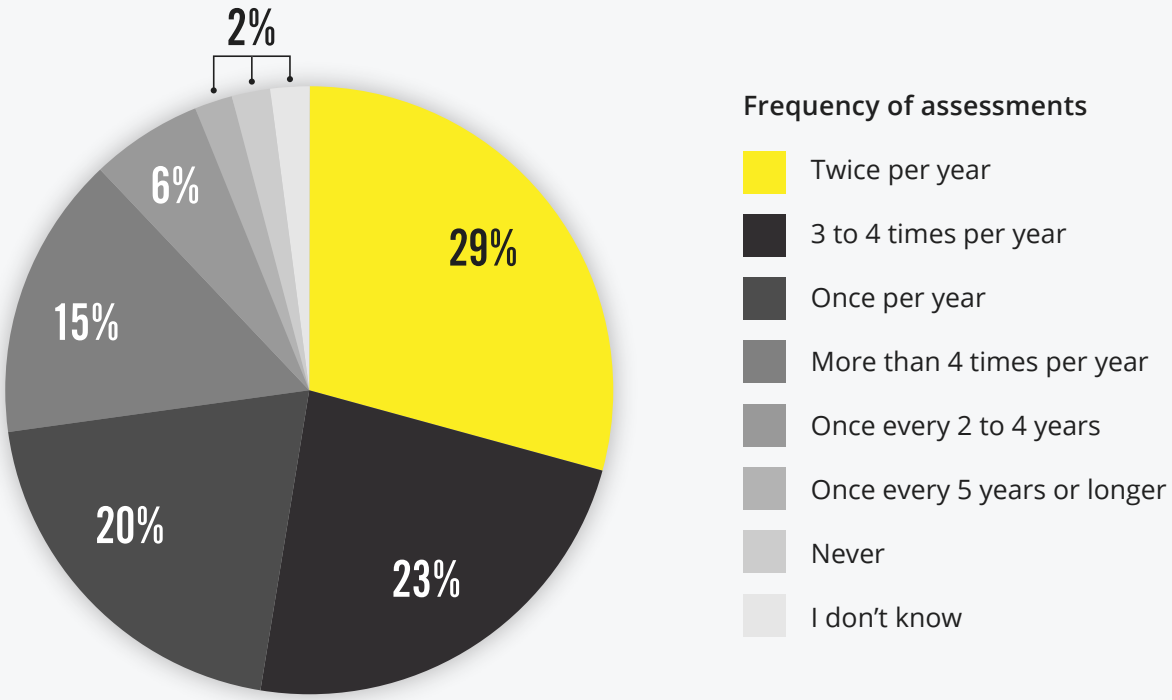


3% I don't know

Experiencing a cybersecurity incident is no longer a matter of "if" but rather a matter of "when." Just under half (46%) of our respondents follow best practices when it comes to preparing for an incident response by having a formal, tested incident response plan in place. More than one-fifth of respondents have a formal incident response plan but have not tested it.

A shocking 23% don't have a plan in place at all.

APPROXIMATELY HOW FREQUENTLY DOES YOUR ORGANIZATION CONDUCT IT SECURITY VULNERABILITY ASSESSMENTS?

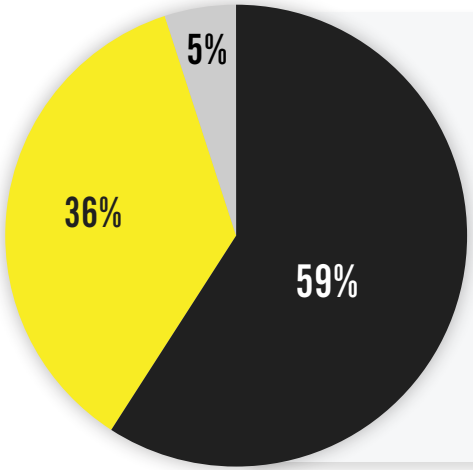


IT security vulnerability assessments are a valuable tool for organizations to employ to find weaknesses in their security buildout, and most of our respondents are putting that tool to work for their organization in some capacity. Over half of our survey respondents (52%) said that their company conducts vulnerability assessments two to four times per year. Quarterly assessments are a requirement under some compliance standards and are considered a best practice. Another fifth (20%) said that their employer conducts assessments only once per year — well below the recommended standard. Even worse, 8% of respondents conduct assessments only every two to five years, allowing dangerous vulnerabilities that could translate into damaging cyberattacks to pile up.

WHICH OF THE FOLLOWING CYBERSECURITY INVESTMENTS DO YOU ANTICIPATE MAKING IN THE NEXT 12 MONTHS?

