CYBER INSECURITY IN HEALTHCARE:

THE COST AND IMPACT ON PATIENT SAFETY AND CARE

Independently conducted by:

Ponemon INSTITUTE

Sponsored by:

proofpoint.

TABLE OF CONTENTS

KEY FINDINGS

BY THE NUMBERS

88%

of organizations had at least one cyber attack over the past 12 months

40

The average number of cyber attacks in this group

$4.9M

The average total cost for the single most expensive cyber attack over the past 12 months

$1.3M

The average cost of disruption to normal healthcare operations was the most expensive financial consequence from a cyber attack—a 30% increase from 2022.

ORGANIZATIONS ARE UNPREPARED TO STOP ATTACKS, WHICH IMPACTS PATIENT SAFETY AND CARE

RANSOMEWARE

54%

of organizations experienced on average **four ransomware attacks** in the past two years.

68%

of this group say ransomware attacks negatively impacted patient safety and care.

BEC

54%

of organizations experienced an average of **five BEC attacks** in the past two years.

69%

of this group say BEC attacks disrupted patient care.

(CONT) ORGANIZATIONS ARE UNPREPARED TO STOP ATTACKS, WHICH IMPACTS PATIENT SAFETY AND CARE

64%

of organizations experienced an average of **four supply chain attacks** in the last two years.

77%

of this group say those attacks impacted patient care.

ONLY 45% of organizations say they have a strategy to stop BEC and supply chain attacks.

MOVING TO THE CLOUD INCREASES RISKS AND VULNERABILITIES

63% of organizations had an average of **21 cloud compromises** during the past two years.

53% of respondents say project management and video conferencing tools were most attacked.

Despite these risks, the use of CASB and encryption tools to protect sensitive information in the cloud decreased significantly.

DATA LOSS AND EXFILTRATION IS ON THE RISE

100%

of organizations had at least one incident where sensitive healthcare data was lost or stolen.

Malicious insiders are the No. 1 cause of data loss and exfiltration.

19

The average number of data loss incidents was 19.

43%

say these incidents impacted patient care.

47% are very concerned that employees don't understand the sensitivity and confidentiality of data they share via email.

EXECUTIVE SUMMARY

A STRONG CYBERSECURITY POSTURE IN HEALTHCARE ORGANIZATIONS IS IMPORTANT TO NOT ONLY SAFEGUARD SENSITIVE PATIENT INFORMATION BUT TO DELIVER THE BEST POSSIBLE MEDICAL CARE.

This second annual report was conducted to determine if the healthcare industry is making progress in achieving these two objectives.

With sponsorship from Proofpoint, Ponemon Institute surveyed 653 IT and IT security practitioners in U.S. healthcare organizations who are responsible for participating in such cybersecurity strategies as setting IT cybersecurity priorities, managing budgets and selecting vendors and contractors.

According to the research, 88 percent of organizations surveyed experienced at least one cyberattack in the past 12 months. For organizations in that group, the average number of cyberattacks was 40. We asked respondents to estimate the single most expensive cyberattack experienced in the past 12 months from a range of less than $10,000 to more than $25 million. Based on the responses, the average total cost for the most expensive cyberattack was $4,991,500, a 13 percent increase over last year. This included all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunities.

At an average cost of $1.3 million, disruption to normal healthcare operations because of system availability problems was the most expensive consequence from the cyberattack, an increase from an average $1 million in 2022. Users' idle time and lost productivity because of downtime or system performance delays cost an average of $1.1 million, the same as in 2022. The cost of the time required to ensure the impact on patient care was corrected increased over 50 percent from an average of $664,350 in 2022 to $1 million in 2023.

of organizations in this research had at least one cyberattack over the past 12 months

The average total cost for the single most expensive cyberattack experienced over the past 12 months

in disruption to normal healthcare operations was on average the most significant financial consequence from the cyberattack

The report analyzes four types of cyberattacks and their impact on healthcare organizations, patient safety and patient care delivery:

CLOUD COMPROMISE

The most frequent attacks in healthcare are against the cloud, making it the top cybersecurity threat, according to respondents. Seventy-four percent of respondents say their organizations are vulnerable to a cloud compromise. Sixty-three percent say their organizations have experienced at least one cloud compromise. In the past two years, organizations in this group experienced 21 cloud compromises. Sixty-three percent say they are concerned about the threat of a cloud compromise, an increase from 57 percent.

BUSINESS EMAIL COMPROMISE (BEC)/SPOOFING PHISHING.

Concerns about BEC attacks have increased significantly. Sixty-two percent of respondents say their organizations are most concerned about a BEC/spoofing phishing incident, an increase from 46 percent in 2022. In the past two years, the frequency of such attacks increased as well from an average of four attacks to five attacks.

RANSOMWARE

Ransomware has declined as a top cybersecurity threat. Sixty-four percent of respondents believe their organizations are vulnerable to a ransomware attack. However, as a concern ransomware has decreased from 60 percent in 2022 to 48 percent in 2023. In the past two years, organizations that had ransomware attacks (54 percent of respondents) experienced an average of four such attacks, an increase from three attacks. While fewer organizations paid the ransom (40 percent in 2023 vs. 51 percent in 2022), the ransom paid increased nearly 30 percent from an average of $771,905 to $995,450.

SUPPLY CHAIN ATTACKS

Organizations are vulnerable to a supply chain attack, according to 63 percent of respondents. However, only 40 percent say this cyber threat is of concern to their organizations. On average, organizations experienced four supply chain attacks in the past two years.

As in the previous report, an important part of the research is the connection between cyberattacks and patient safety. Following are trends in how cyberattacks have affected patient safety and patient care delivery.

- **It is more likely that a supply chain attack will affect patient care.** Sixty-four percent of respondents say their organizations had an attack against their supply chains. Seventy-seven percent of those respondents say it disrupted patient care, an increase from 70 percent in 2022. Patients were primarily impacted by delays in procedures and tests that resulted in poor outcomes such as an increase in the severity of an illness (50 percent) and a longer length of stay (48 percent). Twenty-one percent say there was an increase in mortality rate.
- **A BEC/spoofing attack can disrupt patient care.** Fifty-four percent of respondents say their organizations experienced a BEC/spoofing incident. Of these respondents, 69 percent say a BEC/spoofing attack against their organizations disrupted patient care, a slight increase from 67 percent in 2022. And of these 69 percent, 71 percent say the consequences caused delays in procedures and tests that have resulted in poor outcomes while 56 percent say it increased complications from medical procedures.
- **Ransomware attacks can cause delays in patient care.** Fifty-four percent of respondents say their organizations experienced a ransomware attack. Sixty-eight percent of respondents say ransomware attacks have a negative impact on patient care. Fifty-nine percent of these respondents say patient care was affected by delays in procedures and tests that resulted in poor outcomes and 48 percent say it resulted in longer lengths of stay, which affects organizations' ability to care for patients.
- **Cloud compromises are least likely to disrupt patient care.** Sixty-three percent of respondents say their organizations experienced a cloud compromise, but less than half (49 percent) say cloud compromises disrupted patient care. Of these respondents, 53 percent say these attacks increased complications from medical procedures and 29 percent say they increased mortality rate.
- **Data loss or exfiltration disrupts patient care and can increase mortality rates.** All organizations in this research had at least one data loss or exfiltration incident involving sensitive and confidential healthcare data in the past two years. On average, organizations experienced 19 such incidents in the past two years and 43 percent of respondents say they impacted patient care. Of these respondents, 46 percent say it increased the mortality rate and 38 percent say it increased complications from medical procedures.

OTHER KEY TRENDS IN CYBER INSECURITY

CONCERNS ABOUT EMPLOYEE BEHAVIOR-RELATED THREATS INCREASED SIGNIFICANTLY

61%

of organizations are now worried about the security risks created by BYOD, an increase from 34% in 2022.

62%

are concerned about BEC/spoof phishing, an increase from 46% in 2022.

THE TOTAL COST OF A CYBERSECURITY COMPROMISE

$1.3M

Disruption to normal healthcare operations because of system availability problems increased to $1.3 million from $1 million in 2022.

$1M

The cost of the time taken to ensure impact on patient care was corrected increased to $1 million in 2023 from $664,350 in 2022.

$1.1M

Users' idle time and lost productivity because of downtime or system performance delays averaged $1.1 million.

MALICIOUS INSIDERS AND ACCIDENTAL DATA LOSS ARE THE TOP TWO CAUSES OF DATA LOSS AND EXFILTRATION

Malicious insiders are **the number one cause** of data loss and infiltration.

32%

Yet only 32% say they are prepared to prevent and respond to this threat.

Accidental data loss is **the second highest cause** of data loss and exfiltration.

47%

say their organizations are very concerned that employees do not understand the sensitivity and confidentiality of data they share by email.

MORE PROGRESS IS NEEDED TO REDUCE THE RISK OF DATA LOSS OR EXFILTRATION

19

All organizations in this research have experienced at least one data loss or exfiltration incident involving sensitive and confidential healthcare data.

The average number of such incidents is 19.

43%

say data loss or exfiltration impacted patient care.

Of this group:

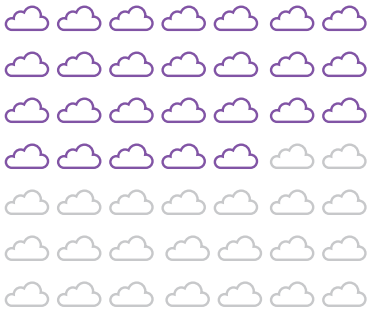
46%

say it increased mortality rates.

38%

say it increased complications from medical procedures.

CLOUD-BASED USER ACCOUNTS/ COLLABORATION TOOLS ARE MOST OFTEN ATTACKED



53%

say project management tools and Zoom/Skype/ video-conferencing tools were attacked.

THE LACK OF PREPAREDNESS TO STOP BEC/SPOOF PHISHING AND SUPPLY CHAIN ATTACKS PUTS ORGANIZATIONS AND PATIENTS AT RISK

45%

While BEC/spoof phishing is considered a top cybersecurity threat, only 45% say their organizations include steps to prevent and respond to such an attack as part of their cybersecurity strategy.

45%

Similarly, only 45% say their organizations have documented the steps to prevent and respond to attacks in the supply chain.

TOP THREE CHALLENGES TO HAVING AN EFFECTIVE CYBERSECURITY POSTURE

EXPERTISE

58%

say they lack in-house expertise, up from 53% in 2022.

STAFFING

50%

say insufficient staffing is a problem, up from 46%.

BUDGET

47%

say they don't have enough budget, up from 41%.

SECURITY AWARENESS TRAINING PROGRAMS CONTINUE TO BE THE PRIMARY STEP TAKEN TO REDUCE INSIDER RISK

More organizations say they are taking steps to address the risk of employees' lack of awareness about cybersecurity threats.

65% in 2023 VS 59% in 2022

Of this group:

say they conduct regular training and awareness programs.

say they monitor the actions of employees.

USE OF CASB AND ENCRYPTION TOOLS TO PROTECT SENSITIVE INFORMATION IN THE CLOUD DECREASED SIGNIFICANTLY

CASB

43% in 2023 VS 53% in 2022

ENCRYPTION TOOLS

59% in 2023 VS 65% in 2022

ANALYSIS

The complete audited findings are presented in the Appendix of this report. Whenever possible, we compare the 2022 findings to this year's report. The report is organized according to the following topics:

- Cloud compromise, ransomware, supply chain and BEC in healthcare
- The impact of cyberattacks on patient care
- The cost of cyber insecurity
- Vulnerabilities in the cloud and risk to patient data
- Solutions and responses to healthcare cyber insecurity

CLOUD COMPROMISE, RANSOMWARE, SUPPLY CHAIN AND BEC IN HEALTHCARE

FIGURE 1.

Healthcare organizations are vulnerable to cyberattacks

Healthcare organizations recognize how vulnerable they are to the four cyberattacks featured in this research. Respondents were asked to rate their organizations' vulnerability to specific types of cyberattacks on a scale from 1 = not vulnerable to 10 = highly vulnerable.

Figure 1 presents the very vulnerable to highly vulnerable responses (7+ on the 10-point scale are presented). As shown, almost all respondents recognize the threat of cloud compromises (74 percent). Concerns about ransomware attacks (64 percent) and supply chain attacks (63 percent) have declined from 72 percent and 71 percent, respectively.

