THE 2024 STUDY ON CYBER INSECURITY IN HEALTHCARE: THE COST AND IMPACT ON PATIENT SAFETY AND CARE

Independently conducted by:

Ponemon INSTITUTE

Sponsored by:

proofpoint.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

AN EFFECTIVE CYBERSECURITY APPROACH CENTERED AROUND STOPPING HUMAN-TARGETED ATTACKS IS CRUCIAL FOR HEALTHCARE INSTITUTIONS, NOT JUST TO PROTECT CONFIDENTIAL PATIENT DATA BUT ALSO TO ENSURE THE HIGHEST QUALITY OF MEDICAL CARE.

This *third annual* report was conducted to determine if the healthcare industry is making progress in reducing human-centric cybersecurity risks and disruptions to patient care.

With sponsorship from Proofpoint, Ponemon Institute surveyed 648 IT and IT security practitioners in 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, 92 percent of organizations surveyed experienced at least one cyberattack in the past 12 months, an increase from 88 percent in 2023. 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 $4,740,000, a 5 percent decrease 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 $1.47 million, disruption to normal healthcare operations because of system availability problems continues to be the most expensive consequence from the cyberattack, a 13 percent increase from an average $1.3 million in 2023. Users' idle time and lost productivity because of downtime or system performance delays decreased from $1.1 million in 2023 to $995,484 in 2024. The cost of the time required to ensure the impact on patient care is corrected also decreased from an average of $1 million average in 2023 to $853,272 in 2024.

92%

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

$4.7M

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

$1.47M

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/ACCOUNT COMPROMISE

The most frequent attacks in healthcare are against the cloud, making it the top cybersecurity threat for the third consecutive year. Sixty-three percent of respondents say their organizations are vulnerable or highly vulnerable to a cloud/account compromise. Sixty-nine percent say their organizations have experienced a cloud/account compromise. In the past two years, organizations in this group experienced an average of 20 cloud compromises.

SUPPLY CHAIN ATTACKS

Organizations are very or highly vulnerable to a supply chain attack, according to 60 percent of respondents. Sixty-eight percent say their organizations experienced an average of four attacks against its supply chain in the past two years.

RANSOMWARE

Ransomware remains an ever-present threat to healthcare organizations, even though concerns about it have declined. Fifty-four percent of respondents believe their organizations are vulnerable or highly vulnerable to a ransomware attack, a decline from 64 percent. In the past two years, organizations that had ransomware attacks (59 percent of respondents) experienced an average of four such attacks. While fewer organizations paid the ransom (36 percent in 2024 vs. 40 percent in 2023), the ransom paid spiked 10 percent to an average of $1,099,200 compared to $995,450 in the previous year.

BUSINESS EMAIL COMPROMISE (BEC)/SPOOFING/IMPERSONATION

Concerns about BEC/spoofing/impersonation attacks have decreased. Fifty-two percent of respondents say their organizations are vulnerable or highly vulnerable to a BEC/spoofing/impersonation incident, a decrease from 61 percent in 2023. Fifty-seven percent of respondents say their organizations experienced an average of four attacks in the past two years.

Nearly seventy-percent of surveyed healthcare organizations report patient care disruptions from cyberattacks.

As in the previous report, an important part of the research is the connection between cyberattacks and patient safety. Among the organizations that experienced the four types of cyberattacks in the study, an average of 69 percent report disruption to patient care.

Specifically, as shown in Table 1 below, an average of 56 percent report poor patient outcomes due to delays in procedures and tests, an average of 53 percent saw an increase in medical procedure complications and an average of 28 percent say patient mortality rates increased, a 21 percent spike over last year.

TABLE 1.

Five ways that cyberattacks impact patient outcomes

CYBERATTACK	Ransomware	BEC	Supply Chain	Cloud/Account Compromise	**2024 Average**
POOR OUTCOMES: DELAY IN TESTS/PROCEDURES	61%	69%	48%	44%	**56%**
INCREASE COMPLICATIONS FROM MEDICAL PROCEDURES	47%	57%	51%	56%	**53%**
LONGER LENGTH OF STAY	58%	52%	45%	52%	**52%**
INCREASE IN PATIENTS TRANSFERRED OR DIVERTED TO OTHER FACILITIES	52%	50%	38%	36%	**44%**
INCREASE IN MORTALITY RATE	29%	24%	26%	32%	**28%**

The following are additional trends in how cyberattacks have affected patient safety and patient care delivery.

- **Supply chain attacks are most likely to affect patient care.** Sixty-eight percent of respondents say their organizations had an attack against their supply chains. Of this group, 82 percent say it disrupted patient care, an increase from 77 percent in 2023. Patients were primarily impacted by an increase in complications from medical procedures (51 percent) and delays in procedures and tests that resulted in poor outcomes (48 percent).
- **A BEC/spoofing/impersonation attack causes delays in procedures and tests.** Fifty-seven percent of respondents say their organizations experienced a BEC/spoofing/impersonation incident. Of these respondents, 65 percent say a BEC/spoofing/impersonation attack disrupted patient care. Sixty-nine percent say the consequences caused delays in procedures and tests that have resulted in poor outcomes and 57 percent say it increased complications from medical procedures.
- **Ransomware attacks cause delays in patient care.** Fifty-nine percent of respondents say their organizations experienced a ransomware attack. Of this group, 70 percent say ransomware attacks had a negative impact on patient care. Sixty-one percent say patient care was affected by delays in procedures and tests that resulted in poor outcomes and 58 percent say it resulted in longer lengths of stay, which affects organizations' ability to care for patients.
- **Cloud/account compromises are least likely to disrupt patient care.** Sixty-nine percent of respondents say their organizations experienced a cloud/account compromise. In this year's study, 57 percent say the cloud/account compromises resulted in disruption in patient care operations, an increase from 49 percent in 2023. Fifty-six percent of respondents say cloud/account compromises increased complications from medical procedures and 52 percent say it resulted in a longer length of stay.
- **Data loss or exfiltration has had an impact on patient mortality.** Ninety-two percent of organizations had at least two data loss incidents involving sensitive and confidential healthcare data in the past two years. On average, organizations experienced 20 such incidents in the past two years. Fifty-one percent say the data loss or exfiltration resulted in a disruption in patient care. Of these respondents, 50 percent say it increased the mortality rate and 37 percent say it caused delays in procedures and tests that resulted in poor outcomes.

OTHER KEY TRENDS IN CYBER INSECURITY

CARELESS USERS WERE THE TOP CAUSE OF DATA LOSS AND EXFILTRATION

31% say data loss or exfiltration was caused by employees not following policies.

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

52% are very concerned about employee negligence or error.

CLOUD-BASED PRODUCTIVITY TOOLS ARE MOST OFTEN ATTACKED

61%

say text messaging was the most attacked collaboration tool.

59%

say email was the second highest attacked collaboration tool.

TOP 2 CHALLENGES TO HAVING AN EFFECTIVE CYBERSECURITY POSTURE

55%

say they lack in-house expertise.

49%

say they lack clear leadership, up from 14% in 2023.

BUDGETS INCREASED BECAUSE CYBER SAFETY IS PATIENT SAFETY

Concerns about budget decreased from

47% to 40%

$66M

Average annual budget for IT increased, up 12% YoY.

19%

Percentage in IT budget dedicated to information security.

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

More organizations say they are taking steps to address the risk caused by employees.

71% in 2024 VS **65%** in 2023

Of this group:

say they conduct regular training and awareness programs.

say they monitor the actions of employees.

TOP 3 CYBERSECURITY TOOLS TO PROTECT AGAINST EMAIL-BASED ATTACKS

53%

anti-virus/
anti-malware

52%

patch and vulnerability management

49%

multi-factor authentication

CONCERNS ABOUT INSECURE MOBILE APPS ROSE SIGNIFICANTLY

59%

are worried about the security risks created by insecure mobile apps (eHealth), up from 51% in 2023.

TRENDS FOR AI IN HEALTHCARE

54%

say they have embedded AI in cybersecurity and patient care.

57%

say AI is very effective in improving organizations' cybersecurity posture.

USING AI FOR TIME, COST, AND PRODUCTIVITY

55%

say that AI-based security tools will increase productivity for IT security personnel.

48%

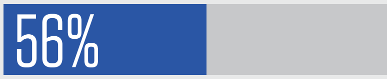
say AI simplifies patient care and administrators' work by performing tasks in less time and cost than humans.

USING AI TO PROTECT AGAINST EMAIL-BASED ATTACKS

36%

use AI and machine learning to understand human behavior.

Of this group:



say understanding human behavior to protect emails is very important.

CHALLENGES TO ADOPTING AI

63% agree safeguarding confidential and sensitive data used in organizations’ AI is difficult or very difficult.

✓ ✓ ✓ ✓ ✓ ✓ ✗ ✗ ✗

32% say there are errors and inaccuracies in data inputs ingested by AI.

✓ ✓ ✓ ✗ ✗ ✗ ✗ ✗ ✗

34% believe there’s a shortage of mature and/or stable AI tools.

✓ ✓ ✓ ✗ ✗ ✗ ✗ ✗ ✗

32% say interoperability issues among AI technologies deter widespread acceptance.

✓ ✓ ✓ ✗ ✗ ✗ ✗ ✗ ✗

KEY FINDINGS

ANALYSIS

In this section, we provide an analysis of the findings in the third annual report. The complete audited findings are presented in the Appendix of this report. Whenever possible, we compare the 2022 and 2023 findings to this year's research. The report is organized according to the following topics:

- Cybersecurity threats in healthcare: cloud/account compromise, ransomware, supply chain and business email compromise (BEC)/spoofing/impersonation
- The impact of cyberattacks on patient care
- The cost of cyber insecurity
- The insider risk to sensitive data and patient safety
- AI and machine learning in healthcare
- Solutions and responses to cyber insecurity

CYBERSECURITY THREATS IN HEALTHCARE: CLOUD/ACCOUNT COMPROMISE, RANSOMWARE, SUPPLY CHAIN AND BUSINESS EMAIL COMPROMISE (BEC)/SPOOFING/IMPERSONATION

FIGURE 1.

HEALTHCARE ORGANIZATIONS BELIEVE THEY ARE VERY OR HIGHLY 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) The most frequent attacks in healthcare are against the cloud, making it the top cybersecurity threat for the third consecutive year.

As shown, 63 percent of respondents say their organizations are vulnerable or highly vulnerable to a cloud/account compromise and 60 percent say they are vulnerable or highly vulnerable to supply chain attacks. Slightly more than half of respondents (54 percent) say their organizations are vulnerable or highly vulnerable to ransomware attacks and 52 percent say their organizations are very or highly vulnerable to BEC/spoofing/impersonation attacks. As indicated, respondents expressed slightly less concern about being vulnerable to all four types of cyberattacks in 2024 compared to the previous two years.