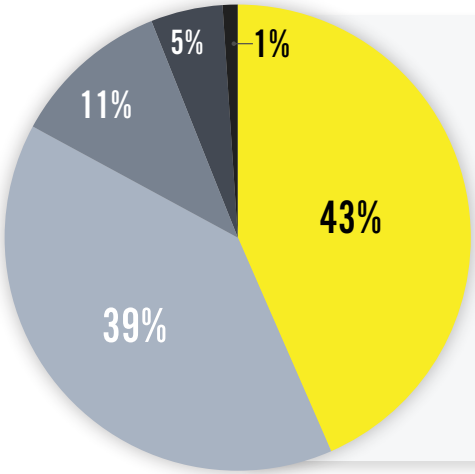
CLOUD SECURITY	28%
CYBER INSURANCE	27%
ENDPOINT DETECTION AND RESPONSE (EDR)	26%
DARK WEB MONITORING	23%
EMAIL/COLLABORATION TOOL SECURITY	23%
NETWORK SECURITY	20%
MANAGED SOC/MDR	19%
AUTOMATED PEN TESTING	18%
SECURITY AWARENESS TRAINING	17%
SECURE REMOTE ACCESS (SASE)	15%
VULNERABILITY ASSESSMENT	13%
WE DO NOT ANTICIPATE INVESTING IN CYBERSECURITY	3%

Even in a time of strained budgets, companies recognize how important IT security is for their continued success — and they're making investments in it. Cloud security (28%), cyber insurance (27%) and endpoint detection and response (EDR) (26%) are the top three areas in which respondents said they plan to invest in the next year. Surprisingly, only 17% of respondents are planning to invest in security awareness training, a low-cost way to reduce security incidents by up to 70%, and 3% of respondents said their companies will not be making any cybersecurity investments at all.



HOW ARE YOUR ORGANIZATION'S IT NEEDS MANAGED?

- *We have a dedicated internal IT team*
- *We have a co-managed relationship with an IT service provider*
- *We outsource everything to an IT service provider*



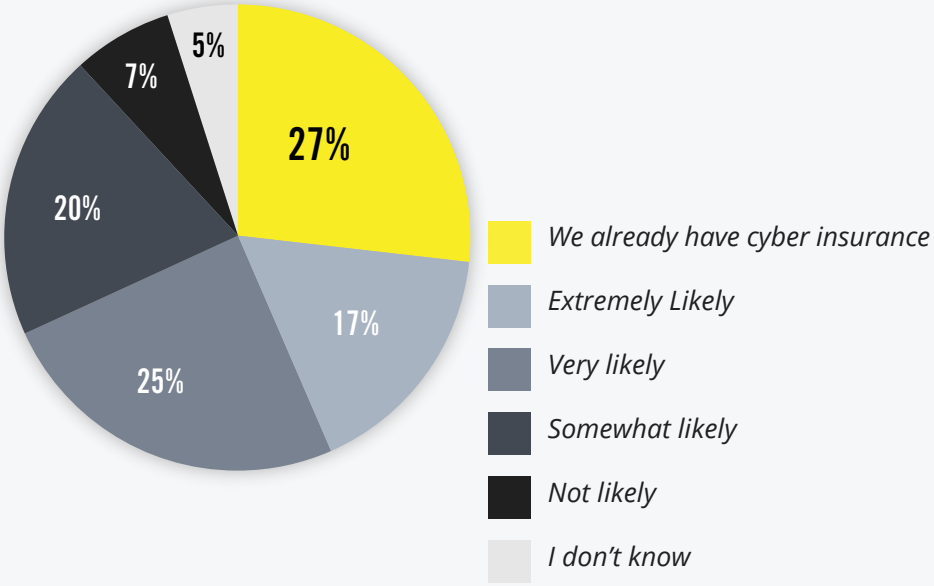
HOW ARE YOUR ORGANIZATION'S IT SECURITY NEEDS MANAGED?

- *We have a dedicated internal IT team*
- *We have a co-managed relationship with an IT service provider*
- *We outsource everything to an IT service provider*
- *We outsource everything to a managed security service provider (MSSP)*
- *I don't know*

Our results indicate that by and large, companies prefer to handle their IT management internally, with more than half of respondents saying that their organization has chosen that route. About 41% partially or fully entrust their IT management to a managed service provider (MSP). However, companies choose to handle their IT security a little bit differently. More than half of our respondents said that they manage their security with the help of an IT service provider (55%).

62% OF THE BUSINESSES SURVEYED PLAN TO BUY CYBER INSURANCE IN THE NEXT 12 MONTHS.

HOW LIKELY IS YOUR ORGANIZATION TO INVEST IN CYBER INSURANCE IN THE NEXT 12 MONTHS?



Businesses have undergone unprecedented transformation in the past few years. That's especially evident when considering remote work. From workers connecting from home offices to road warriors connecting on the move, companies need to be ready to support a dynamic workforce. Almost all of our respondents (95%) said that their IT team supports a remote workforce in some capacity. More than one-third (38%) of respondents said that 11% to 25% of their company's workforce is remote. Another quarter (25%) indicated that 26% to 50% of their employer's staff work remotely. This illustrates how essential it is for companies to consider on-site and remote threats when devising their security plan.