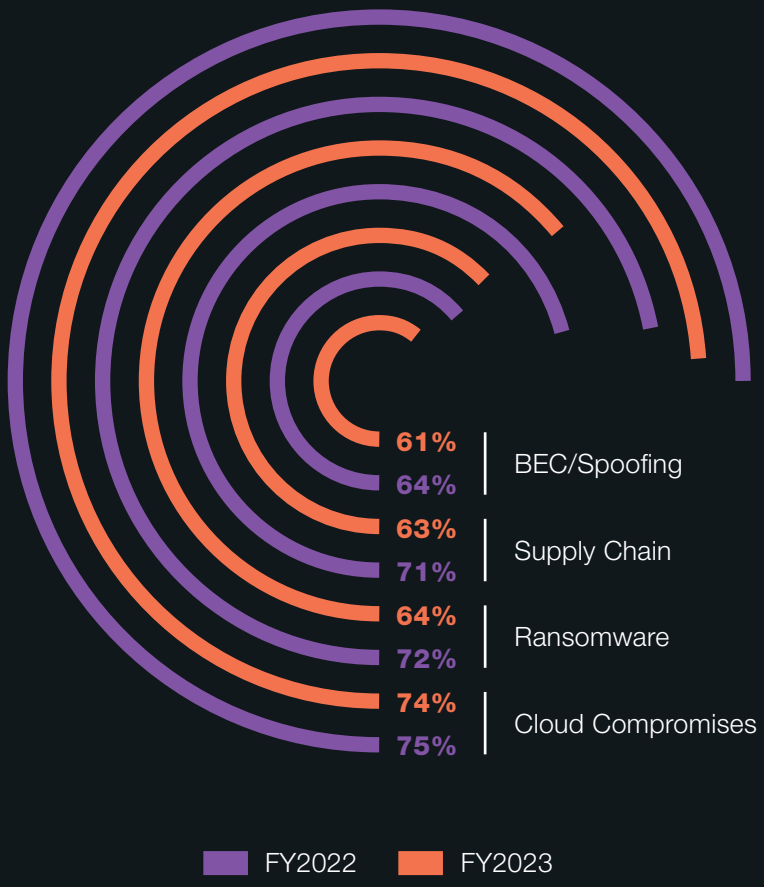
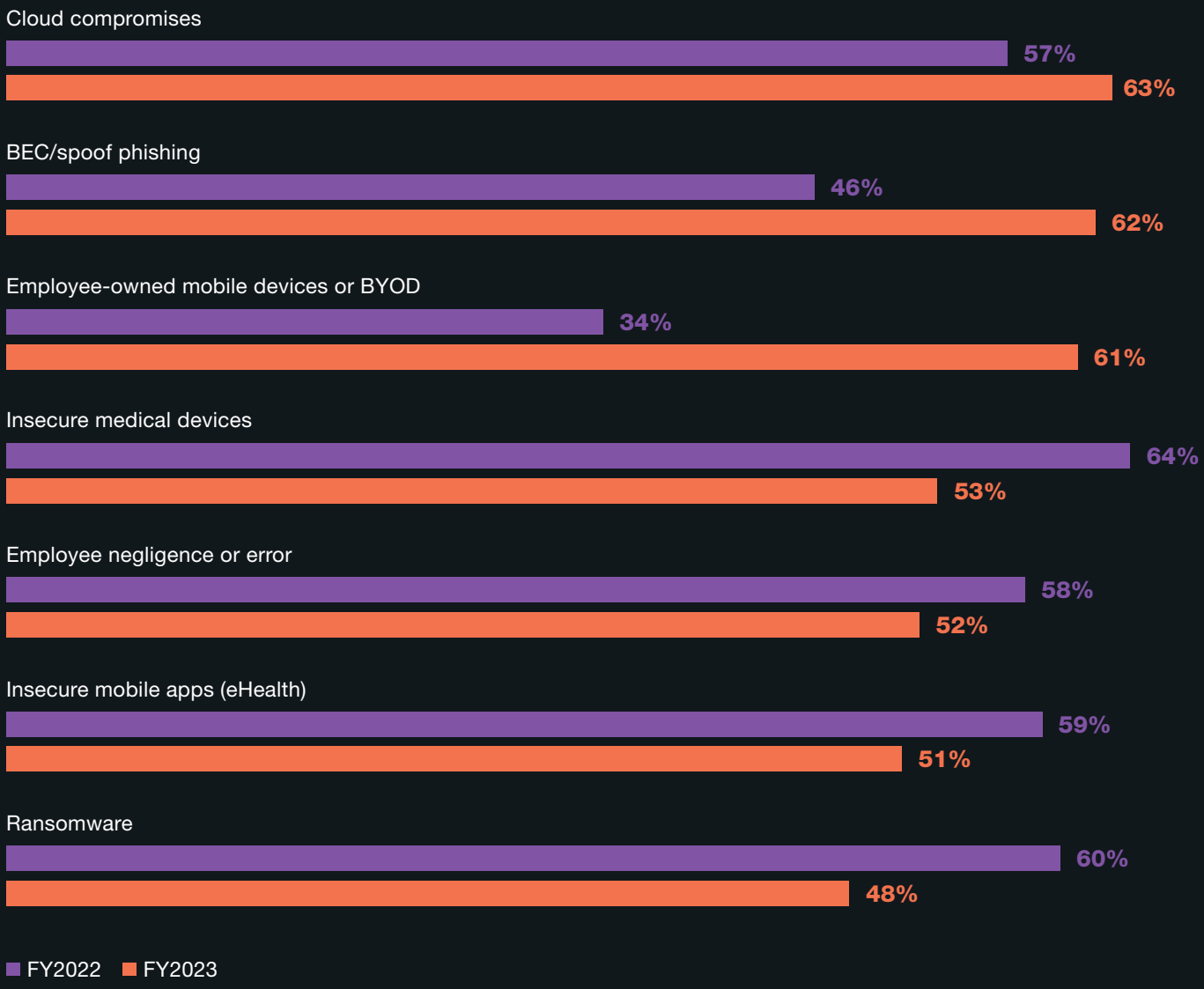


FIGURE 2.

The top cybersecurity threats of greatest concern

In this year's research, cloud compromises and BEC/spoof phishing attacks replace insecure medical devices and ransomware as the top cybersecurity threats in healthcare. As shown in Figure 2, last year's two top concerns were insecure medical devices and ransomware (64 percent and 60 percent of respondents, respectively). Today, cloud compromises and BEC/spoof phishing (63 percent and 62 percent, respectively) are the top threats to prepare for. Since 2022, threats created by employee-owned mobile devices or BYOD have increased significantly from 34 percent to 61 percent, respectively.

More than one response permitted



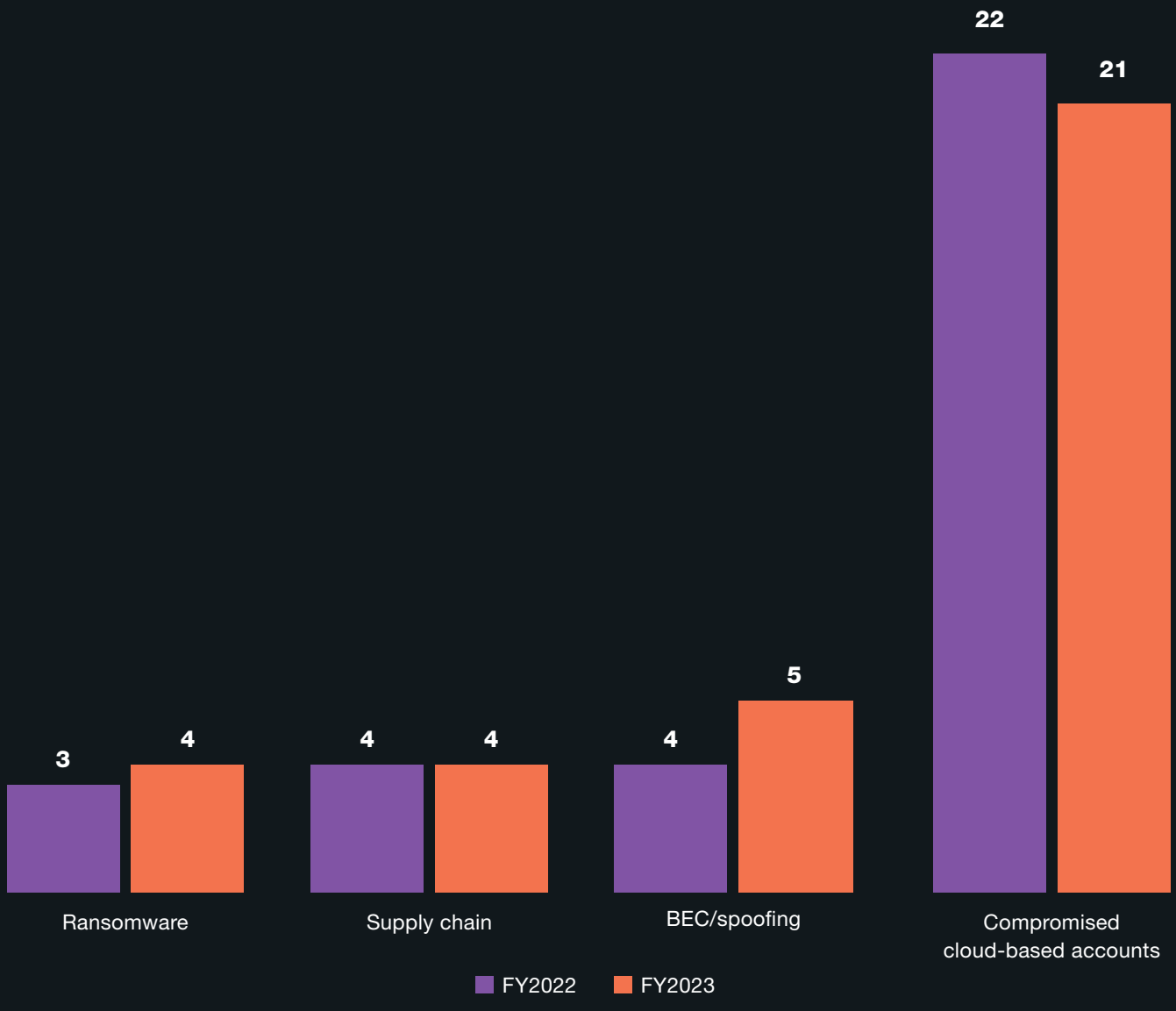
Cloud compromises continue to be the most frequent type of attack against healthcare organizations.

Figure 3A shows the average frequency for each type of cyberattack. Cloud compromise results from criminals obtaining access to credentials (e.g., user ID and passwords). The consequence is typically an account takeover where criminals then use those validated credentials to commit fraud and transfer sensitive data to systems under their control. Sixty-three percent of respondents say their organizations experienced a cloud compromise. The average number of cloud compromises for these healthcare organizations was 21 in the past two years.

FIGURE 3A.

Average number of attacks for the four types of cyberattacks in the past two years

Extrapolated value



Organizations that had a ransomware attack (54 percent of respondents) experienced an average of four ransomware attacks in the past two years. Ransomware is a sophisticated piece of malware that blocks the victim's access to files. While there are many strains of ransomware, they generally fall into two categories. Crypto ransomware encrypts files on a computer or mobile device making them unstable. It takes the files hostage, demanding a ransom in exchange for the decryption key needed to restore the files. Locker ransomware is a virus that blocks basic computer functions, essentially locking the victim out of their data and files located on the infected devices. Instead of targeting files with encryption, cybercriminals demand a ransom to unlock the device.

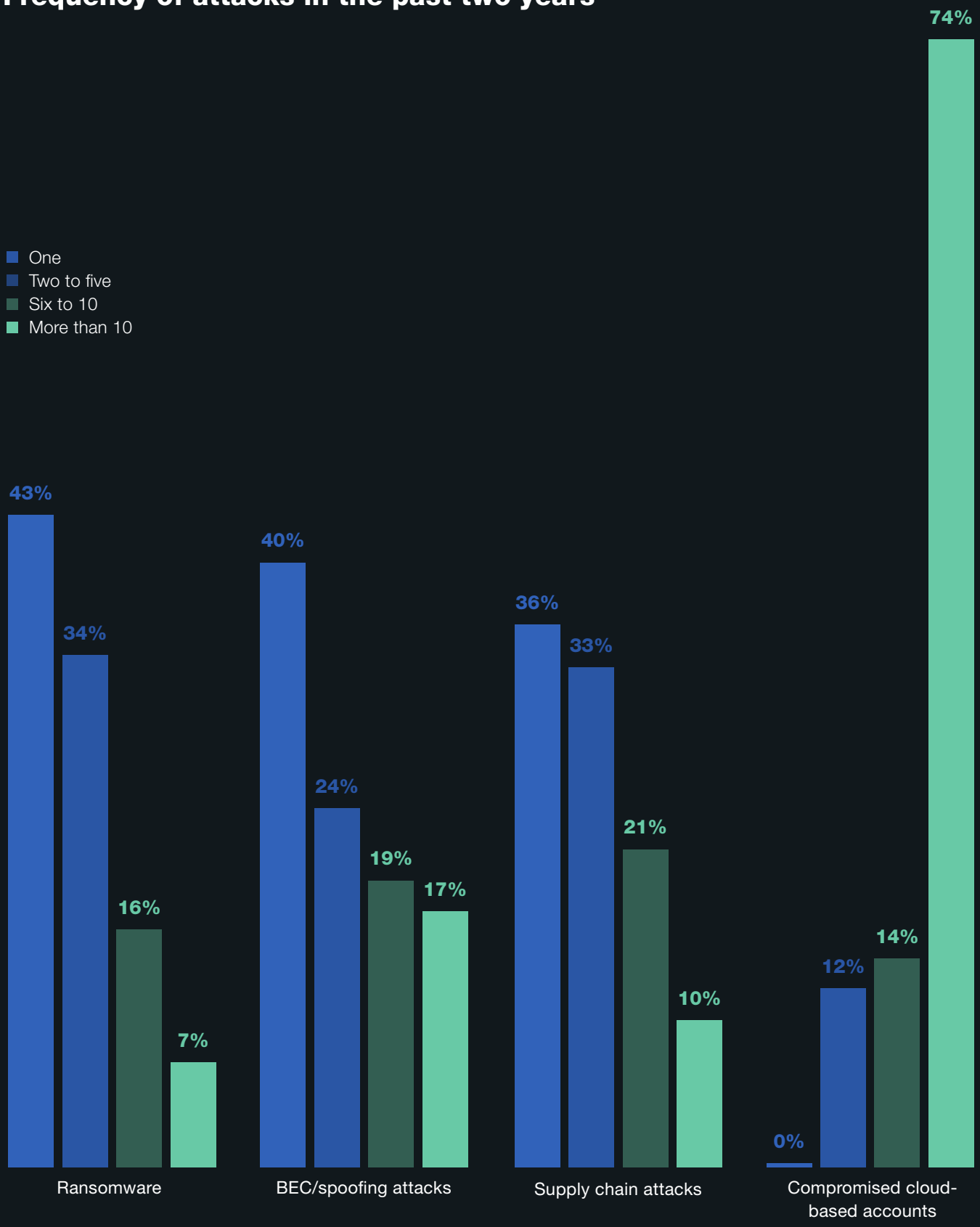
In the past two years, 64 percent of respondents say their organizations' supply chains were attacked an average of 4 times. Supplier impersonation and compromise attacks occur when a malicious actor impersonates or successfully compromises an email account in the supply chain. The attacker then observes, mimics and uses historical information to craft scenarios to spoof employees in the supply chain.

In the past two years, 54 percent of healthcare organizations experienced an average of 5 BEC/spoofing phishing attacks. BEC attacks are a form of cybercrime that uses email fraud to attack healthcare organizations to achieve a specific outcome. Examples include invoice scams, spear phishing that are designed to gather data for other criminal activities, attorney impersonation and CEO fraud.

Figure 3A presents the extrapolated average number of attacks. Figure 3B shows how many attacks for the four types of cyberattacks they experienced on a scale from 1 to more than 10. Seventy-four percent of respondents say cloud-based user accounts were compromised more than 10 times. Most organizations represented in this research had one incident involving the following: ransomware (43 percent of respondents), BEC/spoofing attacks (40 percent) and supply chain attacks (36 percent).

FIGURE 3B.

Frequency of attacks in the past two years



ACCORDING TO THE RESEARCH, CYBERATTACKS HAVE DISRUPTED CARE, INCREASING THE RISK TO PATIENTS.

FIGURE 4.

Did cyberattacks disrupt patient care?

Figure 4 shows the four types of cyberattacks featured in this research and if they had a negative impact on patient safety and delivery of care. Such disruptions include delays in procedures and tests that have resulted in poor outcomes, longer lengths of stay, increases in patients transferred or diverted to other facilities, increases in complications from medical procedures and increases in mortality rate.

Of those organizations that experienced these attacks, more respondents this year (77 percent vs. 70 percent in 2022) believe the supply chain attacks disrupted patient care followed by the BEC/spoofing and ransomware attacks (69 percent and 68 percent, respectively). Cloud compromises are having less impact on patient care, a decrease from 64 percent to 49 percent.