On a scale from 1 = not vulnerable to 10 = highly vulnerable, 7+ responses presented

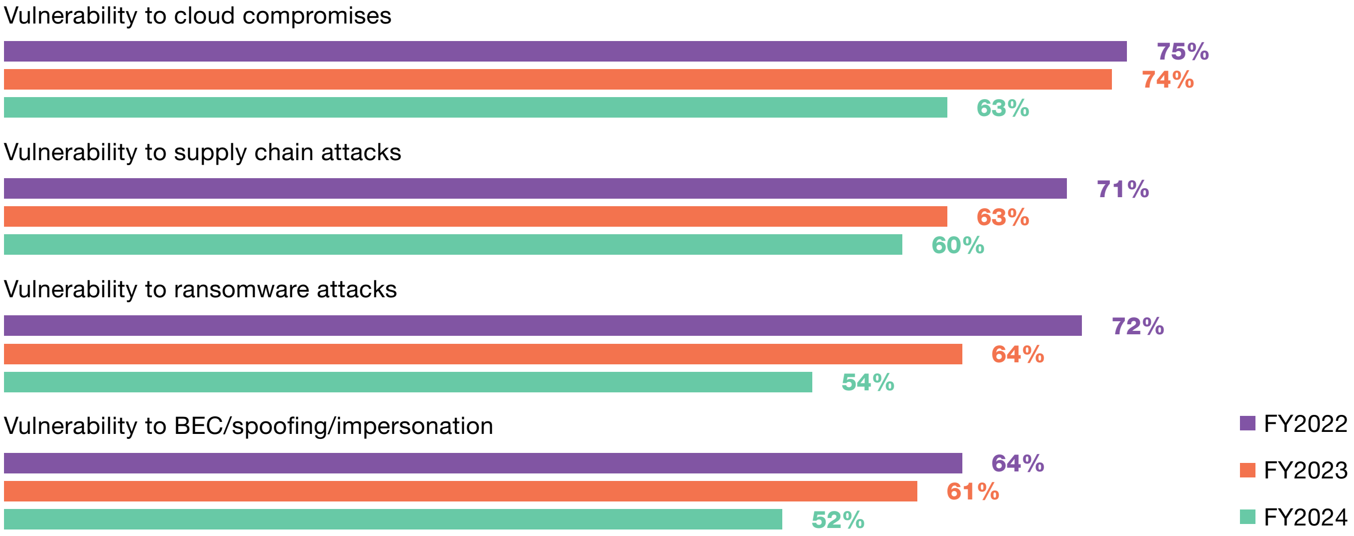


FIGURE 2.

The top cybersecurity threats of greatest concern

Respondents were asked to select the threats their organizations are most concerned about. The findings are presented in Figure 2. In this year's research, concerns about insecure mobile apps (eHealth) have increased to become the top cybersecurity threat in healthcare. Organizations are less worried about employee-owned mobile devices or BYOD, which decreased significantly from 61 percent in 2023 to 53 percent of respondents in 2024.

BEC/spoofing/impersonation decreased from 62 percent in 2023 to 46 percent of respondents in 2024 and cloud/account compromise decreased from 63 percent in 2023 to 55 percent of respondents in 2024. However, concerns about insecure mobile apps (eHealth) increased from 51 percent to 59 percent in 2024. Cloud/account compromises and insecure medical devices complete the top three list.

Six responses permitted

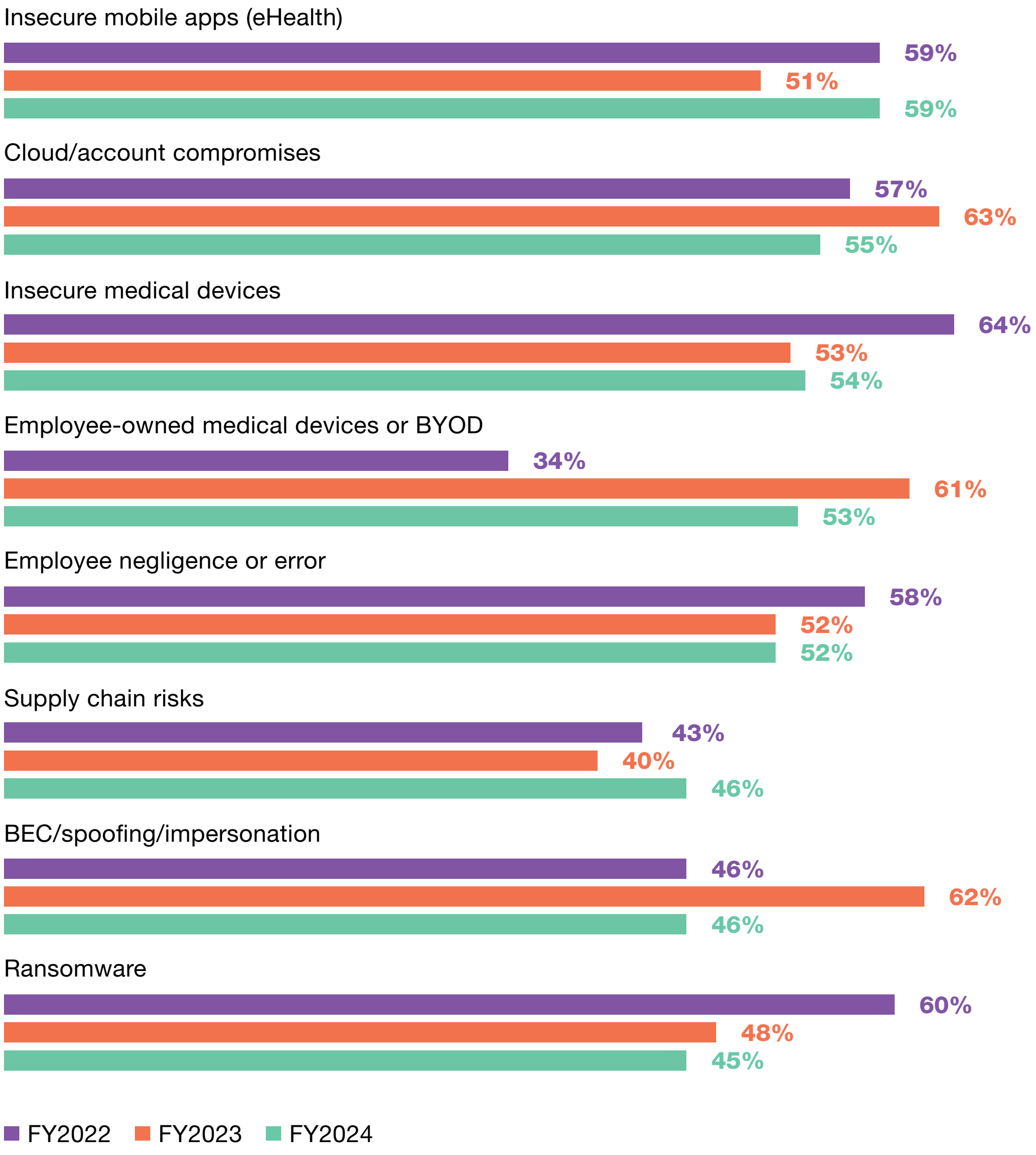


FIGURE 3.

Healthcare organizations are more prone to successful cloud/ account compromises and supply chain attacks

Figure 3 presents the percentage of organizations that experienced four different types of cyberattacks. Sixty-nine percent of respondents say they have experienced a cloud/account compromise. The average number of cloud/account compromises for these healthcare organizations was 20 in the past two years (see Figure 4). A cloud/account 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.

Organizations that had a ransomware attack (59 percent) 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, 68 percent of respondents say their organizations' supply chains were attacked an average of four times. Supplier impersonation and compromise attacks occur when a malicious actor impersonates or successfully compromise 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 respondents say their healthcare organizations experienced an average of four BEC/spoofing/impersonation 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 impersonations and CEO fraud.

Yes responses presented

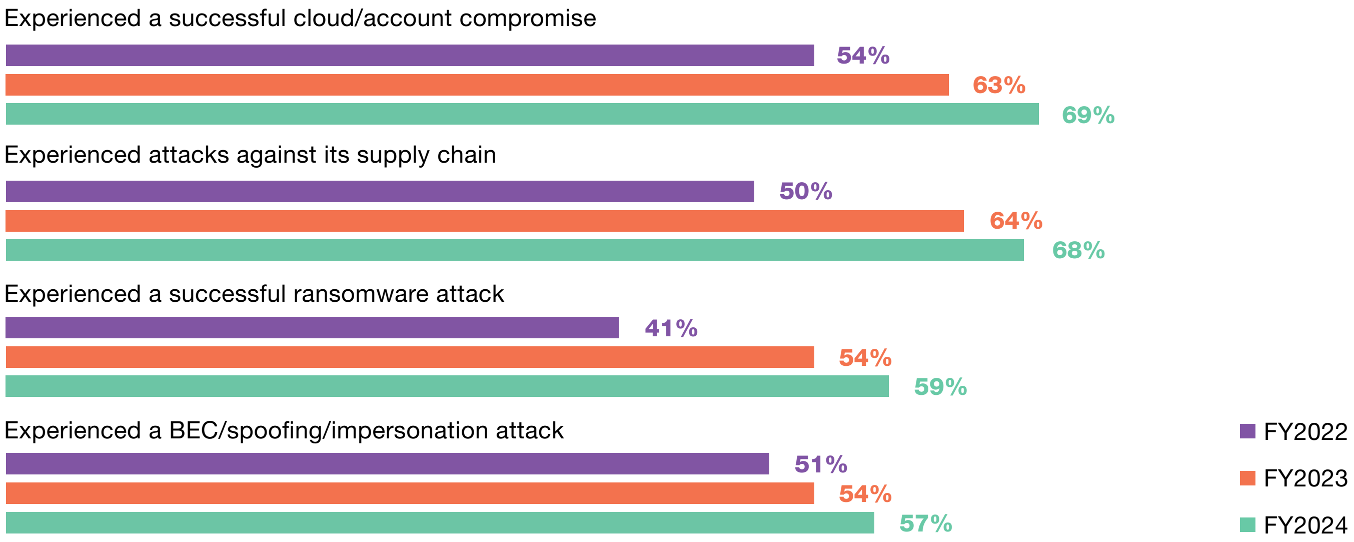


FIGURE 4.

By far, in the past two years the most cyberattacks involved cloud-based user accounts.