APPROXIMATELY WHAT PERCENTAGE OF YOUR WORKFORCE WORKS REMOTELY?

100% — all employees work remotely	***1%***
76% to 99%	***4%***
51% to 99%	***13%***
26% to 50%	***25%***
11% to 25%	***38%***
1% to 10%	***19%***
0% — all employees work at a company site	***5%***

Cyber insurance has become a must-have for businesses. The majority of our respondents (79%) said that their organization has cyber insurance. Our respondents also indicated that if their company doesn't have cyber insurance, they're planning to invest in it soon. Nearly two-thirds of respondents (62%) said that their organization is at least somewhat likely to purchase cyber insurance in the next 12 months.

95% OF RESPONDENTS SUPPORT REMOTE WORKERS.

THE CYBERSECURITY CHALLENGES THAT BUSINESSES FACE

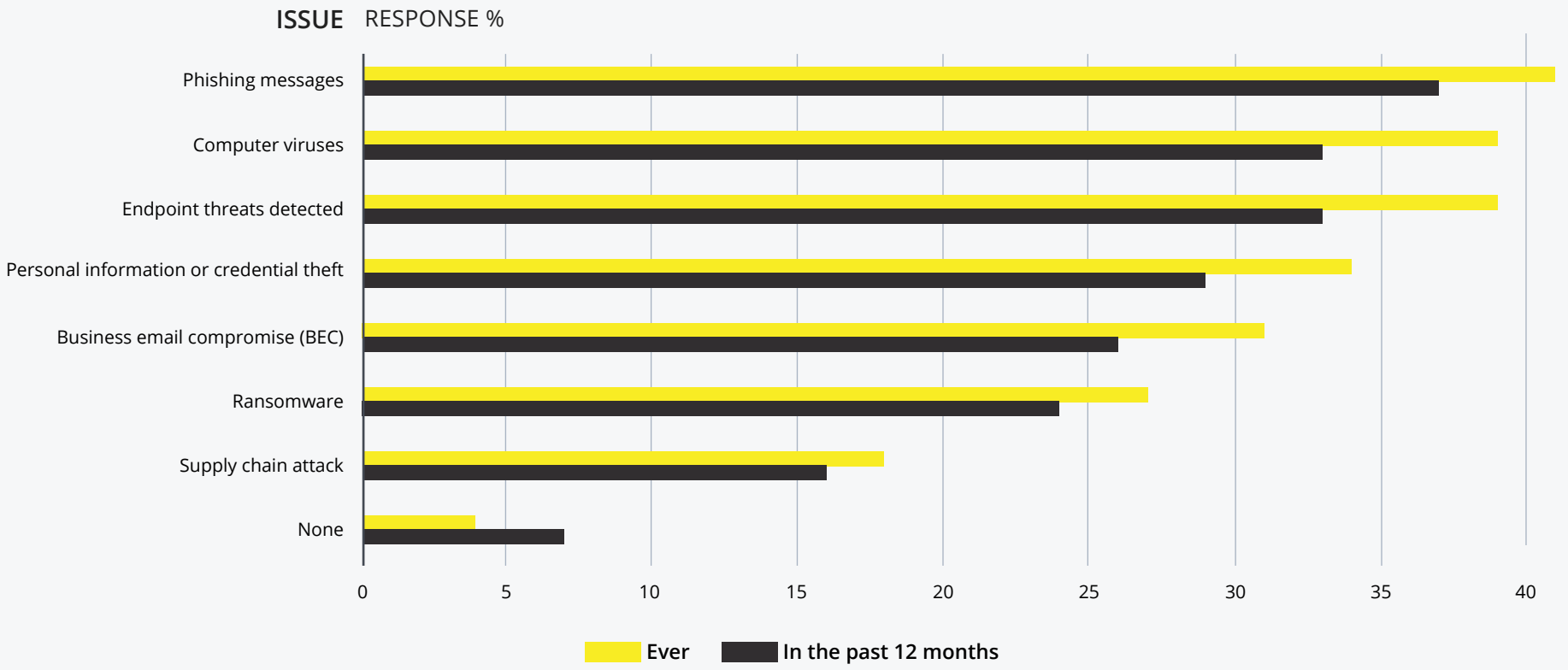
Cybersecurity is a fast-paced and complex world that brings a variety of challenges to businesses. When considering the IT security challenges that respondents anticipate encountering in the next year, no single challenge outstripped the rest of the pack. What is interesting is that four of the top five security management challenges our respondents selected are people-based challenges: human error (20%), IT and security skills (18%), insider risk (15%) and security awareness training (11%). An increase in security awareness training and strong security policies can mitigate some of these risks.

WHAT DO YOU ANTICIPATE WILL BE YOUR TOP SECURITY MANAGEMENT CHALLENGE IN THE NEXT 12 MONTHS?