Yes responses presented

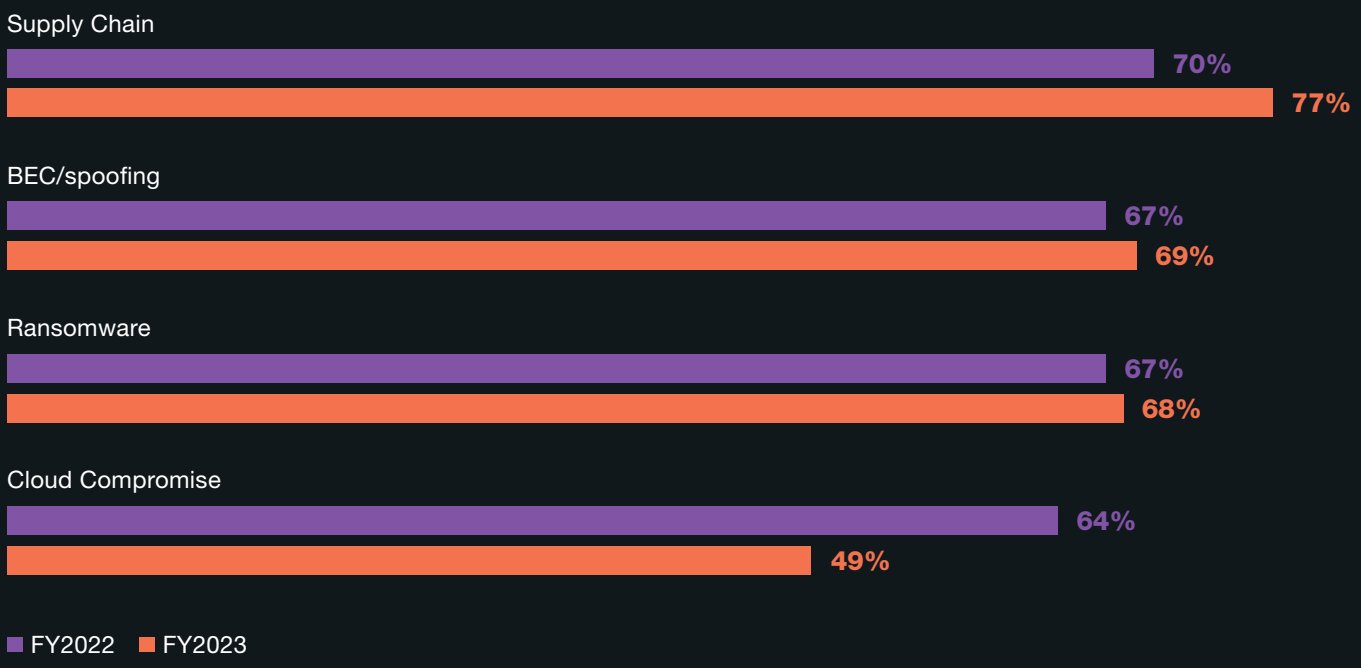
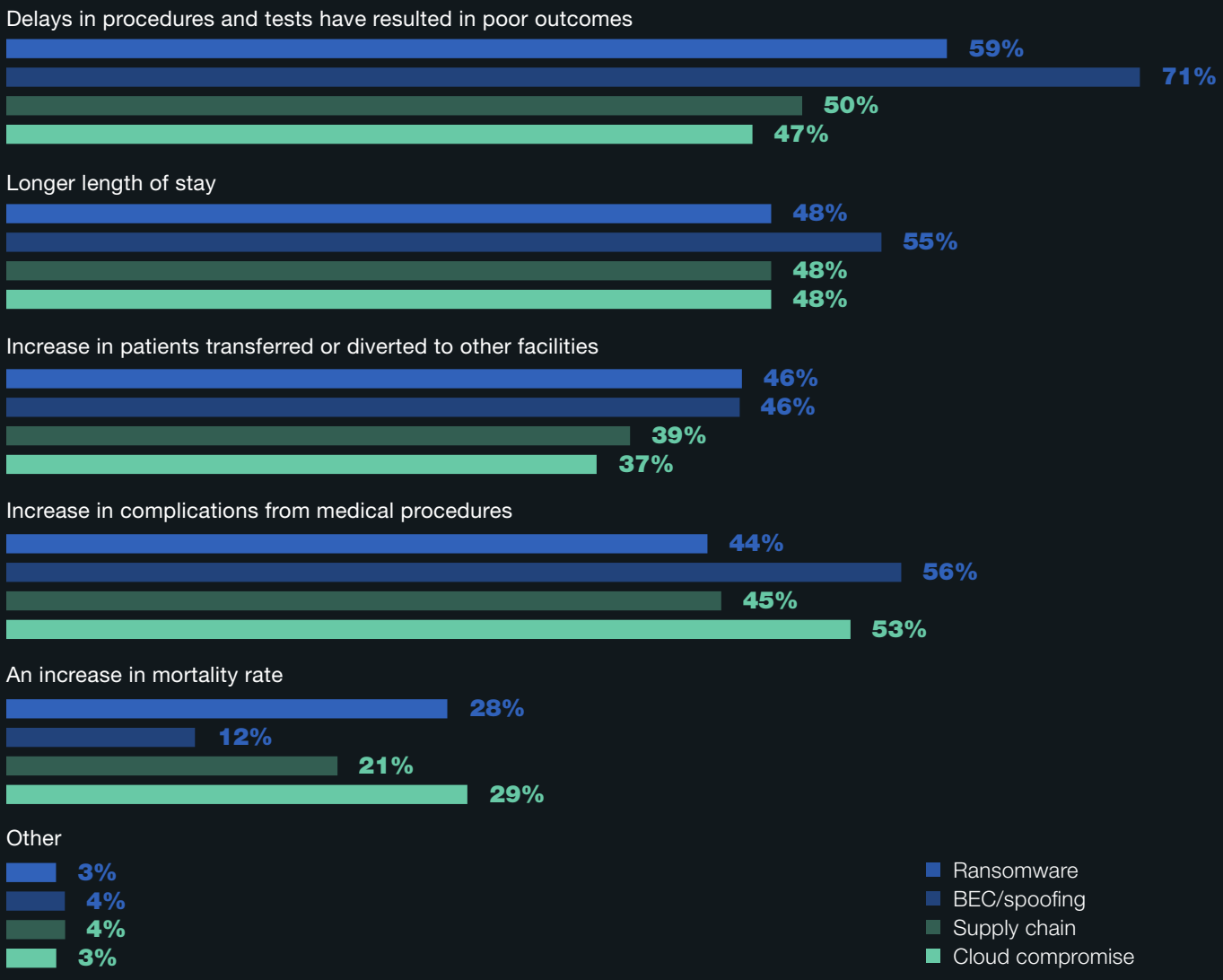


FIGURE 5.

If your organization experienced these cyberattacks, what impact did they have on patient care?

To protect patients, organizations need to reduce BEC/spoofing attacks. As shown in Figure 5, 71 percent of respondents in organizations that had a BEC/spoofing attack say it caused delays in procedures and tests that resulted in poor outcomes such as the increase in the severity of the illness. These attacks also were more likely to cause longer lengths of stay (55 percent) and increases in complications from medical procedures (56 percent). Cloud compromises and ransomware were more likely to increase mortality rates (29 percent and 28 percent, respectively).

More than one response permitted



SYSTEM AVAILABILITY PROBLEMS AND DOWNTIME ARE THE MOST SIGNIFICANT FINANCIAL CONSEQUENCES FROM A CYBERSECURITY COMPROMISE.

Organizations also are spending more to ensure the impact on patient care is corrected.

TABLE 1.

Five average costs of a healthcare cybersecurity compromise

According to the research, 88 percent of organizations in this research experienced at least one cyberattack. In the past year, organizations experienced an average of 40 cyberattacks. As shown in Table 1, the average total cost for the single most expensive cyberattack was $4,991,500 million, an increase from $4,429,000. This includes all direct cash outlays, direct labor expenditures, indirect labor costs, overheard costs and lost business opportunities.

Respondents estimated that the highest cost ($1.3 million) was caused by disruption to normal healthcare operations because of system availability problems, an increase from $1 million in 2022. The cost due to users' idle time and lost productivity because of downtime or system performance delays was $1.1 million, the same as in 2022. The cost caused by the time required to ensure the impact on patient care was corrected increased from an average of $664,350 to $1 million in this year's report.

Other changes were a decrease in damage or theft of IT assets and infrastructure from $930,090 in 2022 to $748,725 in 2023 and an increase in remediation and technical support activities from $708,640 in 2022 to $748,725 in 2023.

HEALTHCARE CYBERSECURITY COMPROMISE	2023 AVERAGE COST	2022 AVERAGE COST
Disruption to normal healthcare operations because of system availability problems	$1,297,790	$1,018,670
Users' idle time and lost productivity because of downtime or system performance delays	$1,148,045	$1,107,250
Time required to ensure impact on patient care is corrected	$1,048,215	$664,350
Damage or theft of IT assets and infrastructure	$748,725	$930,090
Remediation & technical support activities, including forensic investigations, incident response activities, help desk and delivery of services to patients	$748,725	$708,640
Total	$4,991,500	$4,429,000

AS HEALTHCARE ORGANIZATIONS MOVE SENSITIVE PATIENT DATA TO THE CLOUD, RESPONDENTS RECOGNIZE THE RISKS.

FIGURE 6.

Which cloud-based user accounts/collaboration tools were most attacked in your organization?

Sixty-three percent of respondents say their organizations' cloud accounts were successfully compromised at some point. As shown in Figure 6, productivity tools, such as project management and videoconferencing tools, were the hardest hit (both 53 percent of respondents).

More than one choice permitted

FIGURE 7.

How does your organization protect confidential or sensitive information in the cloud?

More organizations concerned about protecting sensitive data in the cloud are shifting to the use of premium security services from the cloud provider. As shown in Figure 7, the use of premium security service increased from 56 percent of respondents in 2022 to 60 percent in this year's research. The use of a CASB and encryption, tokenization or other cryptographic tools decreased significantly from 53 percent to 43 percent in 2023 and 65 percent to 59 percent in 2023, respectively.

More than one response permitted

FIGURE 8.

What best describes your organization's approach to user access and identity management in the cloud?

Organizations are likely to use a combination of several approaches to user access and identity management in the cloud. To secure access to patient data in the cloud there are specific methods to pursue. As in last year's research, a hybrid combination is still the most often used. Fifty-six percent in 2023 vs. 60 percent of respondents in 2022 say their organizations use a combination of approaches, according to Figure 8.

This is followed by separate identity management interfaces for the cloud and on-premises environments (50 percent in 2023 vs. 53 percent in 2022) and unified identity management interface for both the cloud and on-premises environments (43 percent in 2023 vs. 48 percent in 2022). The deployment of SSO has declined from 37 percent in 2022 to 30 percent in 2023.

More than one response permitted

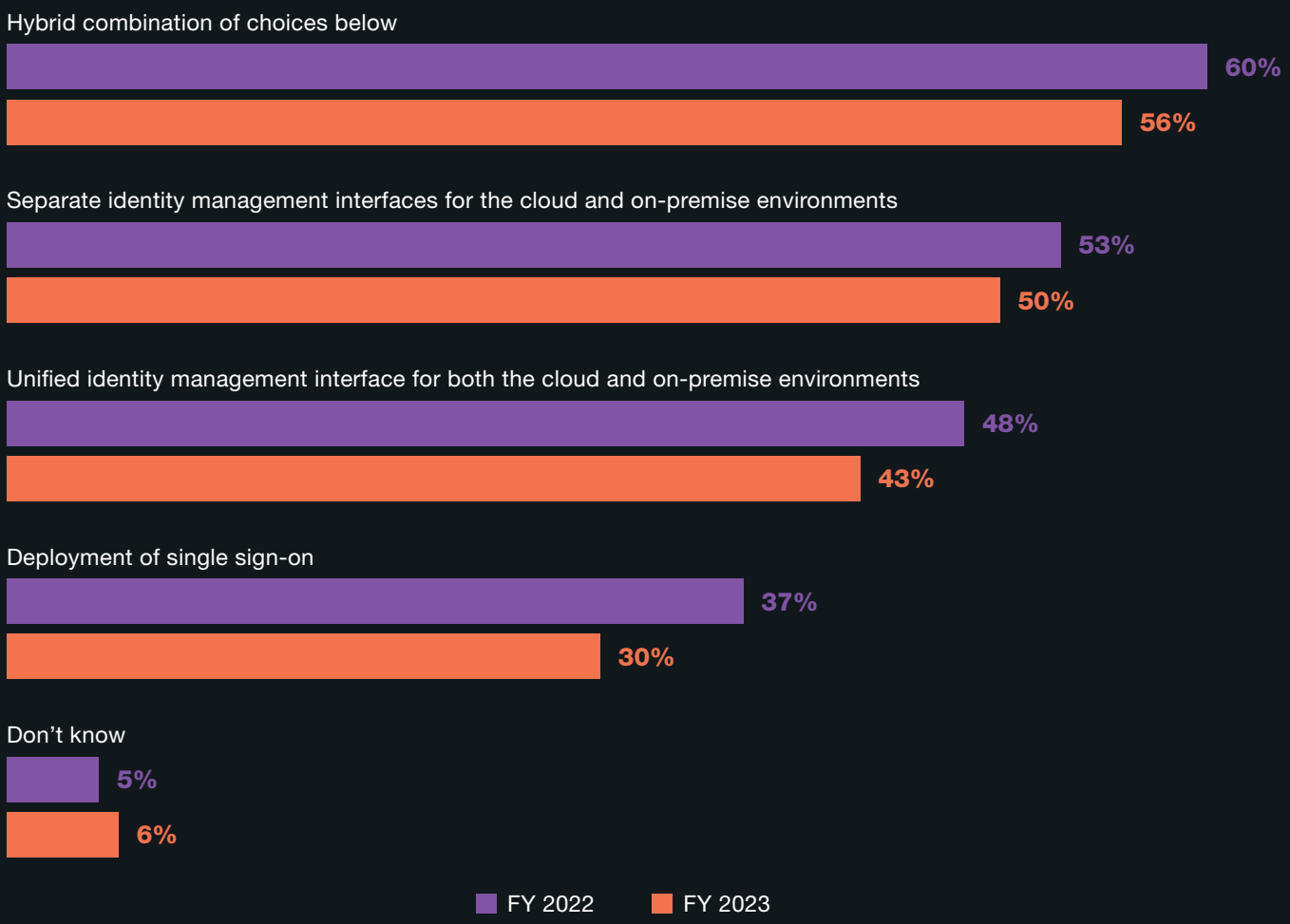


FIGURE 9.

How would you characterize the data loss or exfiltration?

More progress is needed to achieve a healthier security posture. All healthcare organizations in this research have experienced at least one data loss or exfiltration incident involving sensitive and confidential healthcare data. The average number of such incidents is 19. As shown here, malicious insiders (32 percent of respondents) most often caused data loss and infiltration followed by accidental data loss (27 percent).

A common example of accidental data loss is mistakes made when employees are emailing documents. Almost half of respondents (47 percent) in this survey say their organizations are very concerned that employees do not understand the sensitivity and confidentiality of data they share by email.