Respondents were asked how many of the four cyberattacks their organizations experienced over the past two years. Figure 4 shows the average number of the four cyberattacks. Organizations experienced an average of 20 attacks against the cloud which explains the previous finding that most organizations believe they are vulnerable or very vulnerable to such attacks. In contrast, only an average of 4 ransomware attacks, supply chain attacks and BEC/spoofing/impersonation attacks were experienced in the past two years.

Extrapolated averages presented

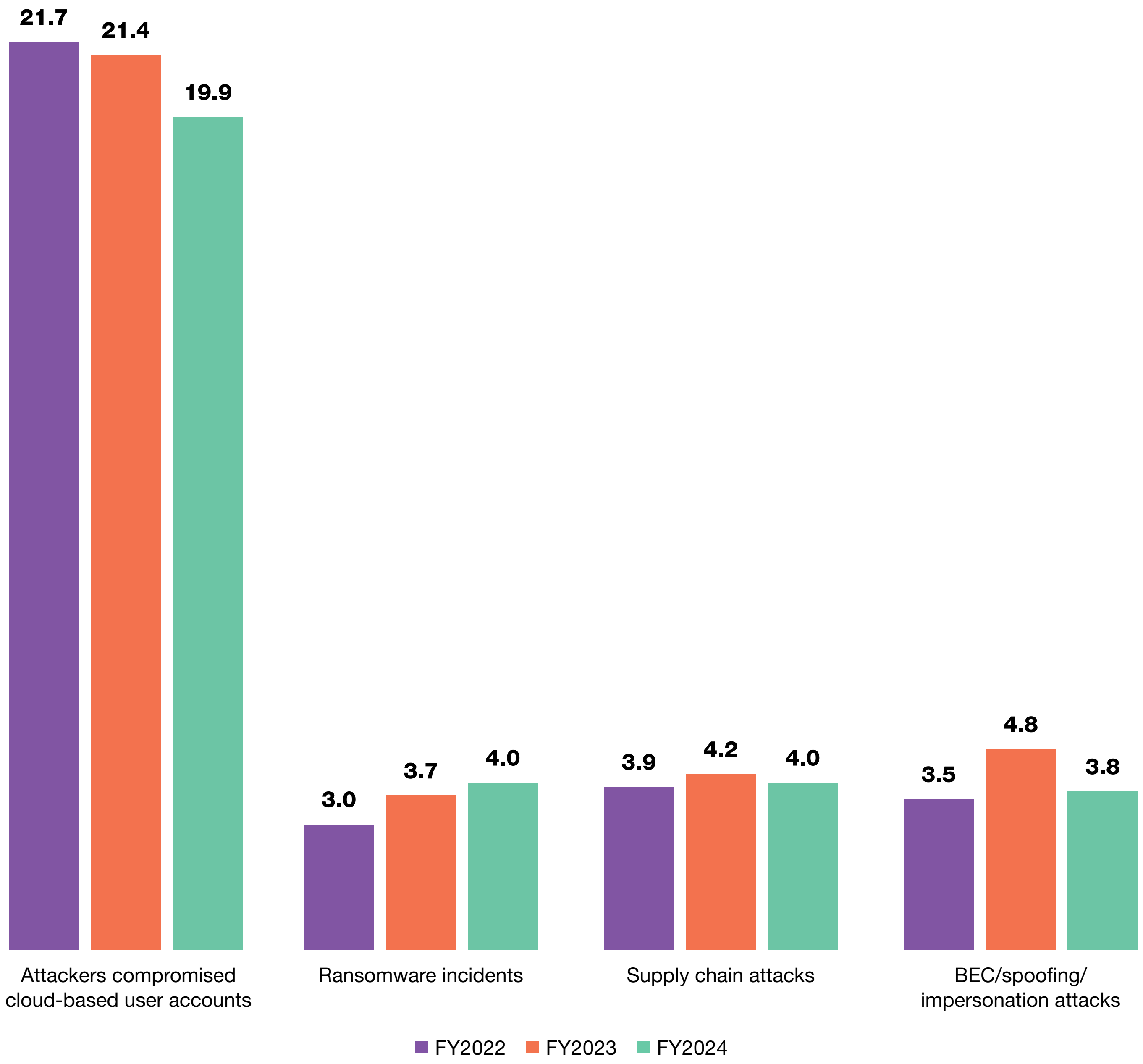


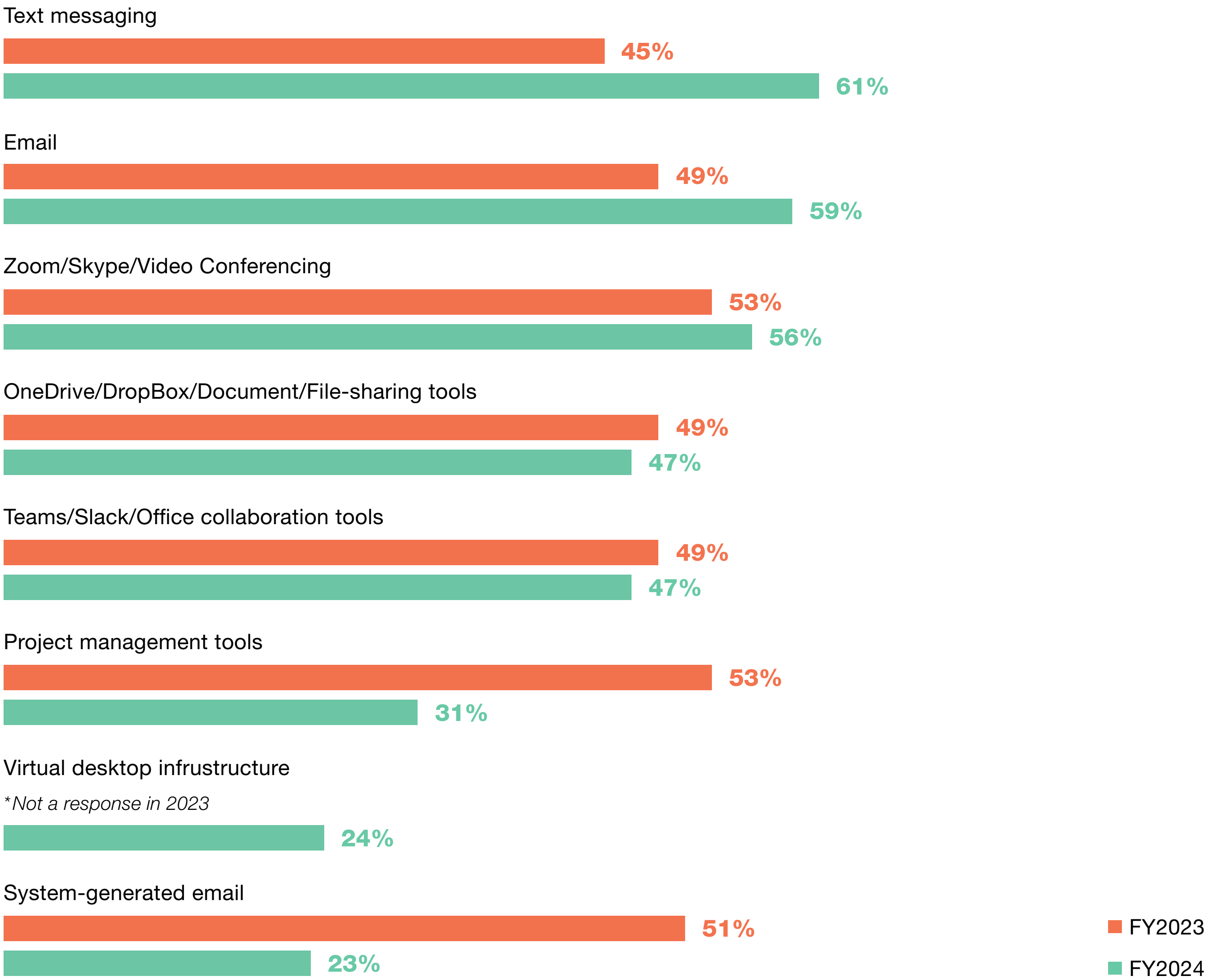
FIGURE 5.

Text messaging and email were the two most attacked cloud-based user accounts/collaboration tools.

Sixty-nine percent of organizations experienced a cloud/account compromise. Respondents were asked which cloud-based user accounts/collaboration tools were most attacked in their organizations.

As shown in Figure 5, of these respondents, cloud-based user accounts/collaboration tools that enable productivity were most often attacked. The tool most often attacked is text messaging, a significant increase from 45 percent in 2023 to 61 percent in 2024. Attacks against emails increased significantly from 49 percent to 59 percent of respondents. Fifty-six percent of respondents say Zoom/Skype/Videoconferencing is the third greatest target. A reason is the increase in remote working and the use of these tools.

More than one response permitted



THE IMPACT OF CYBERATTACKS ON PATIENT CARE

FIGURE 6.

CYBERATTACKS CONTINUE TO DISRUPT PATIENT CARE, INCREASING THE RISK TO PATIENTS.

Attacks against the supply chain continue to have the most impact on patient care. Figure 6 shows the four types of cyberattacks featured in this research and the percentage of respondents who say that if their organizations had such an attack, it impacted patient safety and delivery of care.

Sixty-eight percent of respondents say their organizations had a supply chain attack. Of these respondents, 82 percent say it resulted in a disruption in patient care, an increase from 77 percent of respondents in 2023.

Fifty-nine percent say their organizations had a ransomware attack and 70 percent of these respondents say it disrupted patient care. Sixty-nine percent of organizations had a cloud/account compromises and are becoming more impactful on patient care, a significant increase from 49 percent in 2023 to 57 percent of respondents in 2024. Fifty-seven percent of organizations had a BEC/spoofing/impersonation attack and there was a slight decrease from 69 percent to 65 percent of respondents in having an impact on patient care.