Challenge	Response
Human error	***20%***
IT and security skills	***18%***
Insider risk	***15%***
Budget	***13%***
Security awareness training	***11%***
Building a security culture	***9%***
Staffing	***6%***
Supply chain risk	***6%***
Other	***1%***

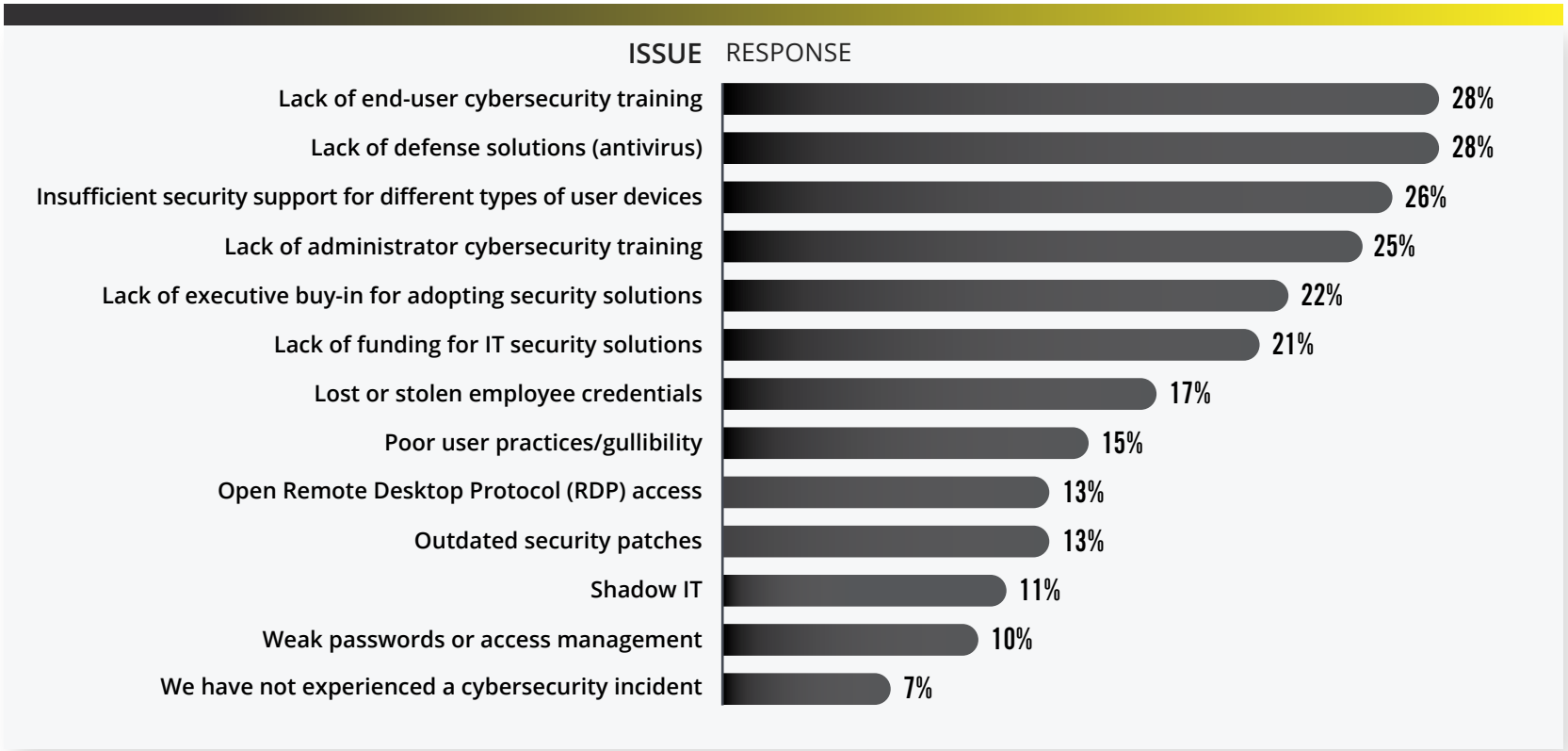
PEOPLE ARE THE TOP CYBERSECURITY CHALLENGE THAT IT TEAMS FACE.

WHICH OF THE FOLLOWING CYBERSECURITY ISSUES HAVE IMPACTED YOUR BUSINESSS?



There is no clear leader in the list of cybersecurity issues that businesses have experienced. In fact, the top three challenges are nearly tied. Phishing tops the list of security issues that respondents have encountered (41%), followed closely by viruses (39%) and endpoint threats (39%). More than half of our respondents have also had to contend with a dangerous cyberattack like ransomware or business email compromise at some point (58%). In terms of challenges experienced in the past 12 months, the picture shifts slightly, with the top three issues the same but experienced slightly differently by our survey respondents.

WHAT ARE THE TOP THREE ROOT CAUSES OF YOUR CYBERSECURITY ISSUES?



IF YOU'VE EXPERIENCED A CYBERSECURITY INCIDENT, WHAT WAS YOUR TOTAL DOWNTIME?