Only one choice permitted

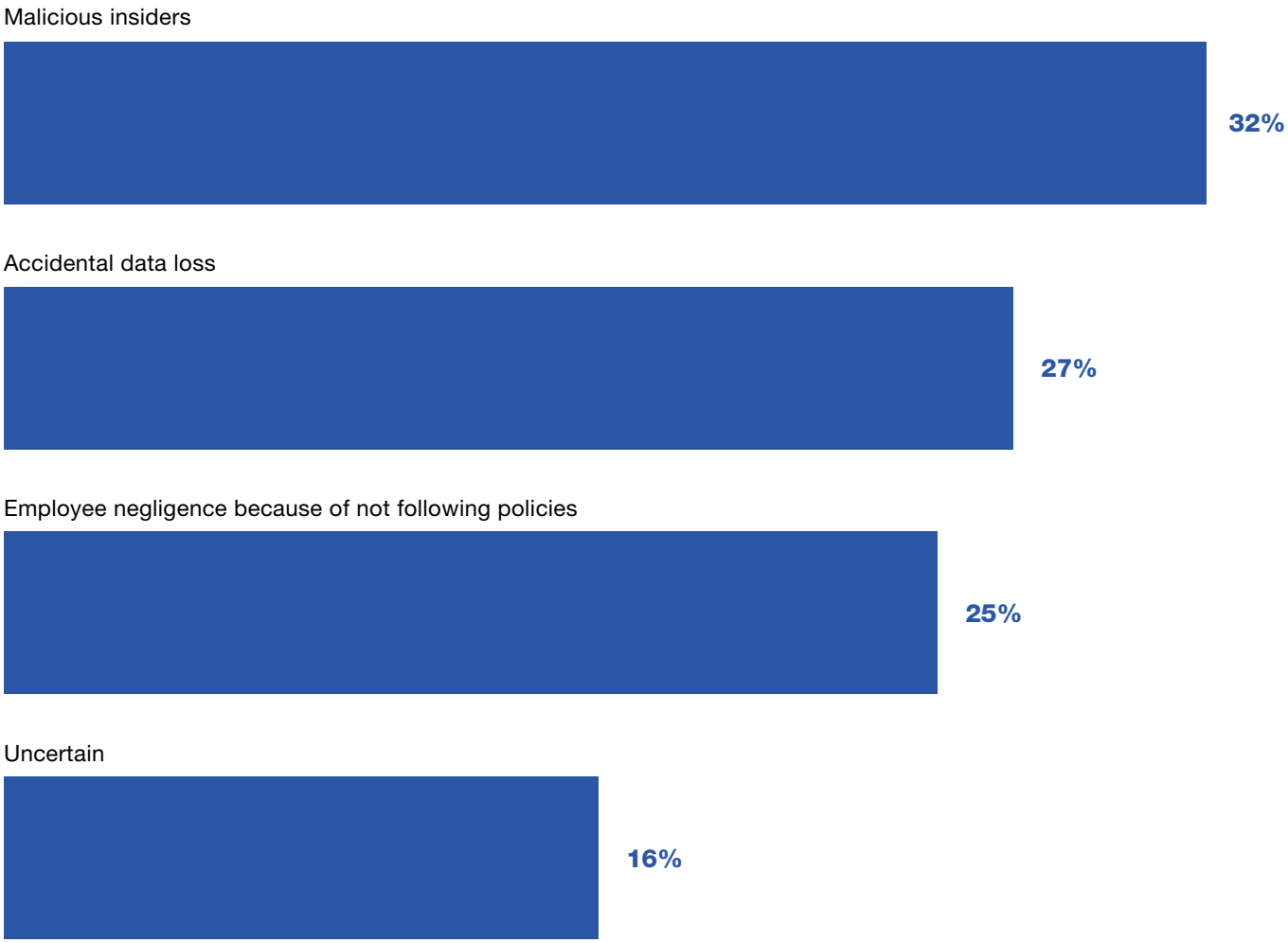


FIGURE 10.

What impact did the data loss protection or exfiltration incident have on patient care?

Data loss or exfiltration can disrupt patient care and increase mortality rates. Forty-three percent of respondents say the data loss or exfiltration incident had an impact on patient care. Of these respondents, 46 percent of respondents say it increased mortality rates and 38 percent say it increased complications from medical procedures, as shown in Figure 10.

More than one response permitted

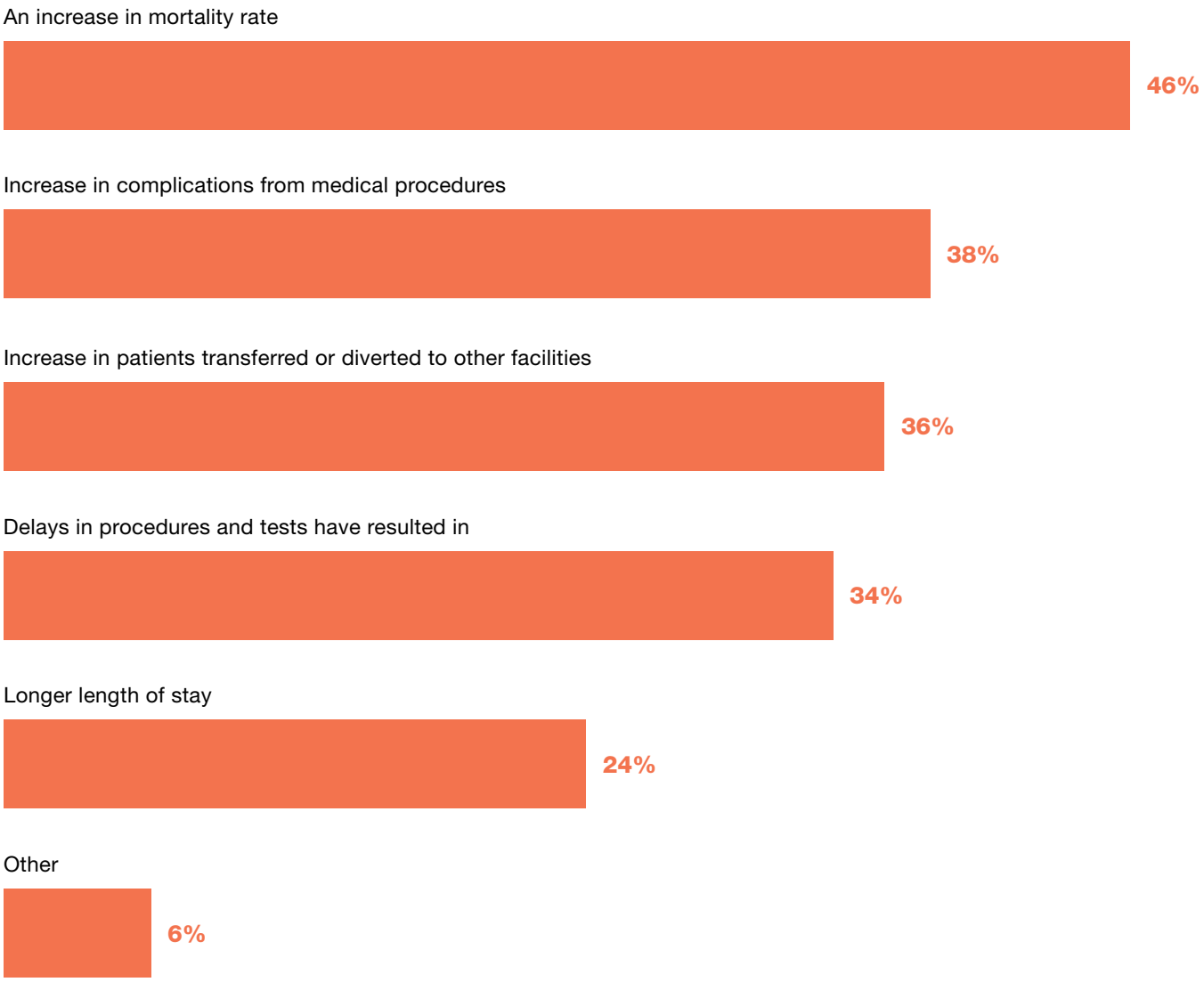


FIGURE 11.

What security methods and technologies does your organization use to reduce the consequences of a data loss or exfiltration incident?

According to Figure 11, the top security methods and technologies used to reduce the consequences are a cloud access security broker (CASB) (67 percent of respondents). CASBs can be used to prevent unauthorized sharing of sensitive data that limit or allow access based on employee status or location. Fifty-four percent say their organizations deploy user and entity behavior analytics (UEBA). Fifty-one percent say their organizations have an enterprise data loss prevention platform that covers multiple channels, including email, web, network endpoint and cloud.

More than one response permitted

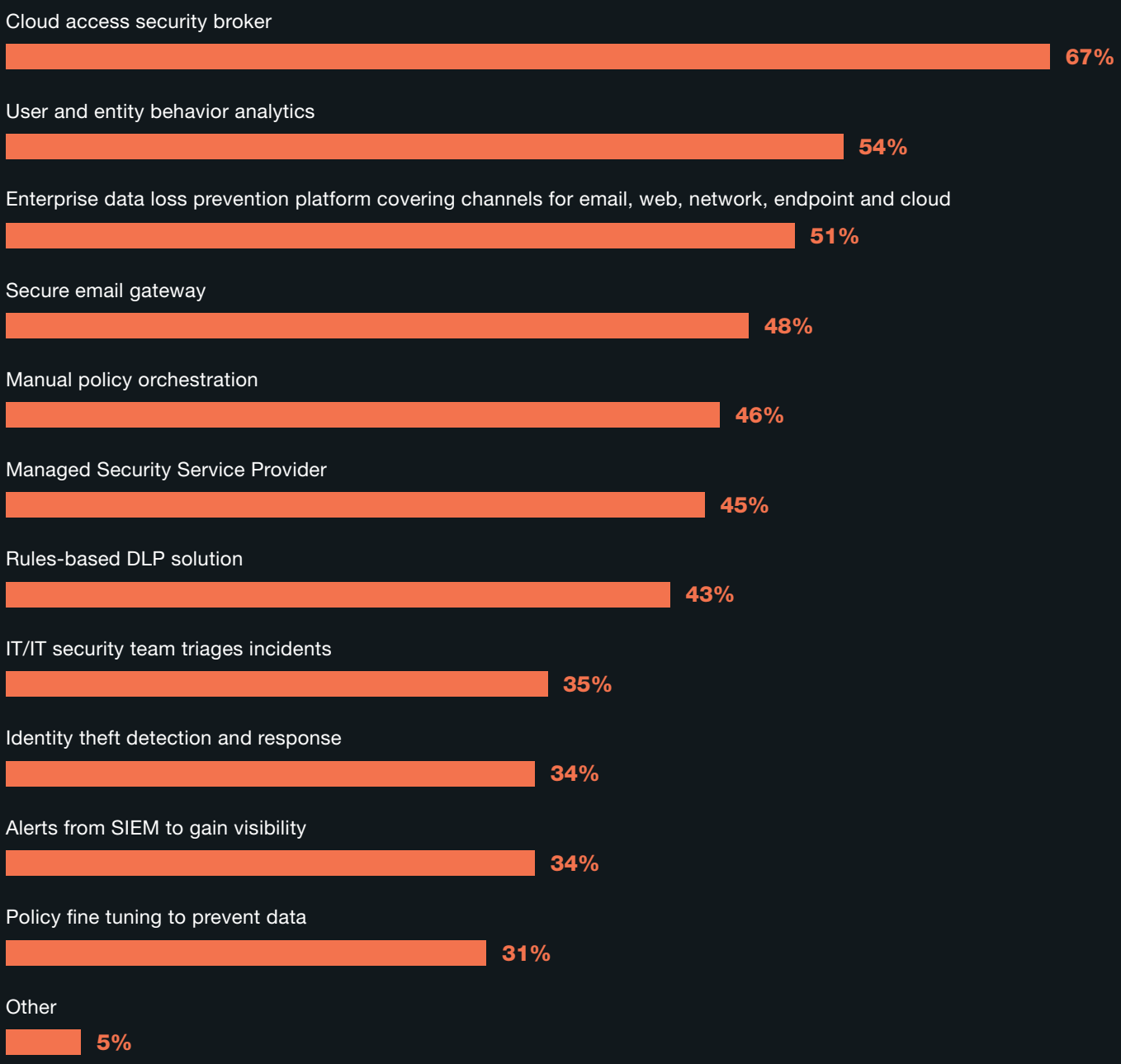
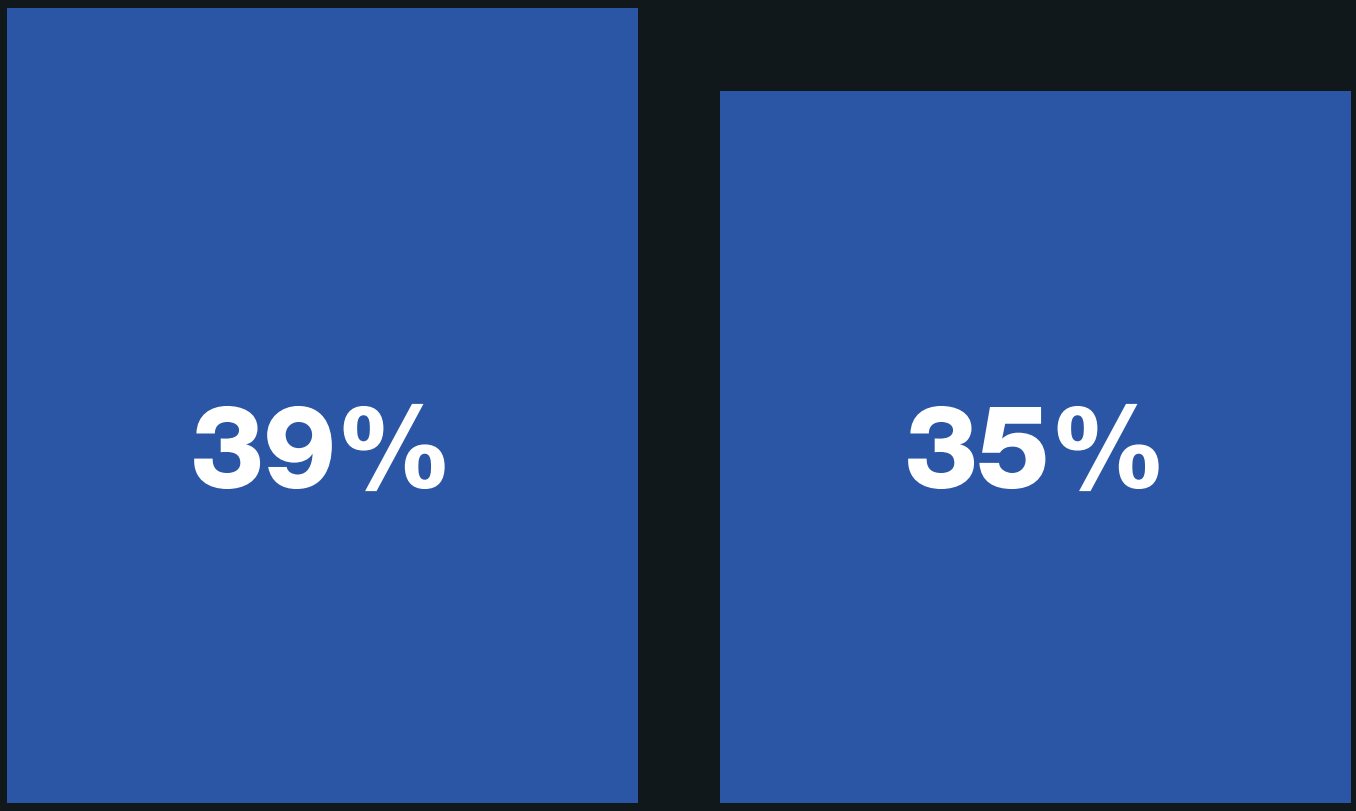


FIGURE 12.

How effective are your data loss prevention solutions in preventing data loss incidents by employees and malicious insiders?

New data loss prevention tools are needed. Respondents were asked to rate the effectiveness of their current solutions in preventing data loss incidents caused by malicious insiders and employees on a scale from 1 = not effective to 10 = very effective. Figure 12 presents the very effective responses (7+ on the 10-point scale). As shown, only 35 percent of respondents say their data loss prevention solutions are very effective in preventing data loss incidents caused by employees. Only 39 percent say these solutions are very effective in preventing data loss incidents caused by malicious insiders.