Yes responses presented

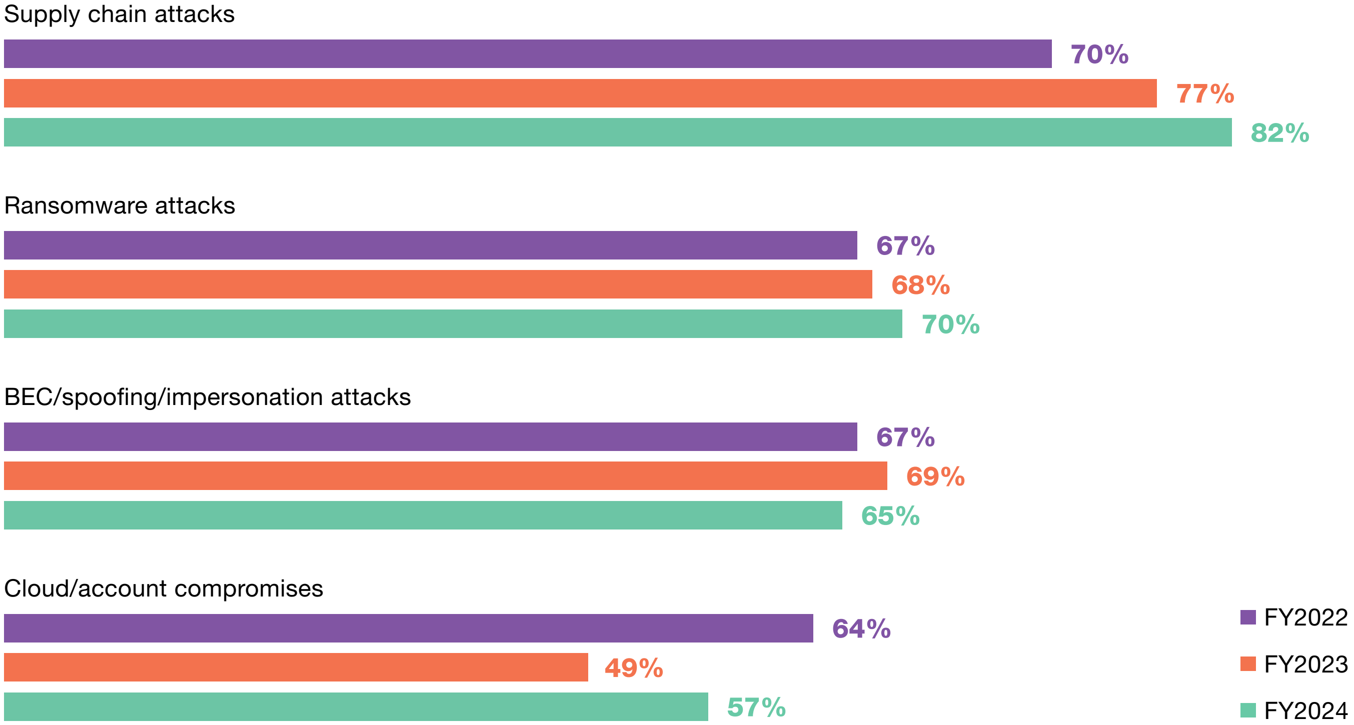
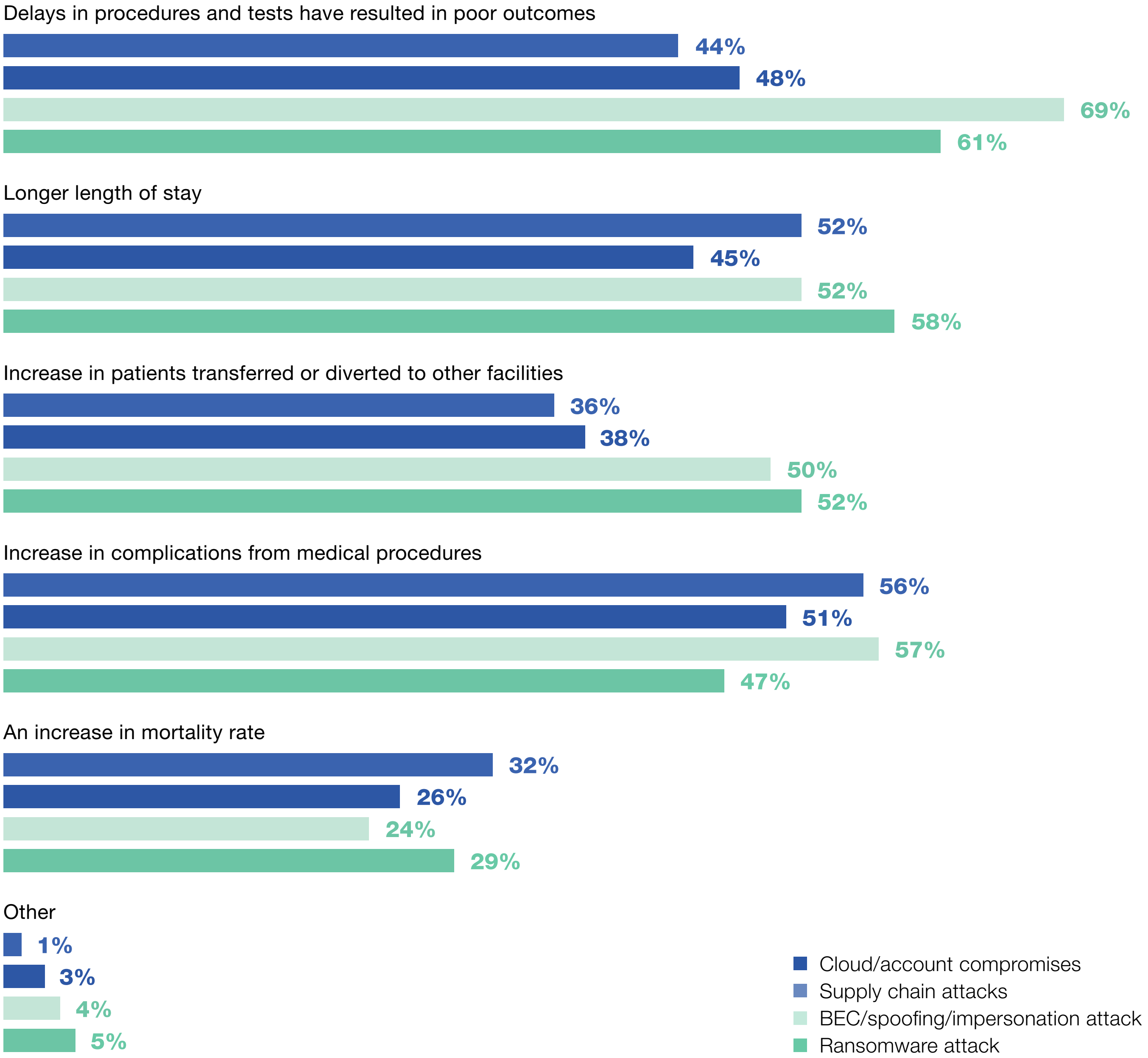


FIGURE 7.

BEC/spoofing/impersonation attacks are most likely to cause delays in procedures and tests that have resulted in poor outcomes.

Respondents were asked if their organization experienced the four cyberattacks what was the impact on patient care. According to Figure 7, of these, 69 percent of respondents say BEC/spoofing/impersonation attacks have caused delays in procedures and tests and have resulted in poor outcomes. This is followed by 61 percent of respondents who say ransomware attacks have resulted in delays and 58 percent of respondents say ransomware attacks have resulted in longer lengths of stay.

More than one response permitted



SYSTEM AVAILABILITY PROBLEMS AND DOWNTIME CONTINUE TO BE THE MOST SIGNIFICANT FINANCIAL CONSEQUENCES FROM A CYBERSECURITY COMPROMISE.

Healthcare is also spending less to ensure the impact on patient care is corrected, as shown in Table 2.

TABLE 2.

Table 2 shows the five average costs of a healthcare cybersecurity compromise. According to the research, 92 percent of respondents say their organizations experienced at least one cyberattack in the past 12 months. The average number of attacks was 40. As shown in Table 2, the average total cost for the **single most expensive cyberattack was $4,740,400**, a slight decline from $4,991,500 in 2023. This includes all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunities.

Respondents estimate that the average highest cost ($1,469,524) was caused by disruption to normal healthcare operations because of system availability problems, an increase from $1,297,790 in 2023. The cost due to users' idle time and lost productivity because of downtime or system performance delays decreased from an average of $1,148,045 to $995,484 in 2024. The time required to ensure the impact on patient care is corrected declined from $1,048,215 in 2023 to $853,272 in 2024.

FIVE AVERAGE COSTS OF A HEALTHCARE CYBERSECURITY COMPROMISE	2024 AVERAGE COST	2023 AVERAGE COST	2022 AVERAGE COST
Disruption to normal healthcare operations because of system availability problems	$1,469,524	$1,297,790	$1,018,670
Users' idle time and lost productivity because of downtime or system performance delays	$995,484	$1,148,045	$1,107,250
Time required to ensure impact on patient care is corrected	$853,272	$1,048,215	$664,350
Damage or theft of IT assets and infrastructure	$711,060	$748,725	$930,090
Remediation & technical support activities, including forensic investigations, incident response activities, help desk and delivery of services to patients	$711,060	$748,725	$708,640
Total	$4,740,400	$4,991,500	$4,429,000

FIGURE 8.

The average total cost for the highest ransomware payment increases. Ransomware remains an ever-present threat to healthcare organizations.

Fifty-nine percent of respondents say their organizations had a ransomware attack. Of these respondents, 36 percent say their organizations paid the ransomware, a slight decrease from 40 percent in 2023. Although fewer respondents say their organizations are paying the ransom as shown in Figure 8, the average total cost increased from $995,450 in 2023 to $1,099,200 in 2024 and from $771,905 in 2022, an increase of 35 percent.