Total Downtime	*Response*
A week or more	*5%*
4 – 6 days	*9%*
2 – 3 days	*20%*
1 day	*15%*
Less than 1 day	*30%*
None – we didn't have any downtime	*10%*
We have not experienced a cybersecurity incident	*5%*
I don't know	*2%*
Prefer not to answer	*1%*
We did not recover	*2%*

One result of cybersecurity problems is costly downtime. Although over half of our respondents were able to get back to work quickly after a cybersecurity incident, reporting downtime of less than three days (65%), 14% said that their downtime was four days or more — an expensive proposition with long-term ramifications.

56% of respondents lost $50,000 or more in a cybersecurity incident.

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 cybersecurity incident	*Response*
Less than $10,000	*16%*
$10,000 to less than $50,000	*17%*
$50,000 to less than $100,000	*17%*
$100,000 to less than $250,000	*18%*
$250,000 to less than $500,000	*10%*
$500,000 to $1 million	*7%*
$1 million or more	*4%*
I don't know	*4%*
We have not experienced a cybersecurity incident	*9%*

Lost revenue, lost productivity and recovery expenses are three major reasons why it is important for businesses to minimize cybersecurity incidents. Just over one-third of respondents (39%) lost $100,00 or more, and 21% lost a whopping $250,000 or more. In today's challenging economy, no business can afford this kind of monetary loss, making high-quality cybersecurity safeguards mission-critical.

HOW DO BUSINESSES FARE AGAINST CYBERATTACKS LIKE RANSOMWARE AND PHISHING?

Almost one-quarter of our survey respondents said that their organization fell victim to a ransomware attack in the past 12 months. Our survey respondents followed a variety of pathways to recover from ransomware disasters. One-third of respondents (33%) said they were successfully able to perform a disaster recovery and restore everything from backups — a low figure considering the expenses and downtime a business can face in the event of a ransomware attack. More than half of respondents (60%) told us that they were forced to reinstall and reconfigure at least some of their systems — a time-consuming operation.

One in five respondents said that their organizations paid the attackers — a practice that is frowned upon by experts and law enforcement because it can embolden cybercrime gangs and, in some cases, support terrorism. About one-fifth of respondents paid the ransom in an effort to recover their data. However, as 14% of respondents found out, paying the ransom doesn't necessarily mean that you will recover your data.

IF YOU WERE A VICTIM OF A RANSOMWARE ATTACK, WHICH OF THE FOLLOWING ACTIONS DID YOU TAKE TO RECOVER YOUR DATA?

Action	*Response*
Performed disaster recovery (DR) and restored everything from full backups	***33%***
Restored a portion of the systems and reinstalled and reconfigured the rest	***31%***
Reinstalled and reconfigured all of our systems from scratch	***29%***
We paid the ransom to have our data decrypted	***21%***
We decided not to pay the ransom and lost our data completely	***17%***
We paid the ransom but still could not decrypt our data, losing it completely	***14%***
We could not recover and have closed or are closing our business	***7%***
No action was needed	***4%***
We have never been hit with a ransomware attack	***14%***

THINKING ABOUT THE RANSOMWARE ATTACK YOU EXPERIENCED, WHAT WAS THE LOCATION OF THE DATA THAT WAS ENCRYPTED DURING THE ATTACK?

Location	*Response*
On-premise server(s)	***40%***
Private cloud	***38%***
Non-server endpoints (e.g., PCs, laptops or workstations)	***31%***
Public cloud	***24%***
SaaS	***16%***

As we discussed earlier, one in five of our respondents said that their organization paid the attacker when they experienced a successful ransomware attack. For about half of those businesses, that ransom payment was less than $5,000 (51%). Even though that may seem like an acceptable cost to retrieve your data and get back to work, paying the ransom doesn't always work out and may be illegal.

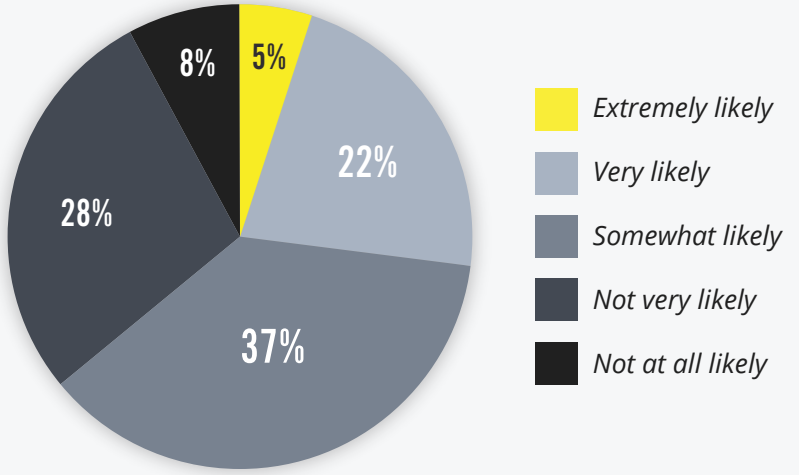
THINKING ABOUT THE RANSOMWARE ATTACK YOU EXPERIENCED, WHAT WAS THE COST OF THE RANSOM?