On a scale from 1 = not effective to 10 = very effective, 7+ responses presented



Effectiveness of current DLP solutions in preventing data loss incidents caused by malicious insiders

Effectiveness of current DLP solutions in preventing data loss incidents caused by employees

THE LACK OF PREPAREDNESS TO STOP BEC/ SPOOF PHISHING AND SUPPLY CHAIN ATTACKS PUTS PATIENTS AT RISK.

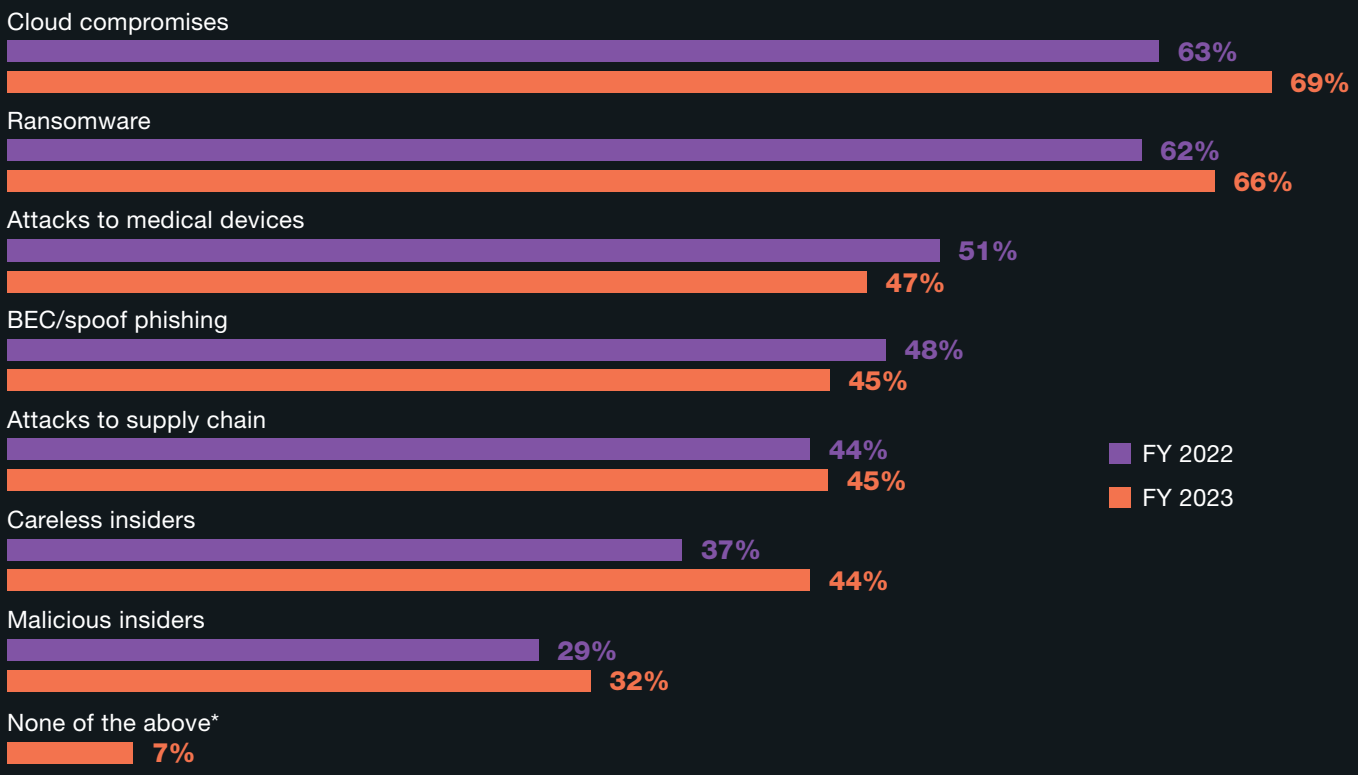
FIGURE 13.

Does your organization include the prevention and response to the following threats as part of its cybersecurity strategy?

According to Figure 13, most organizations focus on steps to prevent and respond to cloud compromises (69 percent of respondents) and ransomware attacks (66 percent).

While BEC/spoof phishing is considered a top cybersecurity threat to healthcare organizations only 45 percent of respondents say their organizations include prevention and response practices to such an attack as part of their cybersecurity strategy. Forty-five percent say they have documented the steps which prevent and respond to attacks to the supply chain. Only 32 percent say they are improving their ability to respond to attacks caused by malicious insiders, which is the primary cause of data loss and infiltration incidents.

More than one response permitted



*Not a response in FY 2022

FIGURE 14.

What challenges keep your organization's cybersecurity posture from being fully effective?

As the sophistication and frequency of cyberattacks increase, in-house expertise is more important than ever. However, as shown in Figure 14, 58 percent of respondents say their organizations lack in-house expertise (an increase from 53 percent in last year's research) and 50 percent say insufficient staff is a challenge. Lack of budget is also a factor (47 percent).

Three responses permitted

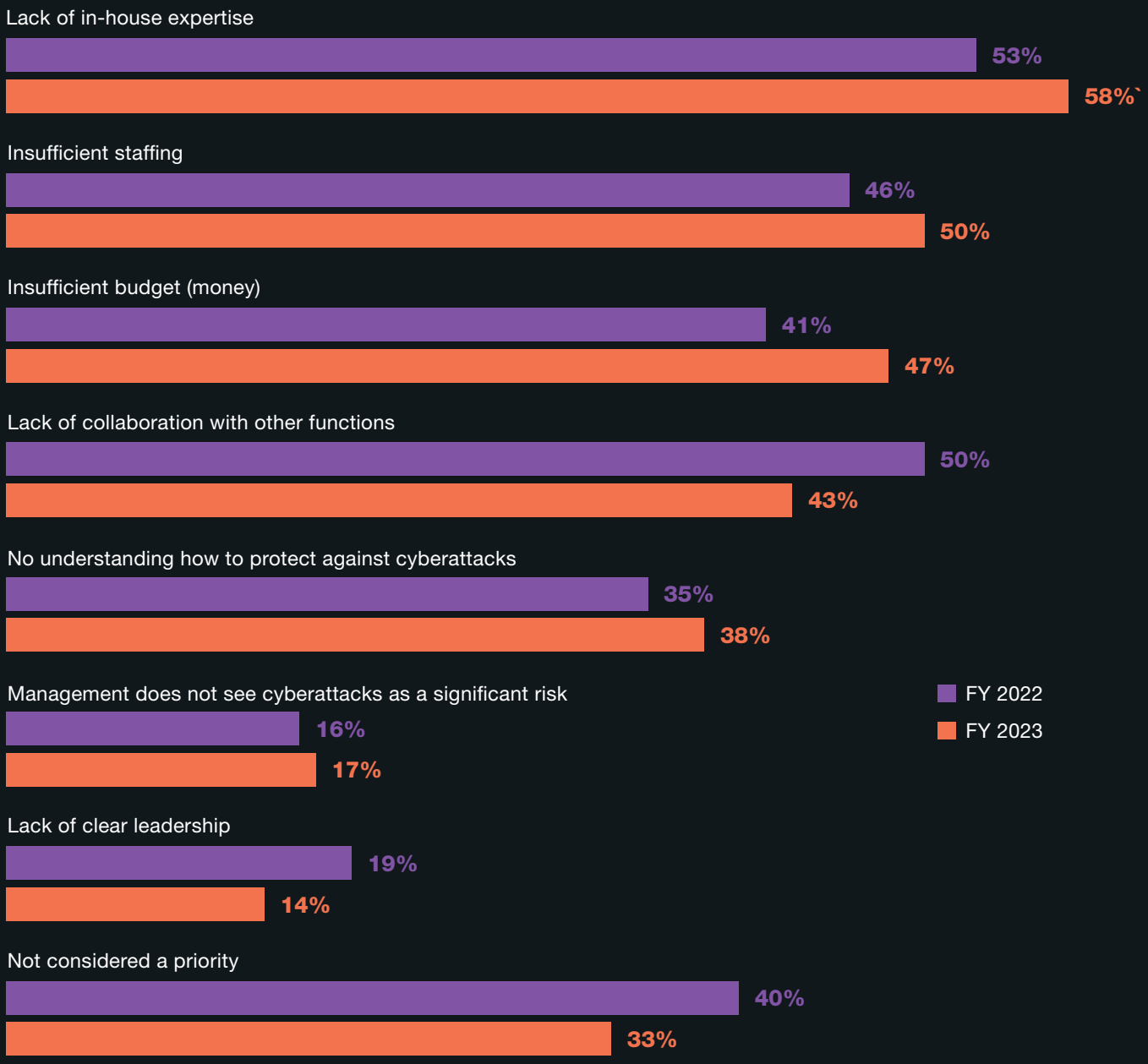


FIGURE 15.

Steps taken to reduce the risk of employees' lack of awareness

Security awareness training programs and employee monitoring are the top two steps taken to reduce the insider risk. More organizations (65 percent in 2023 vs. 59 percent in 2022) are taking steps to address the risk of employees' lack of awareness about cybersecurity threats.

As shown in Figure 15, of these respondents, 57 percent vs. 63 percent of respondents in 2022 say their organizations conduct a regular training and awareness program. Fifty-four percent vs. 59 percent in 2022 say their organizations monitor the actions of employees.

More than one response permitted

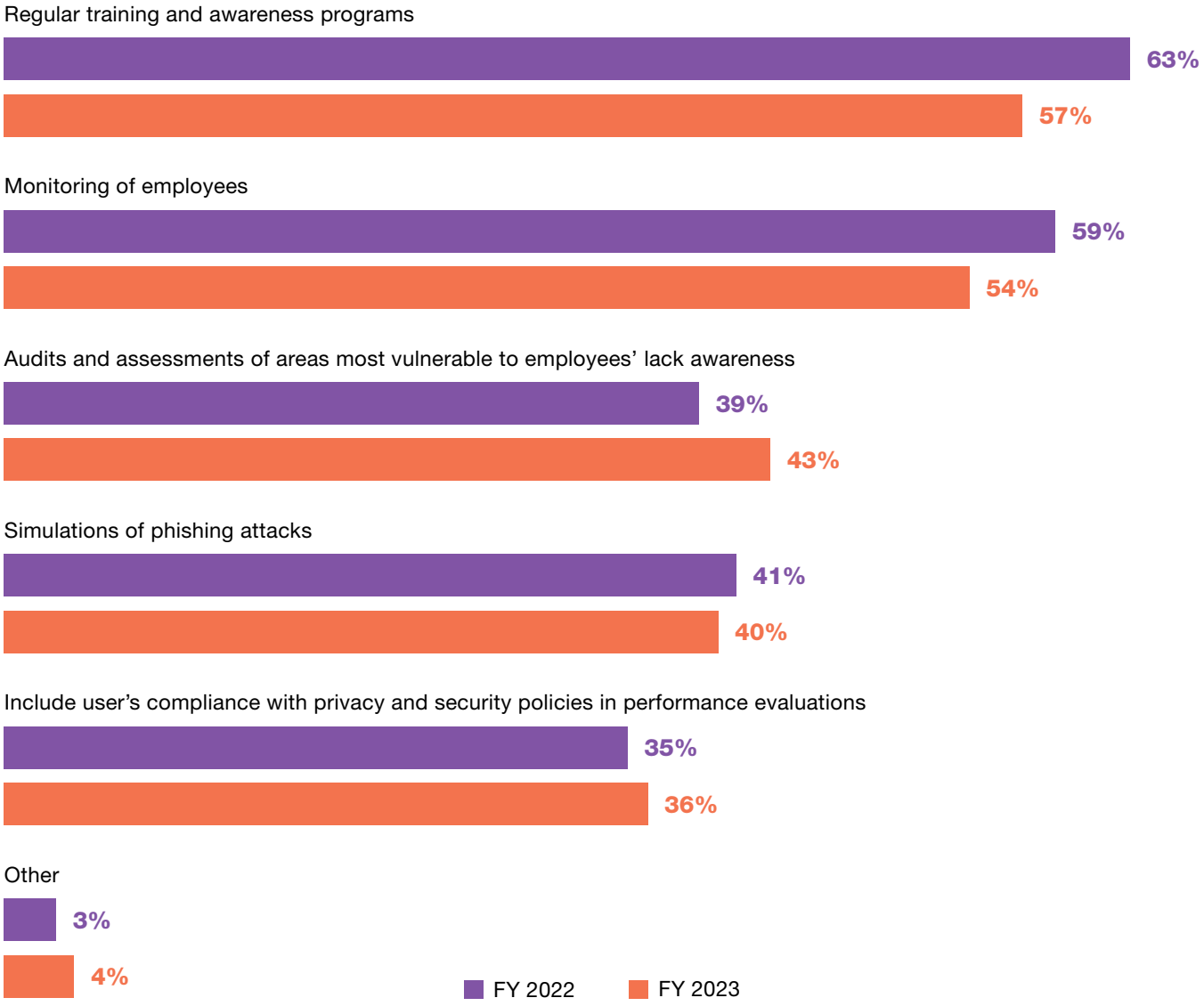


FIGURE 16.

Technologies used to reduce phishing and email-based attacks

The use of identity and access management to reduce phishing and email-based attacks increased significantly from 56 percent to 65 percent of respondents. As shown in Figure 16, multi-factor authentication continues to be a primary solution to reducing phishing and email-based attacks (58 percent). Domain-based message authentication increased from 38 percent to 43 percent.