Extrapolated values

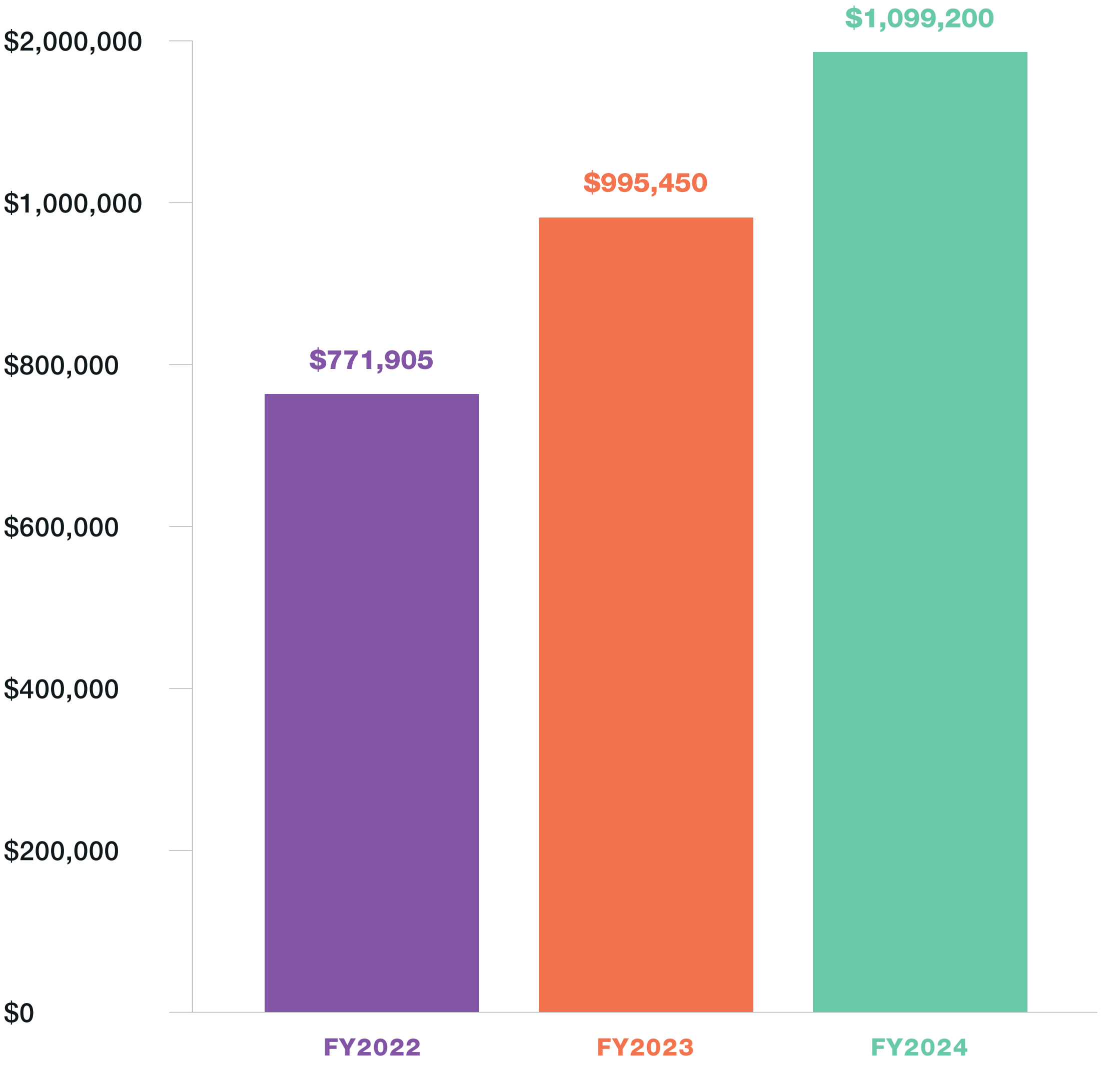


FIGURE 9.

CARELESS USERS ARE A TOP ROOT CAUSE OF DATA LOSS AND EXFILTRATION INCIDENTS.

Respondents were asked to identify the root causes of the data loss and exfiltration incident and their responses are shown in Figure 9. Ninety-two percent of organizations in this research had an average of at least two data loss or exfiltration incidents involving sensitive and confidential healthcare data in the past two years.

Healthcare organizations experienced an average of 20 such incidents in the past two years. According to the research, employees were the primary root cause of the data loss and exfiltration incident. Thirty-one percent of respondents say it was employee negligence because of not following policies, 26 percent of respondents say it was due to accidental data loss and 21 percent of respondents say employee sends PII or PHI to an unintended recipient via email.

More than one response permitted

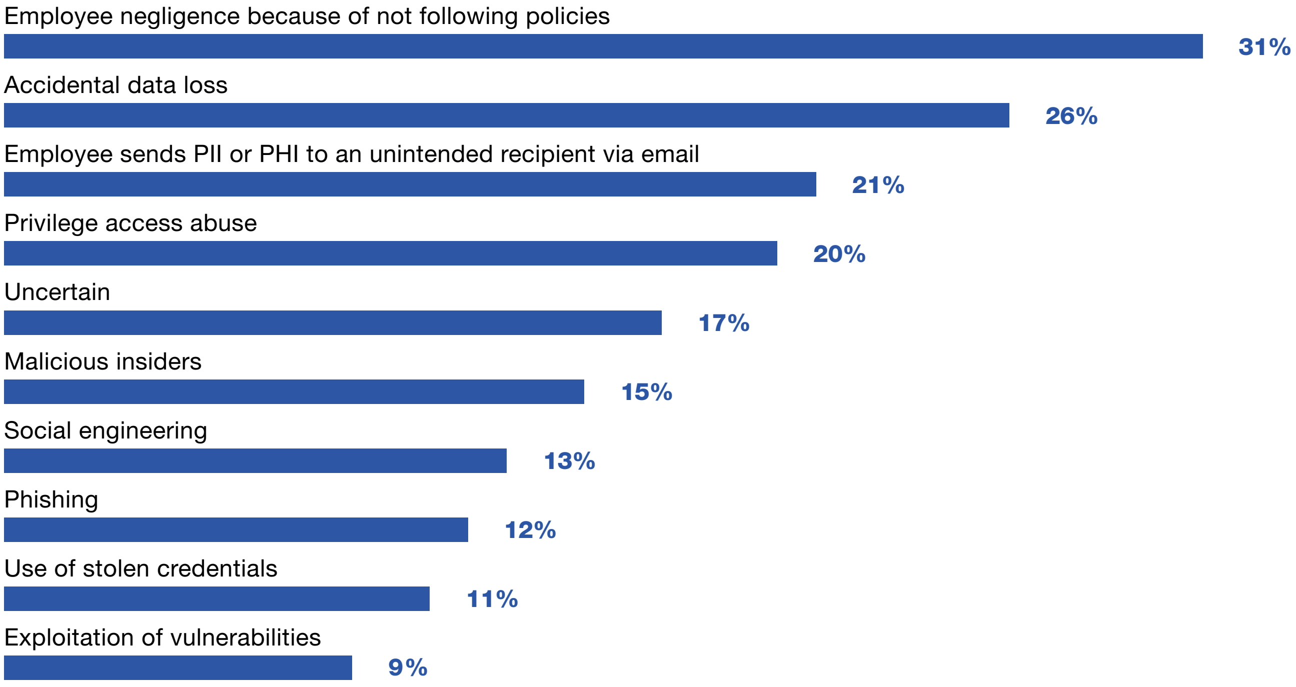


FIGURE 10.

Data loss or exfiltration has had an impact on patient mortality.

Respondents were asked what impact the data loss protection or exfiltration incident had on patient care. Fifty-one percent of the 92 percent of respondents that had a data loss or exfiltration say the incident resulted in a disruption in patient care operations. Of these respondents, as shown in Figure 10, 50 percent say it increased the mortality rate and 37 percent of respondents say it caused delays in procedures and tests that resulted in poor outcomes.

More than one response permitted

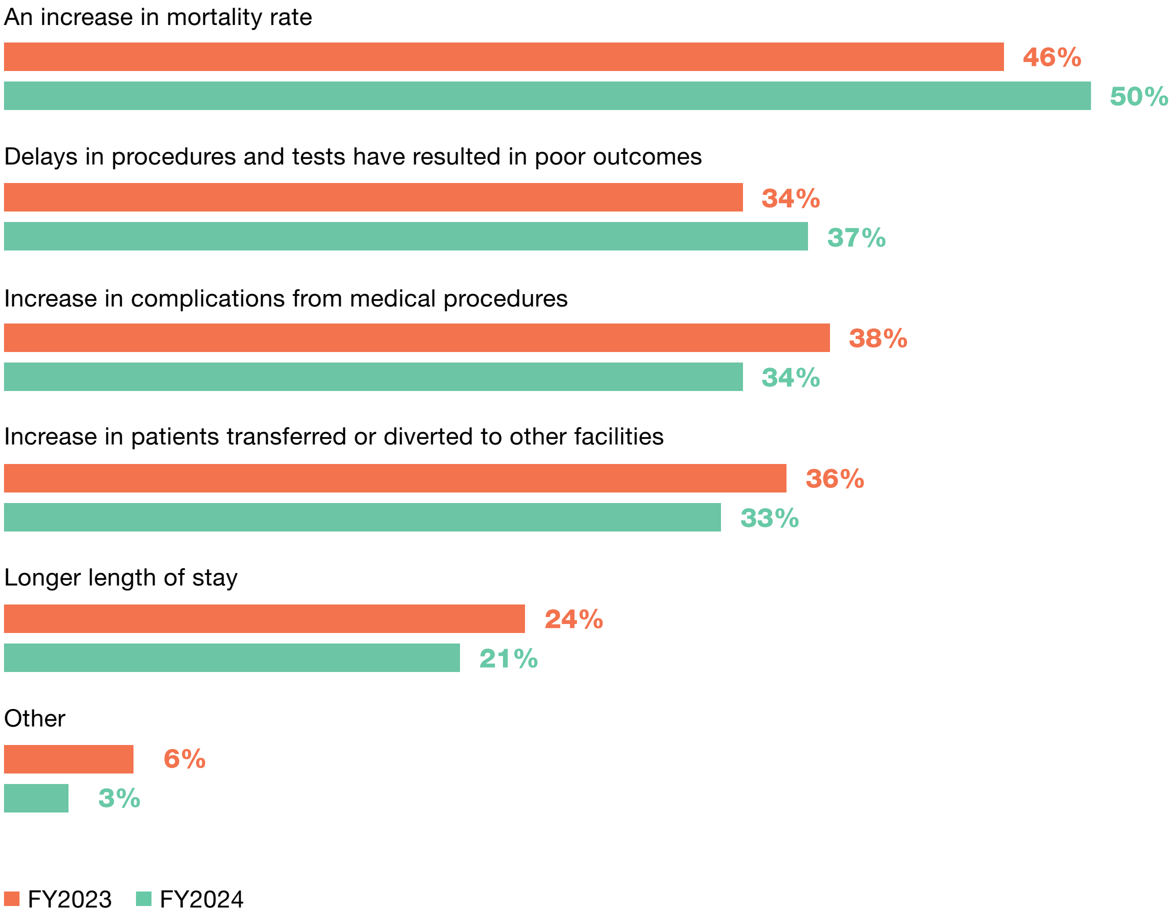


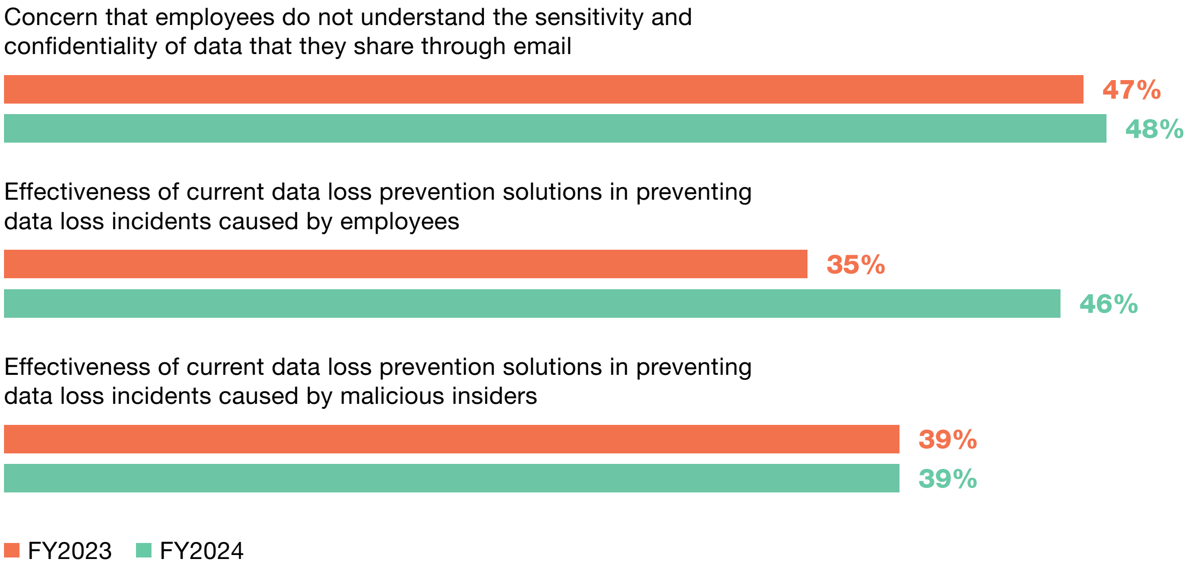
FIGURE 11.