Cost of Ransom	*Response*
$50,000 or more	***6%***
$25,000 to less than $50,000	***9%***
$10,000 to less than $25,000	***12%***
$5,000 to less than $10,000	***13%***
$1,000 to less than $5,000	***21%***
$500 to less than $1,000	***15%***
Less than $500	***15%***
I don't know	***5%***
I prefer not to answer	***2%***

With the number and frequency of ransomware attacks growing constantly, it's no surprise that most IT professionals expect their employers to fall victim to one. Over three-fifths of our survey respondents (64%) said that their company is likely to experience a successful ransomware attack in the next 12 months. More than half (53%) of our respondents indicated that a successful ransomware attack would have a significant impact on their organization. An unfortunate 17% said they believe their company is unlikely to survive a successful ransomware attack.

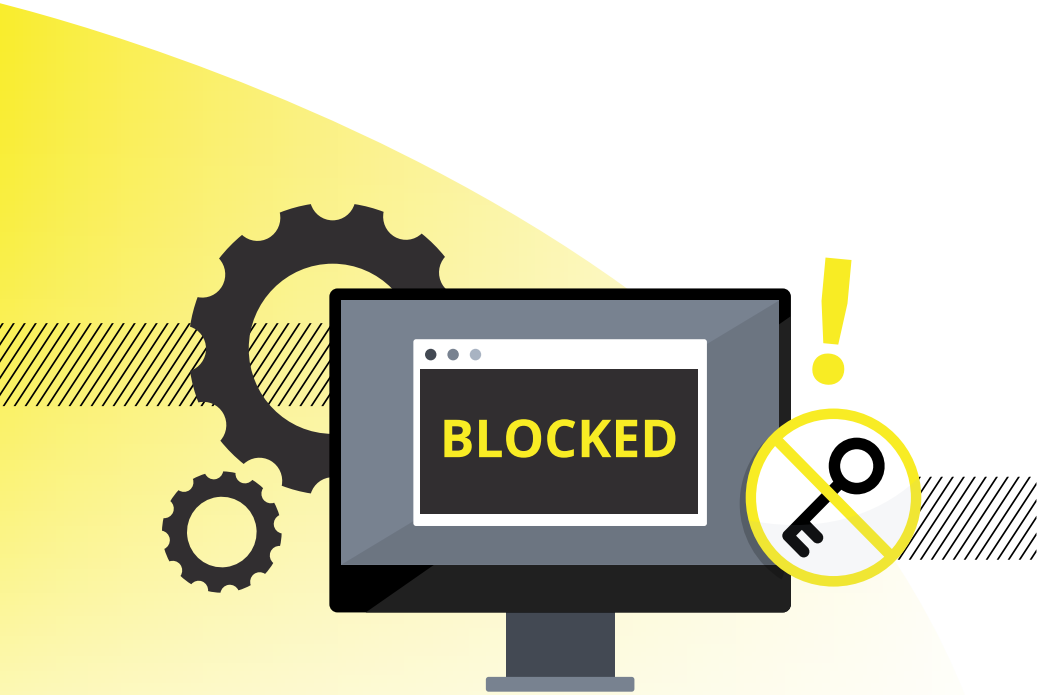
Businesses must take every precaution to put themselves in the best possible position to recover from a ransomware attack. Having a BCDR solution, a ransomware-specific incident response plan and EDR with a ransomware rollback feature will go a long way toward mitigating disaster.

WHAT DO YOU BELIEVE IS THE LIKELIHOOD YOUR ORGANIZATION WILL EXPERIENCE A SUCCESSFUL RANSOMWARE ATTACK IN THE NEXT 12 MONTHS?



IF A SUCCESSFUL RANSOMWARE ATTACK ON YOUR BUSINESS WERE TO OCCUR, HOW MUCH IMPACT DO YOU THINK IT WOULD HAVE?

Severity of Impact	*Response*
Extreme impact – it would be difficult to recover	***17%***
Significant impact	***53%***
Minimal impact	***28%***
No impact	***2%***