More than one response permitted

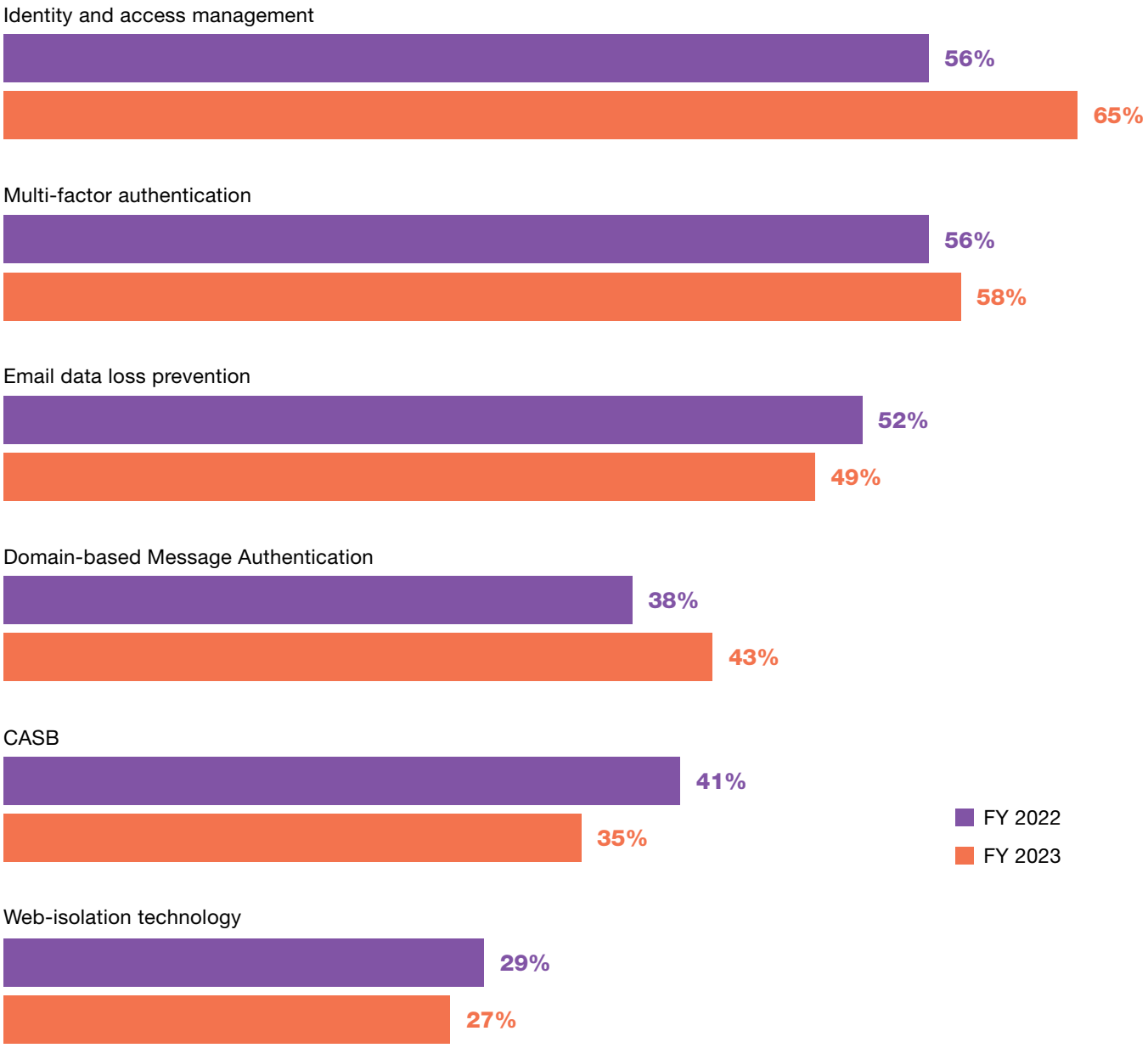
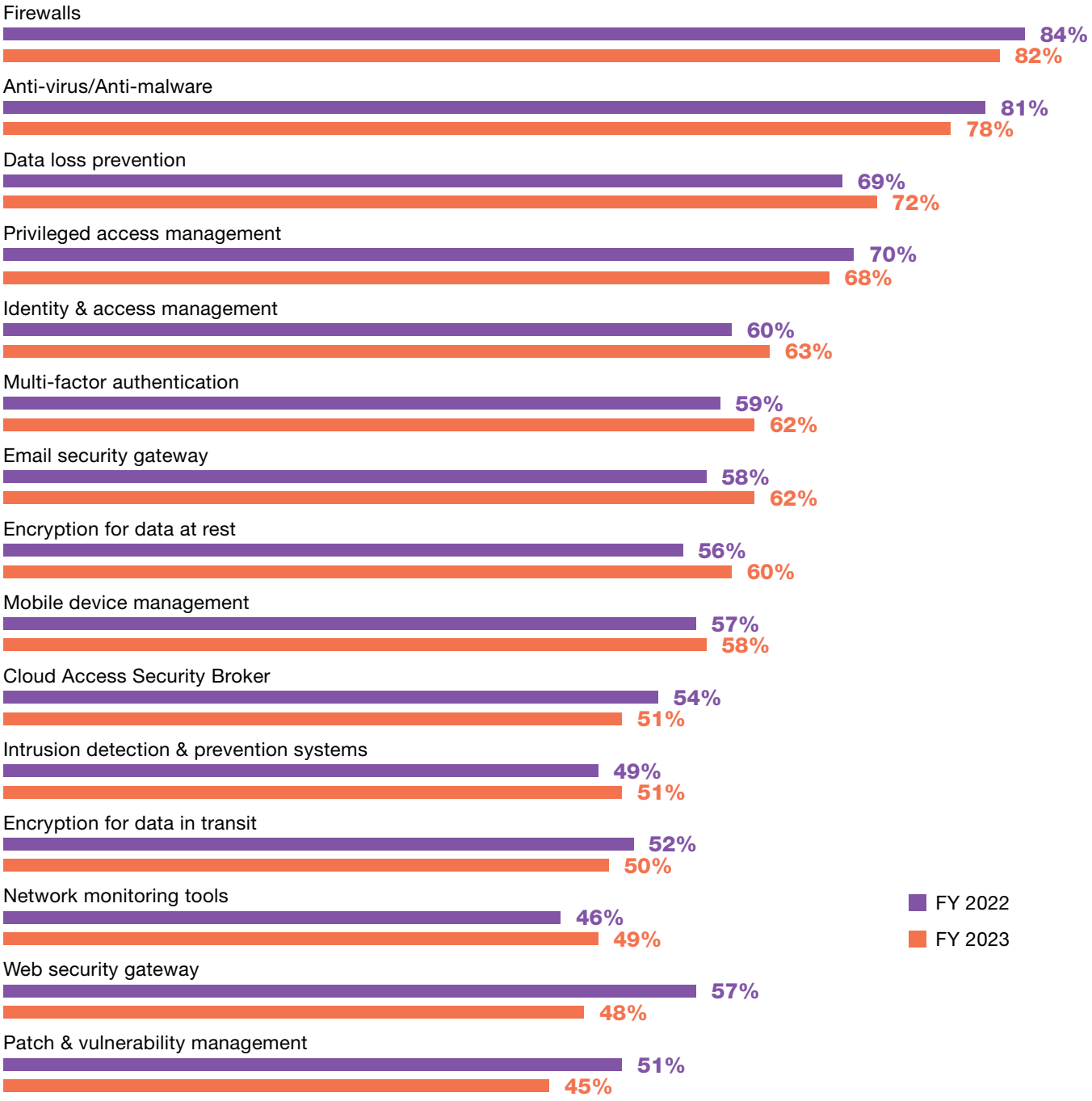


FIGURE 17.

The top technologies fully deployed to stop cyberattacks

The top technologies that organizations have fully implemented are shown in Figure 17. Since 2022, technologies fully deployed to stop cyberattacks have not changed significantly. As part of their cybersecurity strategy, the technologies most fully deployed are firewalls (82 percent of respondents), anti-virus/anti-malware (78 percent) and data loss prevention (72 percent). The use of web security gateways and patch & vulnerability management declined to 48 percent and 45 percent, respectively.

More than one response permitted



METHODOLOGY

OUR FINAL SAMPLE CONSISTED OF 653 SURVEYS OR A 3.8 PERCENT RESPONSE RATE

A sampling frame of 17,085 IT and IT security practitioners in healthcare organizations who are responsible for participating in cybersecurity strategies, including setting IT cybersecurity priorities, managing budgets and selecting vendors and contractors, were selected as participants to this survey. Table 1 shows 715 total returns. Screening and reliability checks required the removal of 62 surveys. Our final sample consisted of 653 surveys or a 3.8 percent response rate.

TABLE 1.

SAMPLE RESPONSE	FREQUENCY	PERCENTAGE
Sampling frame	17,085	100%
Total returns	715	4.2%
Rejected or screened surveys	62	0.4%
Final sample	653	3.8%

FIGURE 18.

Type of organization

Figure 18 reports the respondent's type of organizations. Twenty percent of respondents are from organizations that are private healthcare providers. This is followed by public healthcare provider (19 percent of respondents), healthcare insurer (18 percent of respondents), payer (14 percent) and healthcare insurance (11 percent).

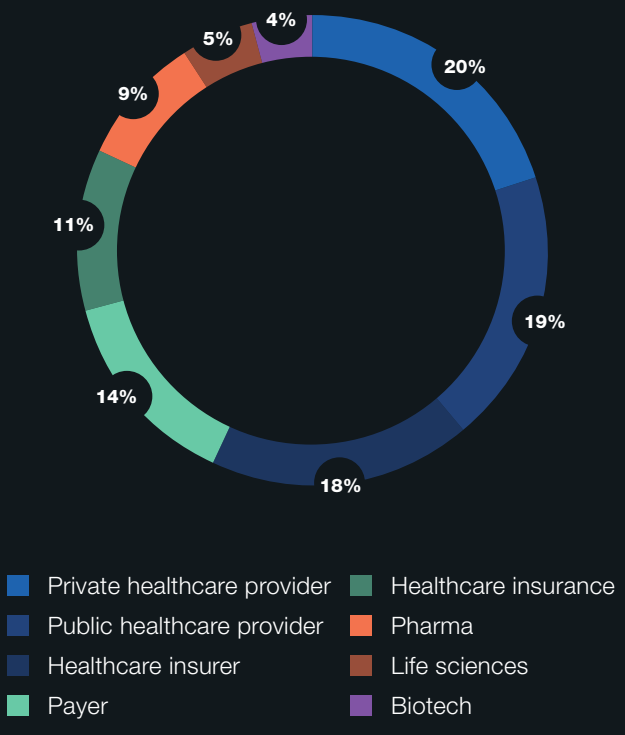


FIGURE 19.

Current position within the organization

Figure 19 reports the respondent's organizational level within participating organizations. By design, more than half (77 percent) of respondents are at or above the supervisory levels. The largest category is manager (29 percent).

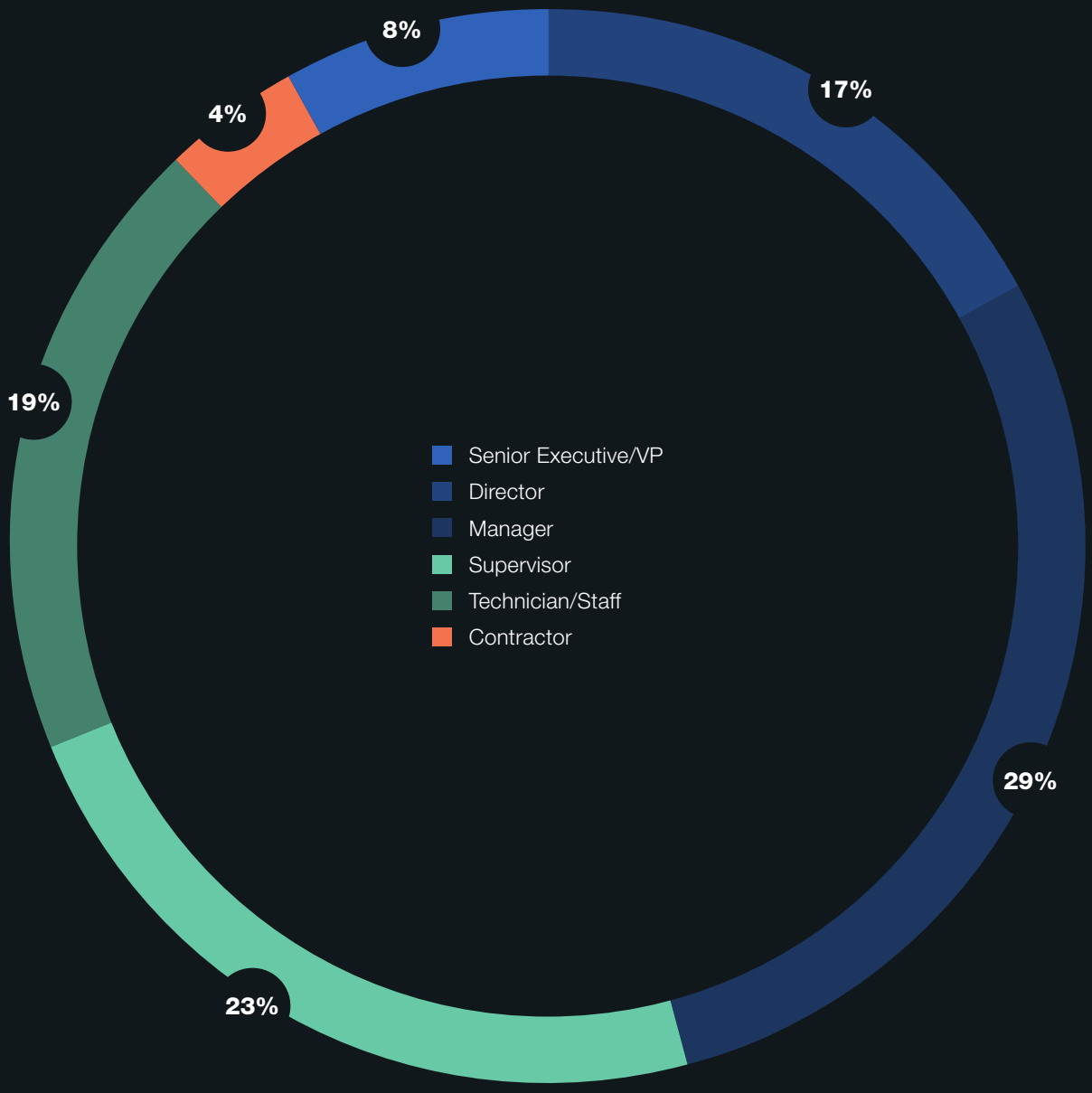


FIGURE 20.

Direct reporting channel

As shown in Figure 20, 20 percent of respondents report to the chief information security officer, 19 percent report to the chief information officer, 11 percent report to cloud administration, 9 percent report to the CEO/executive committee and 9 percent report to data center management.