New data loss prevention tools are needed to prevent security incidents caused by employees and malicious insiders.

Respondents were asked how effective their data loss prevention solutions are in preventing data loss incidents by employees and malicious insiders and how concerned their organizations are about the insider risk. To understand respondents' perceptions about effectiveness they were asked to rate 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 11 presents the very effective responses (7+ on the 10-point scale). As shown, while effectiveness in data loss prevention solutions in preventing data loss incidents caused by employees has increased from 35 percent of respondents to 46 percent of respondents, there has been no improvement in preventing data loss incidents caused by malicious insiders. About half of respondents (48 percent) are concerned or very concerned that employees do not understand the sensitivity and confidentiality of data shared through email.

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



AI AND MACHINE LEARNING IN HEALTHCARE

FIGURE 12.

FOR THE FIRST TIME, THE RESEARCH INCLUDES THE BENEFITS AND RISKS OF THE USE OF AI IN HEALTHCARE.

Respondents were asked if their organizations adopted AI. As shown in Figure 12, 54 percent of respondents say their organizations have embedded AI in cybersecurity (28 percent) or embedded in both cybersecurity and patient care (26 percent). Fifty-seven percent of these respondents say AI is very effective in improving organizations' cybersecurity posture.

Only one choice permitted

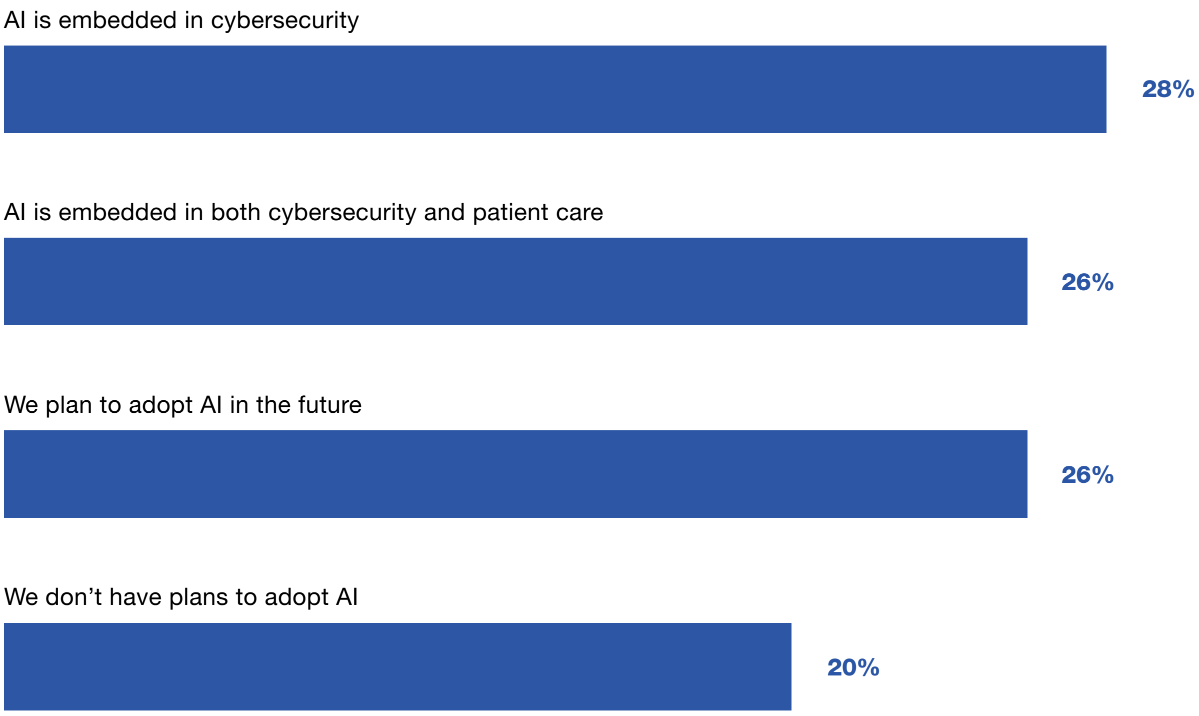


FIGURE 13.

AI can increase the productivity of IT security personnel and reduce the time and cost of patient care and administrators' work.

Respondents were asked what they believe the benefits of AI are when used in healthcare. As shown in Figure 13, 55 percent of respondents agree or strongly agree that AI-based security technologies will increase the productivity of their organizations' IT security personnel. Forty-eight percent of respondents agree or strongly agree that AI simplifies patient care and administrators' work by performing tasks that are typically done by humans but in less time.

Strongly agree and Agree responses combined

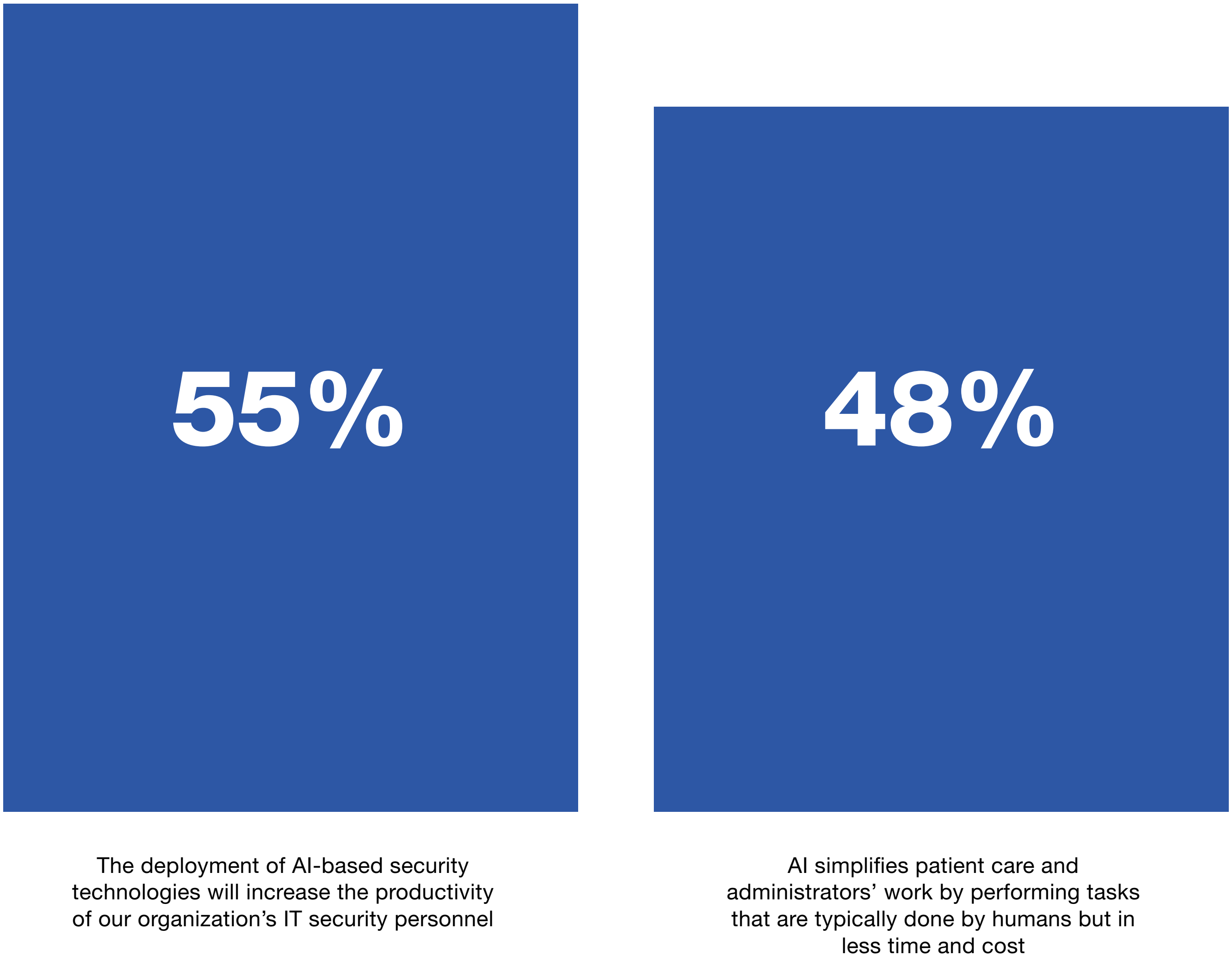


FIGURE 14.

AI can improve the ability to understand employees' behavior but may pose a risk to sensitive and confidential data.

Thirty-six percent of respondents use AI and machine learning to understand human behavior. Of these respondents, 56 percent of respondents say understanding human behavior to protect emails is very important, recognizing the prevalence of socially engineered attacks.

Respondents were asked to rate the difficulty of safeguarding confidential and sensitive patient data in AI on a scale of 1 = not difficulty to 10 = very difficult. Figure 14 shows the difficult and very difficult responses (7+ responses on the 10-point scale). Sixty-three percent of respondents say it is difficult or very difficult to safeguard confidential and sensitive patient data used in AI.

Respondents were asked to rate the effectiveness of AI in improving the cybersecurity posture of their organizations on a scale of 1 = not effective to 10 = highly effective. On a positive note, 57 percent of respondents say AI is effective or very effective in improving the security posture of the organization (7+ responses on the 10-point scale).