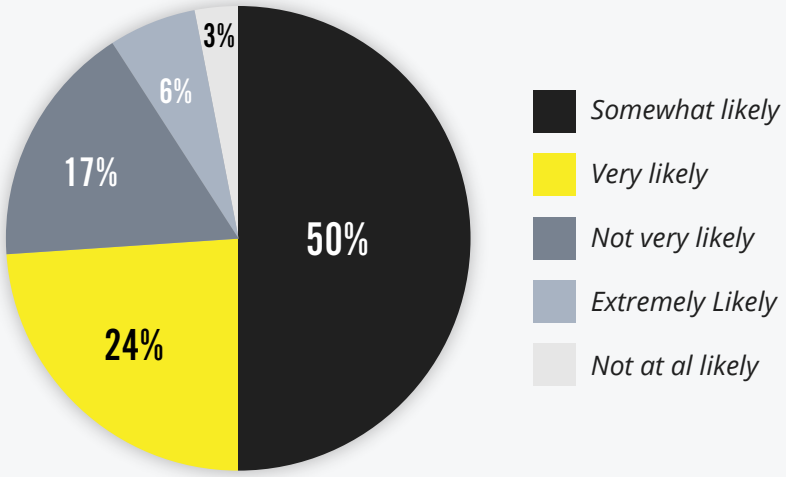


WHICH OF THE FOLLOWING THREAT VECTORS ARE YOU MOST CONCERNED ABOUT BEING THE GATEWAY TO A SUCCESSFUL ATTACK IN THE NEXT 12 MONTHS?

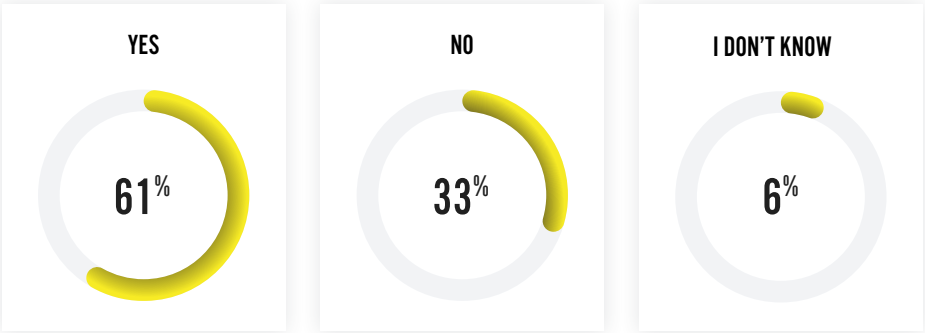
Attack Vector	*Response*
Email	***25%***
Human error (social engineering, distraction)	***16%***
Endpoint (server)	***12%***
Endpoint (laptop)	***11%***
Cloud	***10%***
Network	***8%***
Insider threats	***6%***
Supply chain	***5%***
Unpatched systems (Zero-day attacks)	***5%***
None	***2%***

When considering the vector through which their organization might suffer a successful cyberattack, one-quarter of our respondents chose email, highlighting the importance of having powerful, layered email security solutions in place to minimize risk. Nearly another one-quarter of survey respondents said that they consider endpoints to be their most vulnerable vector (23%). It is interesting to note that 22% of respondents chose a people-related vector, human error or insider threat, as the most likely conduit for a successful cyberattack against their employer. This result reinforces the importance of security awareness training for every employee. Education and training dramatically reduce a company's risk of falling prey to a cybersecurity incident.

WHAT DO YOU BELIEVE IS THE LIKELIHOOD THAT YOUR ORGANIZATION WILL EXPERIENCE A SUCCESSFUL PHISHING ATTACK IN THE NEXT 12 MONTHS?



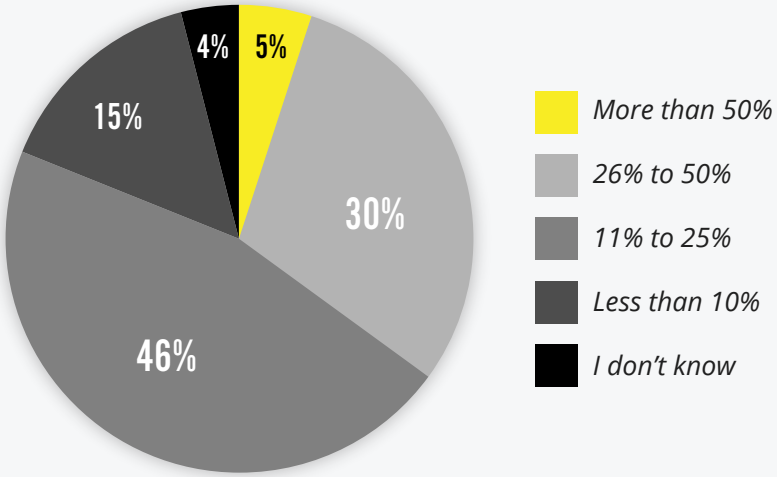
HAVE YOU EXPERIENCED A SUPPLY CHAIN ATTACK THROUGH YOUR SUPPLIER OR SERVICE PROVIDER?



Supply chain cyberattacks have been the story of the year in 2023, with more than 600 businesses worldwide impacted by the MOVEit file transfer exploit. The majority of our survey respondents (61%) said their organization experienced a cyberattack through their supply chain or a third-party service provider. Supply chain cyberattacks are expected to be a continued problem for businesses as the world grows more interconnected.

Most of today's most dangerous and devastating cyberattacks, like ransomware and BEC, typically start with phishing. Unfortunately, most of our survey respondents said they believe their organization is likely to fall victim to a phishing attack in the next year (80%). Now is the time to take measures, such as improving email security and educating users through phishing simulations, to prevent that attack from landing.