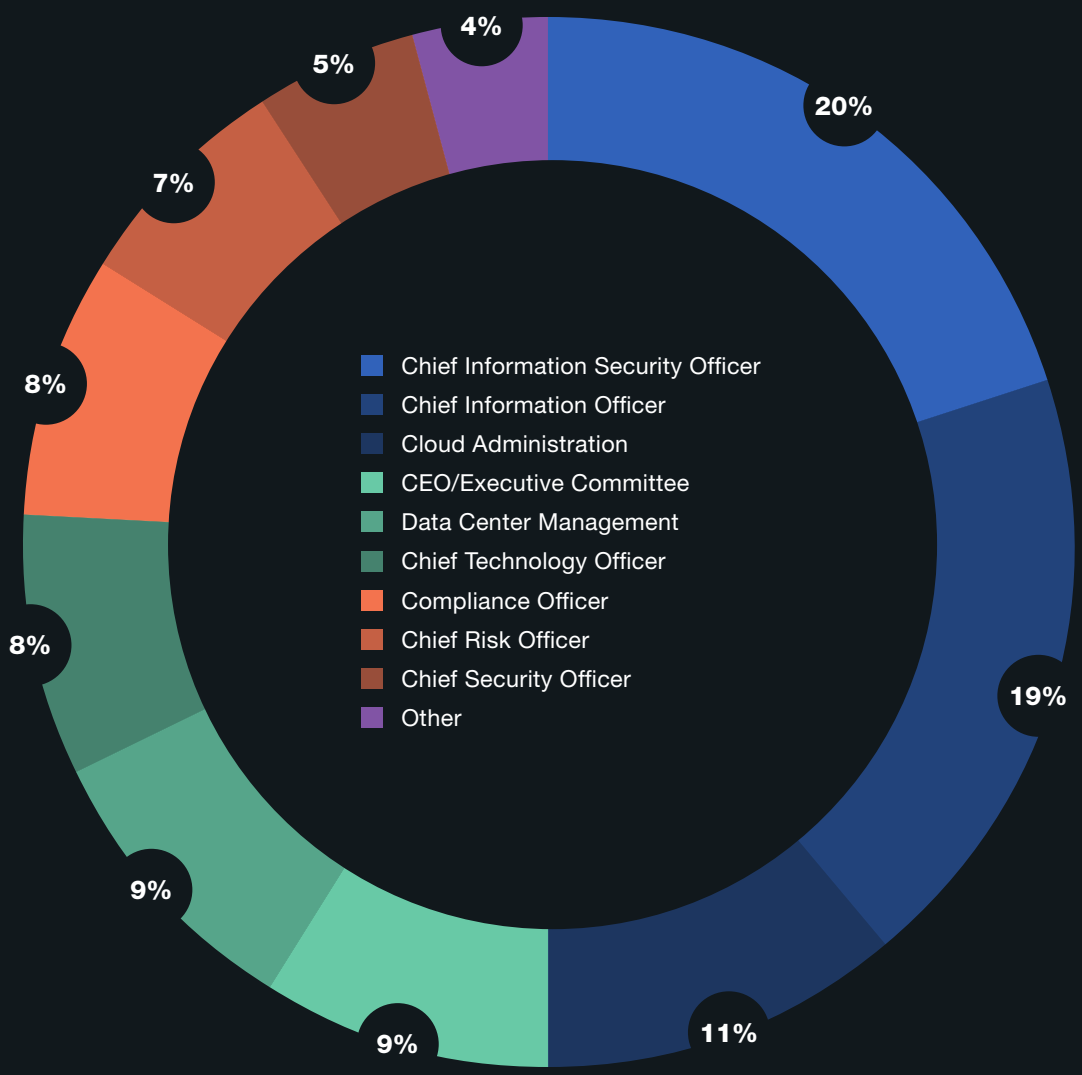
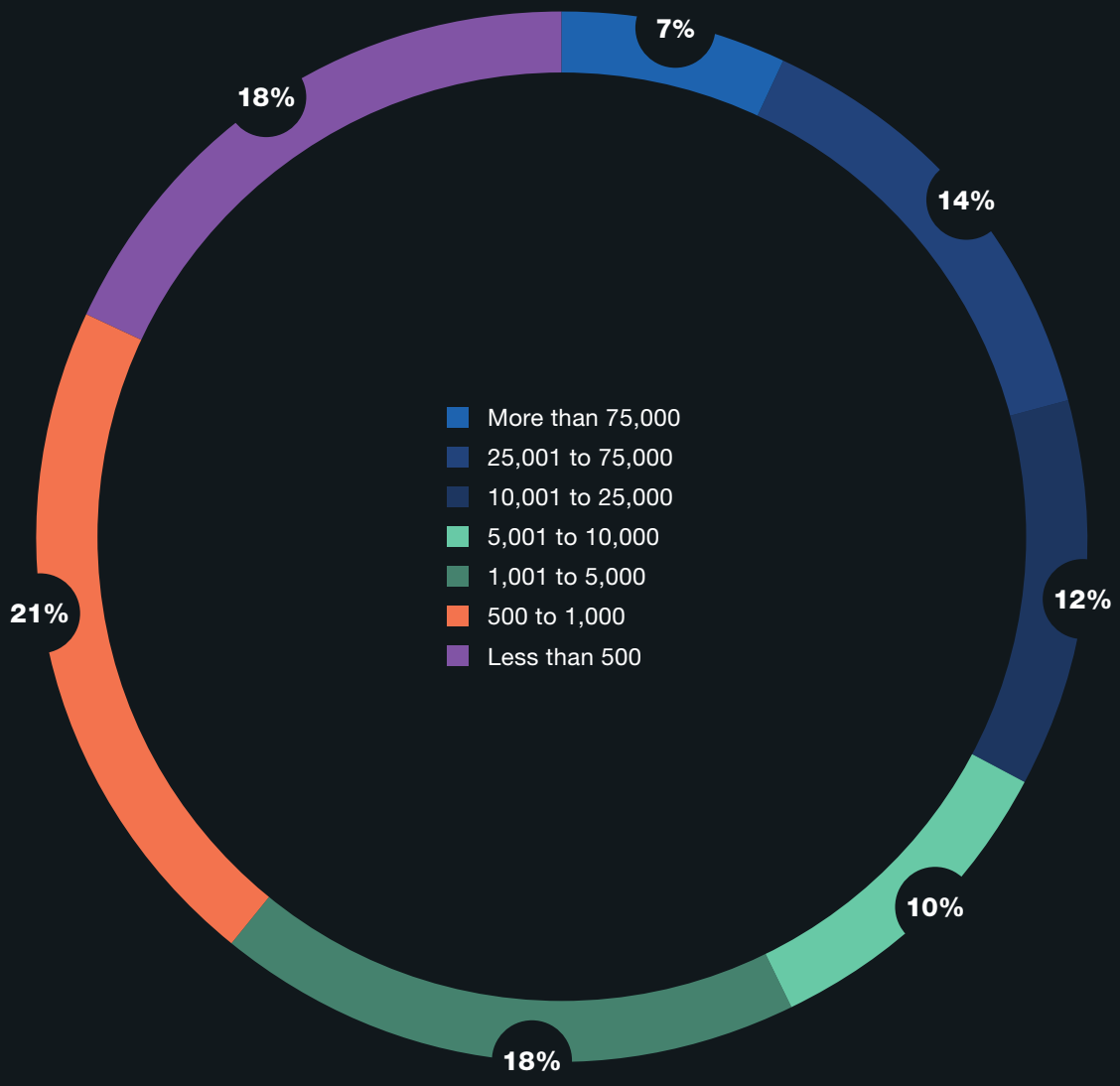


FIGURE 21.

Full-time headcount

As shown in Figure 21, 61 percent of respondents are from organizations with a headcount of more than 1,000 employees.



CAVEATS TO THIS STUDY

THERE ARE INHERENT LIMITATIONS TO SURVEY RESEARCH THAT NEED TO BE CAREFULLY CONSIDERED BEFORE DRAWING INFERENCES FROM FINDINGS.

The following items are specific limitations that are germane to most web-based surveys.

Non-response bias

The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias

The accuracy is based on contact information and the degree to which the list is representative of IT and IT security professionals in healthcare organizations. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-reported results

The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

APPENDIX WITH THE DETAILED AUDITED FINDINGS

THE FOLLOWING TABLES PROVIDE THE FREQUENCY OR PERCENTAGE FREQUENCY OF RESPONSES TO ALL SURVEY QUESTIONS CONTAINED IN THIS REPORT.

All survey responses were captured in March 2023.

SURVEY RESPONSE	FY2023	FY2022
Total sampling frame	17,085	16,451
Total returns	715	698
Rejected returns	62	57
Total sample	653	641
Response rate	3.8%	3.9%

S1	WHICH OF THE FOLLOWING BEST DESCRIBES YOUR ROLE IN IT OR IT SECURITY WITHIN YOUR ORGANIZATION? (Check all that apply)	FY2023	FY2022
	Setting IT cybersecurity priorities	51%	46%
	Managing IT security budgets	45%	42%
	Selecting vendors and contractors	49%	47%
	Participating in IT cybersecurity strategies	51%	51%
	Evaluating and measuring effectiveness of cybersecurity strategies	36%	34%
	Managing cybersecurity risk	34%	36%
	Overseeing governance and compliance	27%	29%
	None of the above [Stop]	0%	0%

PART 1. CYBERSECURITY THREATS TO HEALTHCARE ORGANIZATIONS

Q1	**WHAT CYBERSECURITY THREATS IS YOUR ORGANIZATION MOST CONCERNED ABOUT?** (Please select the top six)	FY2023	FY2022
	BEC/spoof phishing	62%	46%
	Cloud compromises	63%	57%
	Employee negligence or error	52%	58%
	Employee-owned mobile devices or BYOD	61%	34%
	Insecure medical devices	53%	64%
	Insecure mobile apps (eHealth)	51%	59%
	Malicious insiders	45%	37%
	Nation state attacks	19%	17%
	Process failures	31%	36%
	Ransomware	48%	60%
	Supply chain risks	40%	43%
	System failures	35%	36%
	Third-party misuse of patient data	26%	33%
	Use of public cloud services	11%	18%
	Other (please specify)	3%	2%
	Total	600%	600%

Q2	**DOES YOUR ORGANIZATION INCLUDE THE PREVENTION AND RESPONSE TO THE FOLLOWING THREATS AS PART OF ITS CYBERSECURITY STRATEGY?** (Please check all that apply)	FY2023	FY2022
	Attacks to medical devices	47%	51%
	Attacks to the supply chain	45%	44%
	BEC/spoof phishing	45%	48%
	Cloud compromises	69%	63%
	Malicious insiders	32%	29%
	Careless insiders	44%	37%
	Ransomware	66%	62%
	None of the above	7%	
	Total	355%	334%

Q3	WHAT CHALLENGES KEEP YOUR ORGANIZATION'S CYBERSECURITY POSTURE FROM BEING FULLY EFFECTIVE? (Please select the top three challenges)	FY2023	FY2022
	Insufficient budget (money)	47%	41%
	Insufficient staffing	50%	46%
	Lack of in-house expertise	58%	53%
	Lack of clear leadership	14%	19%
	No understanding how to protect against cyberattacks	38%	35%
	Management does not see cyberattacks as a significant risk	17%	16%
	Lack of collaboration with other functions	43%	50%
	Not considered a priority	33%	40%
	Total	300%	300%
	Extrapolated value	6.8	6.9

Q4	USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO BEC/SPOOFING PHISHING (From 1 = not vulnerable to 10 = highly vulnerable)	FY2023	FY2022
	1 or 2	8%	11%
	3 or 4	16%	13%
	5 or 6	15%	12%
	7 or 8	25%	24%
	9 or 10	36%	40%
	Total	100%	100%
	Extrapolated value	6.8	6.9

Q5	USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO SUPPLY CHAIN ATTACKS (From 1 = not vulnerable to 10 = highly vulnerable)	FY2023	FY2022
	1 or 2	2%	5%
	3 or 4	11%	8%
	5 or 6	24%	16%
	7 or 8	23%	23%
	9 or 10	40%	48%
	Total	100%	100%
	Extrapolated value	7.3	7.5

Q6	USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO RANSOMWARE ATTACKS (From 1 = not vulnerable to 10 = highly vulnerable)	FY2023	FY2022
	1 or 2	5%	6%
	3 or 4	10%	9%
	5 or 6	21%	13%
	7 or 8	26%	25%
	9 or 10	38%	47%
	Total	100%	100%
	Extrapolated value	7.1	7.5

Q7	USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO CLOUD COMPROMISES (From 1 = not vulnerable to 10 = highly vulnerable)	FY2023	FY2022
	1 or 2	5%	0%
	3 or 4	6%	9%
	5 or 6	15%	16%
	7 or 8	40%	30%
	9 or 10	34%	45%
	Total	100%	100%
	Extrapolated value	7.3	7.7

Q8	DID YOUR ORGANIZATION EVER EXPERIENCE A RANSOMWARE ATTACK?	FY2023	FY2022
	Yes	54%	41%
	No (please skip to Q16a)	44%	52%
	Unsure (please skip to Q16a)	2%	7%
	Total	100%	100%

Q9	HOW MANY RANSOMWARE INCIDENTS DID YOUR ORGANIZATION EXPERIENCE OVER THE PAST TWO YEARS?	FY2023	FY2022
	One	43%	53%
	Two to five	34%	33%
	Six to 10	16%	9%
	More than 10	7%	5%
	Total	100%	100%
	Extrapolated value	3.7	3.0

Q10A	DID YOUR ORGANIZATION PAY THE RANSOM?	FY2023	FY2022
	Yes	40%	51%
	No	60%	49%
	Total	100%	100%

Q10B	IF YES, HOW MUCH WAS THE RANSOM? (If your organization has had more than one ransomware attack, please select the costliest ransom paid)	FY2023	FY2022
	Less than $10,000	0%	2%
	$10,000 to $25,000	13%	9%
	$25,001 to $50,000	9%	7%
	$50,001 to $75,000	14%	10%
	$75,001 to $100,000	18%	17%
	$100,001 to $250,000	11%	19%
	$250,001 to $500,000	12%	18%
	$500,001 to $1,00,000	9%	8%
	$1,00,001 to $5,000,000	7%	5%
	$5,00,001 to $10,000,000	4%	3%
	More than $10,000,000	3%	2%
	Total	100%	100%
	Extrapolated value	$995,450	$771,905

Q11A	DID THE RANSOMWARE ATTACK RESULT IN A DISRUPTION IN PATIENT CARE?	FY2023	FY2022
	Yes	68%	67%
	No	26%	30%
	Unsure	6%	3%
	Total	100%	100%

Q11B	IF YES, WHAT IMPACT DID THE RANSOMWARE ATTACK HAVE ON PATIENT CARE?	FY2023	FY2022
	An increase in mortality rate	28%	24%
	Delays in procedures and tests have resulted in poor outcomes	59%	64%
	Increase in complications from medical procedures	44%	48%
	Increase in patients transferred or diverted to other facilities	46%	50%
	Longer length of stay	48%	59%
	Other (please specify)	3%	3%
	Total	228%	248%

Q12A	DID YOUR ORGANIZATION EVER EXPERIENCE A BEC/SPOOFING PHISHING ATTACK?	FY2023	FY2022
	Yes	54%	51%
	No (please skip to Q14a)	41%	40%
	Unsure (please skip to Q14a)	5%	9%
	Total	100%	100%

Q12B	IF YES, HOW MANY BEC/SPOOFING ATTACKS DID YOUR ORGANIZATION EXPERIENCE OVER THE PAST TWO YEARS?	FY2023	FY2022
	One	40%	49%
	Two to five	24%	31%
	Six to 10	19%	12%
	More than 10	17%	8%
	Total	100%	100%
	Extrapolated value	4.8	3.5

Q13A	DID THE BEC/SPOOFING ATTACK RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?	FY2023	FY2022
	Yes	69%	67%
	No	26%	30%
	Unsure	5%	3%
	Total	100%	100%

Q13B	IF YES, WHAT IMPACT DID THE BEC/SPOOFING ATTACK HAVE ON PATIENT CARE? (Please select all that apply)	FY2023	FY2022
	An increase in mortality rate	12%	21%
	Delays in procedures and tests have resulted in poor outcomes	71%	60%
	Increase in complications from medical procedures	56%	51%
	Increase in patients transferred or diverted to other facilities	46%	45%
	Longer length of stay	55%	48%
	Other (please specify)	4%	2%
	Total	244%	227%

Q14A	DID YOUR ORGANIZATION EVER EXPERIENCE ATTACKS AGAINST ITS SUPPLY CHAIN?	FY2023	FY2022
	Yes	64%	50%
	No (please skip to Q16a)	30%	44%
	Unsure (please skip to Q16a)	6%	6%
	Total	100%	100%

Q14B	IF YES, HOW MANY SUPPLY CHAIN ATTACKS DID YOUR ORGANIZATION EXPERIENCE OVER THE PAST TWO YEARS?	FY2023	FY2022
	One	36%	44%
	Two to five	33%	29%
	Six to 10	21%	19%
	More than 10	10%	8%
	Total	100%	100%
	Extrapolated value	4.2	3.9