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

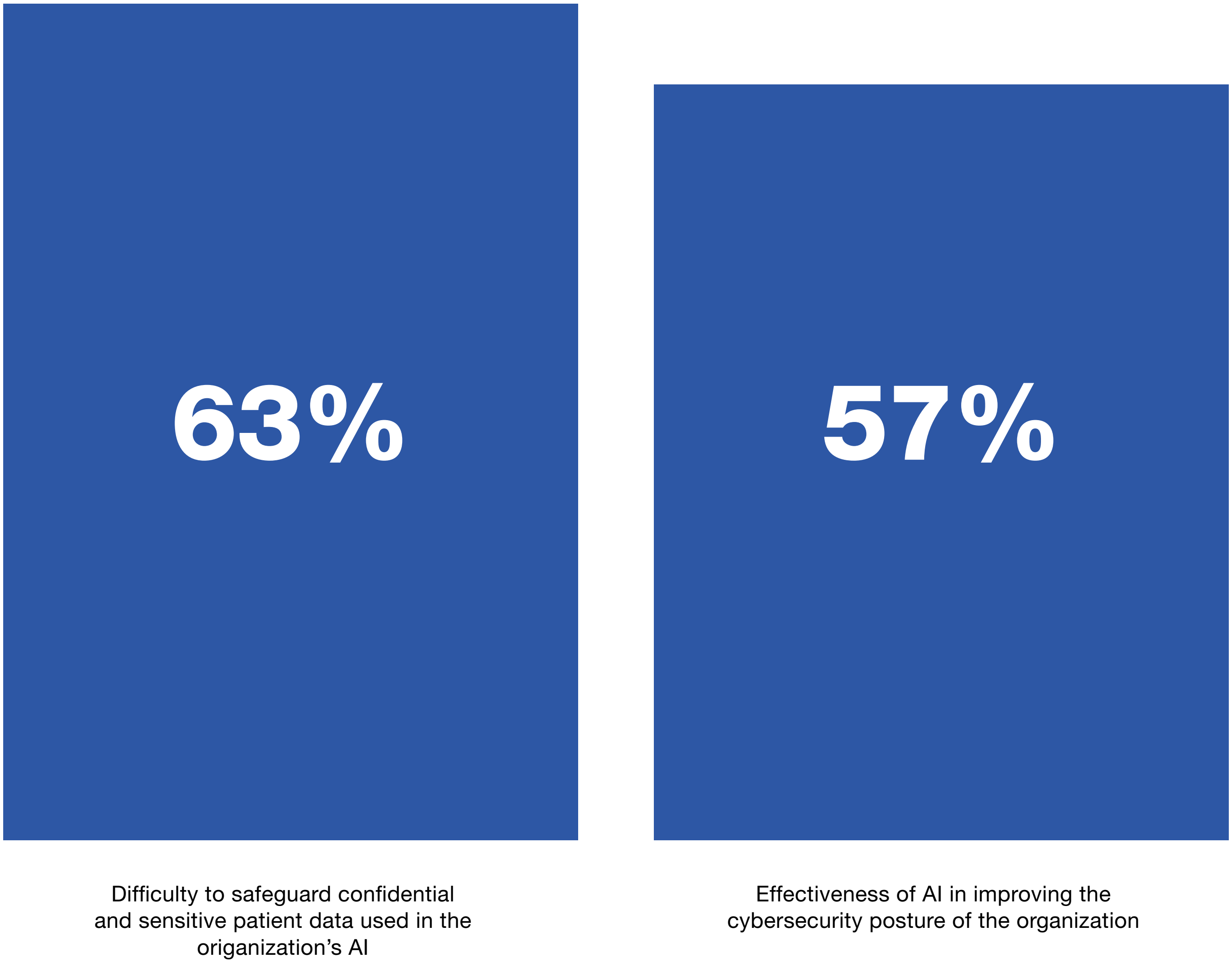
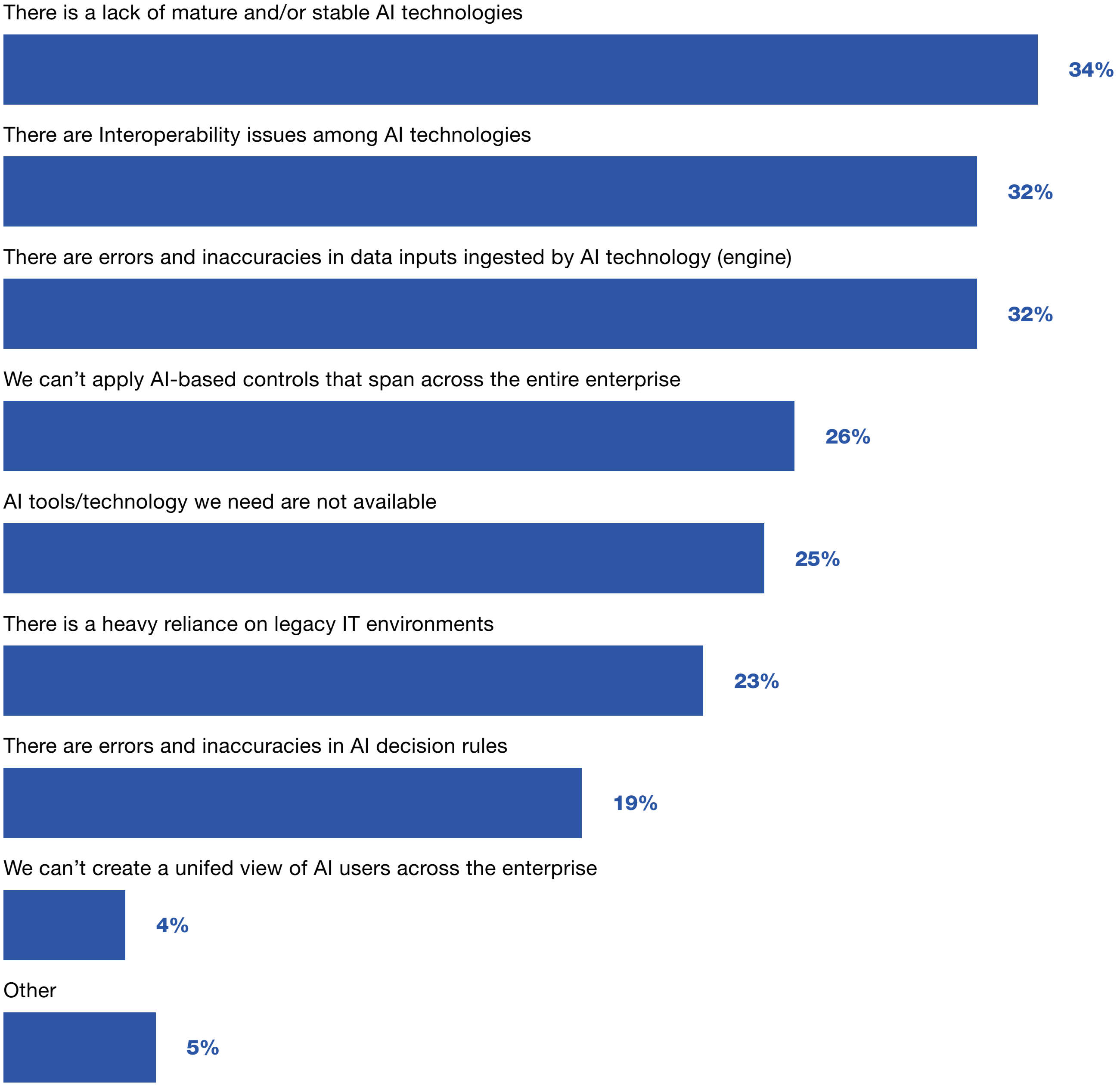


FIGURE 15.

While AI offers benefits, there are issues that may deter wide-spread acceptance.

Respondents were asked to identify the challenges to adopting AI-based security technologies. Figure 15 presents the issues that may delay adoption. The top challenges are the lack of mature and/or stable AI technologies (34 percent of respondents), the interoperability issues among AI technologies (32 percent of respondents) and errors and inaccuracies in data inputs ingested by AI technology (19 percent).

Two responses permitted



SOLUTIONS AND RESPONSES TO CYBER INSECURITY

FIGURE 16.

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

Respondents were asked if their organizations include the prevention and response to certain threats as part of their cybersecurity strategy. As shown in this research, the most common attacks in healthcare target the cloud and it seems organizations are making it a priority in their cybersecurity strategies.

According to Figure 16, a significant number of organizations are concentrating on measures to prevent and respond to cloud compromises (67 percent of respondents) and ransomware attacks (65 percent). In contrast, efforts to address BEC and supply chain attacks are below 50 percent of respondents and should be made more of a priority in cybersecurity strategies.

More than one response permitted

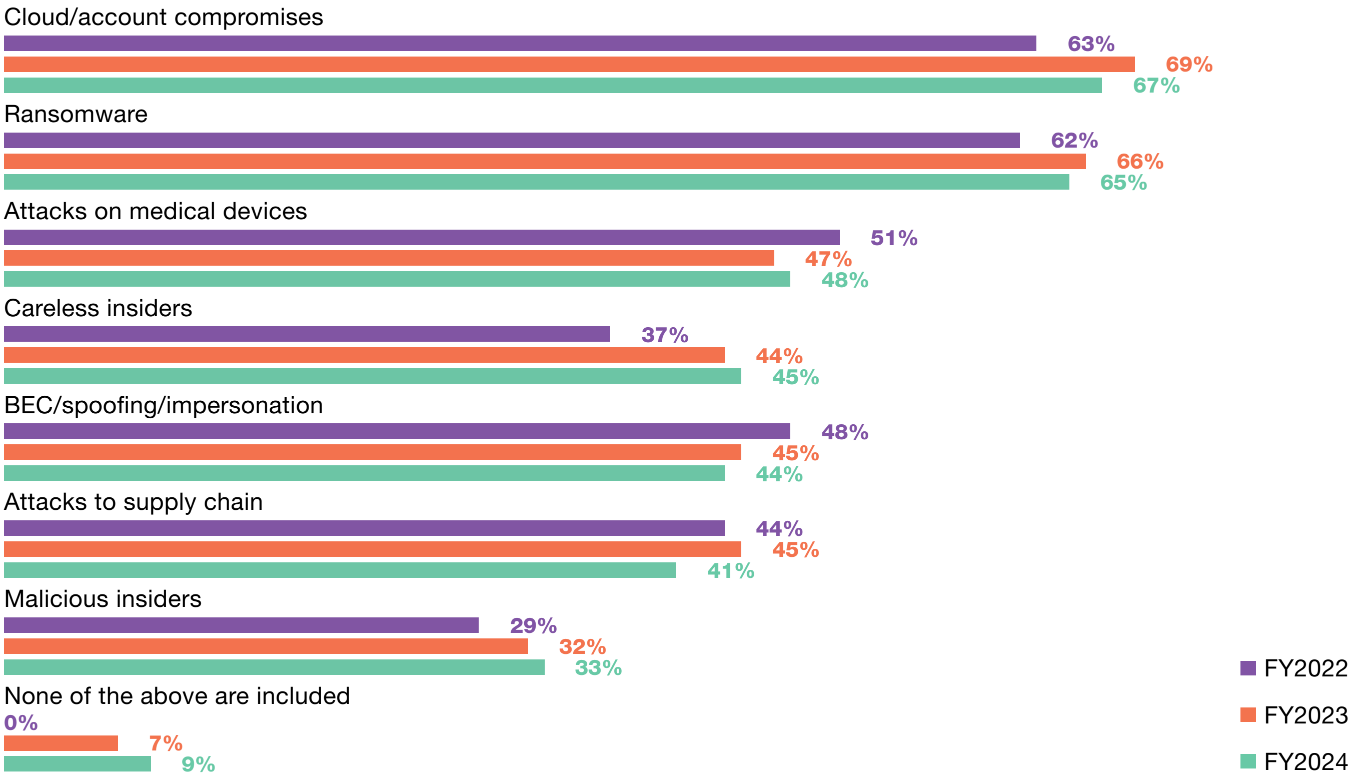


FIGURE 17.