APPROXIMATELY WHAT PERCENTAGE OF YOUR OVERALL IT BUDGET IS DEDICATED TO SECURITY?



For the most part, respondents are choosing to invest in security. Just over three-quarters of our (76%) said that up to 50% of their company's total IT budget is dedicated to security. Drilling deeper, more than half of respondents (60%) said that their IT security budget was unchanged in the past 12 months. Many IT professionals are looking at good news ahead in terms of budget. About three-quarters of respondents (75%) expect their budgets to stay the same or increase in the next year. However, just under one-third of respondents said they expect budget cuts.

60% OF RESPONDENTS EXPECT CYBERSECURITY BUDGETS TO REMAIN FLAT IN 2023, BUT 43% EXPECT AN INCREASE IN 2024 SECURITY SPENDING.

DID YOUR COMPANY'S IT SECURITY BUDGET INCREASE, STAY THE SAME OR DECREASE COMPARED TO 12 MONTHS AGO?

State of 2023 Security Budget	*Response*
Stayed the same	***60%***
Increased	***29%***
Decreased	***7%***
I don't know	***4%***

DO YOU EXPECT YOUR COMPANY'S IT SECURITY BUDGET TO INCREASE, STAY THE SAME OR DECREASE IN THE NEXT 12 MONTHS?

Anticipated 2024 security budget	*Response*
Stay the same	***45%***
Increase	***43%***
Decrease	***7%***
I don't know	***4%***

RESPONDENT DEMOGRAPHICS

Our survey respondents are IT professionals around the world who all face the same challenge: securing their organization's systems and data against constantly growing cyberthreats.

Just over three-quarters of our survey respondents this year were from the United States.

In which country is your corporate headquarters located?

United Kingdom	3%
Belgium	3%
France	2%
Germany	1%
Ireland	1%
Italy	1%
The Netherlands	1%
New Zealand	1%
South Africa	1%
Sweden	1%
Other	3%

WHICH OF THE FOLLOWING RANGES BEST DESCRIBES YOUR COMPANY'S ANNUAL REVENUE?

Annual revenue	Response
Over 1 billion	***13%***
$500 million to $1 billion	***9%***
$100 million to $500 million	***11%***
$50 million to $100 million	***17%***
$10 million to $50 million	***23%***
$1 million to $10 million	***17%***
Less than $1 million	***9%***

WHAT IS THE TOTAL NUMBER OF EMPLOYEES IN YOUR COMPANY?

Company Size	Response
More than 3,000	***7%***
1,001 to 3,000	***12%***
501 to 1,000	***19%***
101 to 500	***31%***
51 to 100	***23%***
Less than 50	***7%***

KEY TAKEAWAYS

To Our 2023 Cybersecurity Survey report offers plenty of food for thought. Here are a few key takeaways based on the responses we received:

- Several of the biggest threats that businesses face every day, like ransomware, are primarily email-based, and that is the top threat vector that survey respondents are concerned about, creating a need for businesses to take steps to mitigate that risk by improving email security.

- IT professionals and IT decision-makers are aware that a successful cyberattack could be extremely damaging or fatal to a business, and they're taking steps to protect their organizations with actions, such as buying cyber insurance, investing in new cybersecurity solutions and developing a relationship with an MSP or MSSP.

- Lack of security awareness training for users and administrators alike is the primary cause of cybersecurity issues as human-centered vectors are the avenues of attack that IT professionals expect problems from the most.

- IT security budgets are expected to stay the same or increase in 2024, enabling IT leaders to fulfill key priorities like upgrading endpoint security, improving cloud security and utilizing a backup and disaster recovery solution. This evidence indicates budget controllers are prioritizing cybersecurity even in a challenging economy.

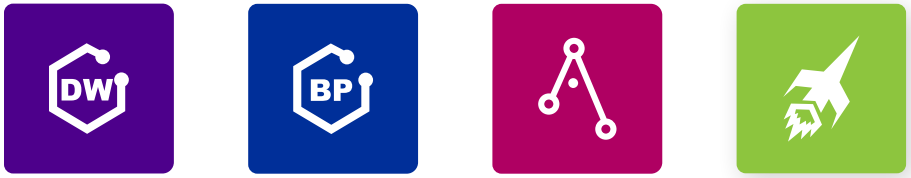
Security remains a paramount concern among respondents. Learn more about how Kaseya's security solutions can protect your business.

REQUEST A DEMO

SURVEY METHODOLOGY

The Kaseya 2023 Cybersecurity Survey polled 2,500 IT professionals around the world about their IT security experiences and opinions in August and September 2023. To simplify the questionnaires, pricing and revenue information was requested in U.S. dollars, and respondents were asked to select from price ranges rather than to specify exact figures. Overall, we've made every attempt to provide the data in a format that is most useful to the widest audience possible. We hope you find this useful and informative.

Learn more about Kaseya's Security Suite



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.

ID AGENT
A Kaseya COMPANY