Q15A	DID THE SUPPLY CHAIN ATTACKS RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?	FY2023	FY2022
	Yes	77%	70%
	No	18%	24%
	Unsure	5%	6%
	Total	100%	100%

Q15B	IF YES, WHAT IMPACT DID THE SUPPLY CHAIN ATTACKS HAVE ON PATIENT CARE? (Please select all that apply)	FY2023	FY2022
	An increase in mortality rate	21%	23%
	Delays in procedures and tests have resulted in poor outcomes	50%	54%
	Increase in complications from medical procedures	45%	48%
	Increase in patients transferred or diverted to other facilities	39%	40%
	Longer length of stay	48%	51%
	Other (please specify)	4%	3%
	Total	207%	219%

PART 2. PROTECTING THE CLOUD

Q16A	DID YOUR ORGANIZATION EVER EXPERIENCE A SUCCESSFUL CLOUD/ACCOUNT COMPROMISE?	FY2023	FY2022
	Yes	63%	54%
	No (Please skip to Q18)	33%	41%
	Unsure (Please skip to Q18)	4%	5%
	Total	100%	100%

Q16B	HOW MANY TIMES HAVE ATTACKERS COMPROMISED CLOUD-BASED USER ACCOUNTS WITHIN YOUR ORGANIZATION OVER THE PAST TWO YEARS?	FY2023	FY2022
	Once	0%	5%
	2 to 5	12%	9%
	6 to 10	14%	6%
	11 to 15	10%	9%
	16 to 20	21%	22%
	21 to 25	19%	22%
	26 to 50	16%	18%
	More than 50	8%	9%
	Total	100%	100%
	Extrapolated value	21.4	21.7

Q16C	WHICH CLOUD-BASED USER ACCOUNTS/COLLABORATION TOOLS WERE MOST ATTACKED IN YOUR ORGANIZATION? (Please select all that apply)	FY2023
	Email	49%
	Text messaging	45%
	Zoom/Skype/Videoconferencing	53%
	Teams/Slack/Office collaboration tools	49%
	Project management tools	53%
	OneDrive/DropBox/Document/file-sharing tools	49%
	Application/system-generated email	51%
	Total	349%

Q17A	DID THE CLOUD COMPROMISES RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?	FY2023	FY2022
	Yes	49%	64%
	No	40%	32%
	Unsure	11%	4%
	Total	100%	100%

Q17B	IF YES, WHAT IMPACT DID THE CLOUD COMPROMISES HAVE ON PATIENT CARE? (Please select all that apply)	FY2023	FY2022
	An increase in mortality rate	29%	18%
	Delays in procedures and tests have resulted in poor outcomes	47%	49%
	Increase in complications from medical procedures	53%	51%
	Increase in patients transferred or diverted to other facilities	37%	37%
	Longer length of stay	48%	50%
	Other (please specify)	3%	2%
	Total	217%	207%

Q18	HOW DOES YOUR ORGANIZATION PROTECT CONFIDENTIAL OR SENSITIVE INFORMATION IN THE CLOUD? (Please select all that apply)	FY2023	FY2022
	We use private data network connectivity	40%	43%
	We use premium security services provided by the cloud provider	60%	56%
	We use encryption, tokenization or other cryptographic tools to protect data in the cloud	59%	65%
	We use a Cloud Access Security Broker (CASB)	43%	53%
	Don't know	18%	6%
	Other (Please specify)	5%	3%
	Total	225%	226%

Q19	WHAT BEST DESCRIBES YOUR ORGANIZATION'S APPROACH TO USER ACCESS AND IDENTITY MANAGEMENT IN THE CLOUD ENVIRONMENT? (Please select all that apply)	FY2023	FY2022
	Separate identity management interfaces for the cloud and on-premise environments	50%	53%
	Unified identity management interface for both the cloud and on-premise environments	43%	48%
	Deployment of single sign-on (SSO)	30%	37%
	Hybrid combination of the above choices	56%	60%
	Don't know	6%	5%
	Total	185%	198%

PART 3. DATA LOSS PROTECTION SOLUTIONS TO REDUCE THE LOSS OR THEFT OF SENSITIVE HEALTHCARE DATA

Q20	HOW MANY DATA LOSS AND EXFILTRATION INCIDENTS INVOLVING SENSITIVE AND CONFIDENTIAL HEALTHCARE DATA OCCURRED WITHIN YOUR ORGANIZATION OVER THE PAST TWO YEARS?	FY2023
	Once	8%
	2 to 5	5%
	6 to 10	12%
	11 to 15	24%
	16 to 20	10%
	21 to 25	23%
	26 to 50	13%
	More than 50	5%
	Total	100%
	Extrapolated value	19

Q21	HOW WOULD YOU CHARACTERIZE THE DATA LOSS OR EXFILTRATION?	FY2023
	Accidental data loss	27%
	Employee negligence because of not following policies	25%
	Malicious insiders	32%
	Uncertain	16%
	Total	100%

Q22A	DID THE DATA LOSS OR EXFILTRATION RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?	FY2023
	Yes	43%
	No	51%
	Unsure	6%
	Total	100%

Q22B	IF YES, WHAT IMPACT DID THE DATA LOSS PROTECTION OR EXFILTRATION INCIDENT HAVE ON PATIENT CARE? (Please select all that apply)	FY2023
	An increase in mortality rate	46%
	Delays in procedures and tests have resulted in poor outcomes	34%
	Increase in complications from medical procedures	38%
	Increase in patients transferred or diverted to other facilities	36%
	Longer length of stay	24%
	Other (please specify)	6%
	Total	184%

Q23	WHAT SECURITY METHODS AND TECHNOLOGIES DOES YOUR ORGANIZATION USE TO REDUCE THE CONSEQUENCES OF A DATA LOSS OR EXFILTRATION INCIDENT? (Please select all that apply)	FY2023
	Rules-based DLP solution	43%
	IT/IT security team triages incidents	35%
	Policy fine tuning to prevent data loss	31%
	Manual policy orchestration	46%
	Alerts from SIEM to gain visibility	34%
	Managed Security Service Provider (MSSP)	45%
	Enterprise data loss prevention platform covering multiple channels for email, web, network, endpoint and cloud	51%
	Cloud access security broker (CASB)	67%
	User and entity behavior analytics (UEBA)	54%
	Secure email gateway (SEG)	48%
	Identity theft detection and response (IDTR)	34%
	Other (please specify)	5%
	Total	493%

Q24	HOW EFFECTIVE ARE YOUR CURRENT DATA LOSS PREVENTION SOLUTIONS IN PREVENTING DATA LOSS INCIDENTS CAUSED BY EMPLOYEES? (From 1 = not effective to 10 = very effective)	FY2023
	1 or 2	18%
	3 or 4	33%
	5 or 6	14%
	7 or 8	16%
	9 or 10	19%
	Total	100%
	Extrapolated value	5.2

Q25	HOW EFFECTIVE ARE YOUR CURRENT DATA LOSS PREVENTION SOLUTIONS IN PREVENTING DATA LOSS INCIDENTS CAUSED BY MALICIOUS INSIDERS (From 1 = not effective to 10 = very effective)	FY2023
	1 or 2	15%
	3 or 4	20%
	5 or 6	26%
	7 or 8	25%
	9 or 10	14%
	Total	100%
	Extrapolated value	5.56

Q26	HOW CONCERNED IS YOUR ORGANIZATION THAT ITS EMPLOYEES DO NOT UNDERSTAND THE SENSITIVITY AND CONFIDENTIALITY OF DATA THAT THEY SHARE THROUGH EMAIL? (From 1 = not concerned to 10 = very concerned)	FY2023
	1 or 2	15%
	3 or 4	17%
	5 or 6	21%
	7 or 8	25%
	9 or 10	22%
	Total	100%
	Extrapolated value	5.94

PART 4. STEPS AND SOLUTIONS TO REDUCING CYBERSECURITY THREATS

Q27A	DOES YOUR ORGANIZATION TAKE STEPS TO ADDRESS THE RISK OF EMPLOYEES' LACK OF AWARENESS ABOUT CYBERSECURITY THREATS, ESPECIALLY BEC/SPOOFING PHISHING?	FY2023	FY2022
	Yes	65%	59%
	No	30%	35%
	Unsure	5%	6%
	Total	100%	100%

Q27B	IF YES, WHAT STEPS DOES IT TAKE? (Please select all that apply)	FY2023	FY2022
	Regular training and awareness programs	57%	63%
	Simulations of phishing attacks	40%	41%
	Monitoring of employees	54%	59%
	Audits and assessments of areas most vulnerable to employees' lack of awareness	43%	39%
	Include user's compliance with privacy and security policies in performance evaluations	36%	35%
	Other (please specify)	4%	3%
	Total	234%	240%

Q28	WHAT TECHNOLOGIES DOES YOUR ORGANIZATION USE TO REDUCE PHISHING AND EMAIL-BASED ATTACKS? (Please select all that apply)	FY2023	FY2022
	Domain-based Message Authentication (DMARC)	43%	38%
	Web-isolation technology	27%	29%
	Multi-factor authentication	58%	56%
	Email data loss prevention	49%	52%
	CASB	35%	41%
	Identity and access management (IAM)	65%	56%
	Total	277%	272%

Q29	TO WHAT EXTENT HAS YOUR ORGANIZATION FULLY IMPLEMENTED THE FOLLOWING SECURITY TECHNOLOGIES? (Please select all that apply)	FY2023	FY2022
	Anti-virus/anti-malware	78%	81%
	Firewalls	82%	84%
	Email security gateway	62%	58%
	Encryption for data in transit	50%	52%
	Network monitoring tools	49%	46%
	Web security gateway	48%	57%
	Intrusion detection & prevention systems (IDPS)	51%	49%
	Encryption for data at rest	60%	56%
	Patch & vulnerability management	45%	51%
	Multi-factor authentication	62%	59%
	Identity & access management	63%	60%
	Privileged access management	68%	70%
	Data loss prevention	72%	69%
	Mobile device management (MDM)	58%	57%
	Cloud Access Security Broker (CASB)	51%	54%
	Total	899%	903%

PART 5. CYBERATTACK EXPERIENCE

Q30	HOW MANY CYBERATTACKS HAS YOUR ORGANIZATION EXPERIENCED OVER THE PAST 12 MONTHS?	FY2023	FY2022
	None (please skip to Part 6)	12%	11%
	1 to 5	13%	12%
	6 to 10	21%	15%
	11 to 25	11%	13%
	26 to 50	9%	11%
	51 to 100	18%	23%
	More than 100	16%	15%
	Total	100%	100%
	Extrapolated value	40	43

*Please note that the cost estimate should include all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunities.

Q31	APPROXIMATELY, HOW MUCH WAS THE TOTAL COST FROM THE ONE MOST SIGNIFICANT CYBERSECURITY ATTACK?	FY2023	FY2022
	Less than $10,000	0%	0%
	$10,001 to $50,000	0%	0%
	50,001 to $100,000	7%	6%
	100,001 to $250,000	13%	12%
	250,001 to $500,000	18%	18%
	500,001 to $1,000,000	14%	16%
	1,000,001 to $5,000,000	19%	21%
	5,000,001 to $10,000,000	11%	13%
	10,000,001 to $25,000,000	15%	12%
	More than $25,000,000	3%	2%
	Total	100%	100%
	Extrapolated value	$4,991,500	$4,429,000

Q32	**TO UNDERSTAND THE RELATIONSHIP OF EACH OF THE FIVE CATEGORIES TO THE TOTAL COST OF A CYBER SECURITY COMPROMISE** (please allocate points to each category for a total of 100 points)	FY2023	FY 2022
	Remediation & technical support activities, including forensic investigations, incident response activities, help desk and delivery of services to patients	15.00	16.00
	Users' idle time and lost productivity because of downtime or system performance delays	23.00	25.00
	Disruption to normal healthcare operations because of system availability problems	26.00	23.00
	Damage or theft of IT assets and infrastructure	15.00	21.00
	Time required to ensure impact on patient care is corrected	21.00	15.00
	Total Points	100.00	100.00

PART 6. SECURITY SPENDING & INVESTMENT

Q33	WHAT IS YOUR ORGANIZATION'S APPROXIMATE ANNUAL BUDGET FOR IT?	FY2023	FY2022
	Less than $1,000,000	2%	0%
	1,000,000 to $5,000,000	3%	2%
	5,000,001 to $10,000,000	8%	6%
	10,000,001 to $25,000,000	11%	10%
	25,000,001 to $50,000,000	25%	17%
	$50,000,001 to $100,000,000	23%	28%
	$100,000,000+	25%	37%
	Cannot estimate	3%	0%
	Total	100%	100%
	Extrapolated value	$59,258,000	$75,200,000

Q34	WHAT PERCENTAGE OF YOUR ORGANIZATION'S IT BUDGET IS DEDICATED TO INFORMATION SECURITY?	FY2023	FY2022
	Less then 5%	5%	3%
	5 to 10%	8%	7%
	11 to 15%	21%	23%
	16 to 20%	37%	35%
	21 to 30%	19%	21%
	More than 30%	10%	11%
	Total	100%	100%
	Extrapolated value	18%	19%

PART 7. YOUR ROLE AND ORGANIZATION

D1	WHAT BEST DESCRIBES YOUR ORGANIZATION?	FY2023	FY2022
	Public healthcare provider	19%	19%
	Private healthcare provider	20%	22%
	Healthcare insurer	18%	13%
	Payer	14%	15%
	Healthcare insurance	11%	9%
	Life sciences	5%	8%
	Biotech	4%	5%
	Pharma	9%	9%
	Total	100%	100%

D2	WHAT ORGANIZATIONAL LEVEL BEST DESCRIBES YOUR CURRENT POSITION?	FY2023	FY2022
	Senior Executive/VP	8%	9%
	Director	17%	16%
	Manager	29%	23%
	Supervisor	23%	14%
	Technician/Staff	19%	33%
	Contractor	4%	5%
	Other (please specify)	0%	0%
	Total	100%	100%

D3	CHECK THE PRIMARY PERSON YOU OR YOUR IT SECURITY LEADER REPORTS TO WITHIN THE ORGANIZATION.	FY2023	FY2022
	CEO/Executive Committee	9%	8%
	Chief Information Officer	19%	21%
	Chief Information Security Officer	20%	19%
	Chief Risk Officer	7%	6%
	Chief Security Officer	5%	4%
	Chief Technology Officer	8%	7%
	Compliance Officer	8%	9%
	Data Center Management	9%	10%
	Cloud Administration	11%	12%
	Other (please specify)	4%	4%
	Total	100%	100%

D4	WHAT IS THE HEADCOUNT OF YOUR ORGANIZATION?	FY2023	FY2022
	Less than 500	18%	16%
	500 to 1,000	21%	25%
	1,001 to 5,000	18%	19%
	5,001 to 10,000	10%	9%
	10,001 to 25,000	12%	13%
	25,001 to 75,000	14%	12%
	More than 75,000	7%	6%
	Total	100%	100%

For more information about this report, please contact Ponemon Institute by sending an email to research@ponemon.org or calling us at 1.800.887.3118.

Ponemon INSTITUTE

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

proofpoint.

About Proofpoint, Inc.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 85 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.