The lack of clear leadership is a growing problem and a threat to healthcare organizations' cyber security posture.

Respondents were asked what challenges keep your organization's cybersecurity posture from being fully effective. While 55 percent of respondents say their organizations' lack of in-house expertise is a primary deterrent to achieving a strong cybersecurity posture, the lack of clear leadership as a challenge increased significantly since 2023 from 14 percent to 49 percent of respondents, as shown in Figure 17.

Not having enough budget decreased from 47 percent to 40 percent of respondents in 2024. Survey respondents note that their annual budgets for IT increased 12 percent from last year ($66 million in 2024 vs. $58 million in 2023) with 19 percent of that budget dedicated to information security. The healthcare industry seems to recognize cyber safety is patient safety based on the findings.

More than one response permitted

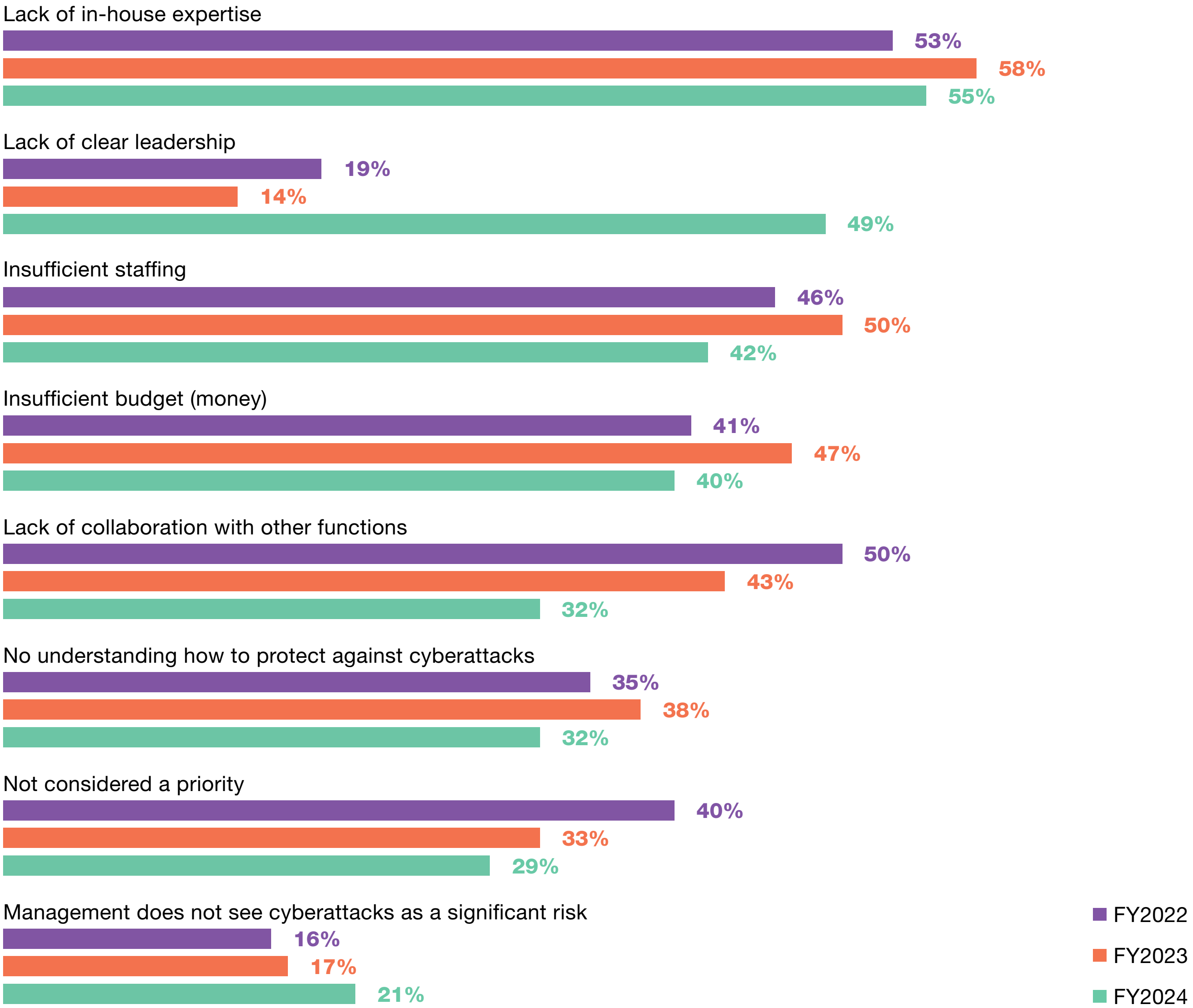


FIGURE 18.

Organizations continue to rely on security training awareness programs to reduce risks caused by employees.

Respondents were asked what steps are taken to address the risk of employees' lack of awareness about cybersecurity threats. Seventy-one percent of respondents say their organizations take steps to address the risk of employees' lack of awareness about cybersecurity threats, an increase from 65 percent of respondents in 2023. As shown in Figure 18, 59 percent of respondents say their organizations conduct regular training and awareness programs. Fifty-three percent of respondents say their organizations monitor the actions of employees.

More than one response permitted

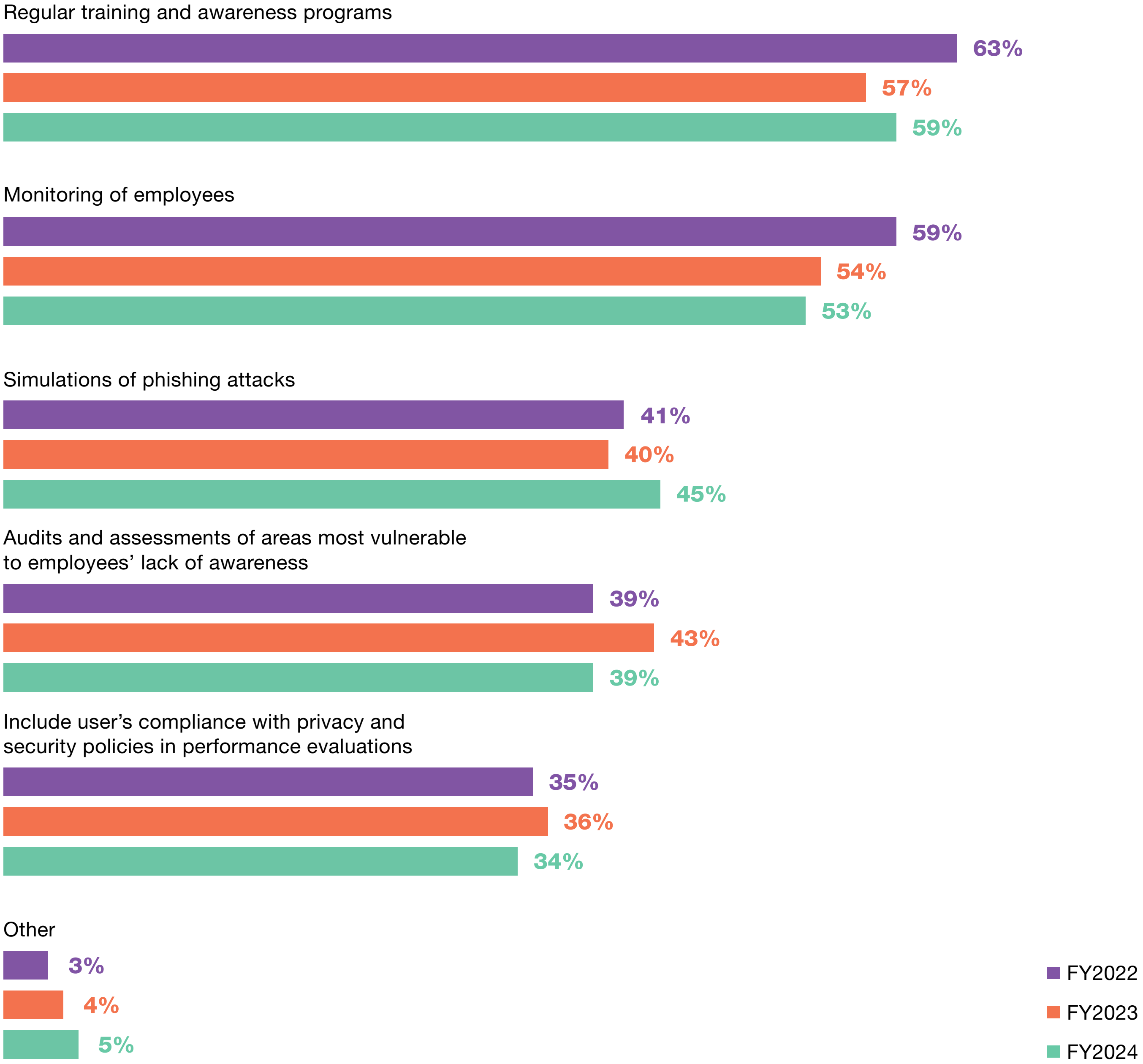


FIGURE 19.

To reduce phishing and other email-based attacks, most organizations are using anti-virus/anti-malware.

Respondents were asked what security methods and technologies their organizations use to reduce phishing and other email-based attacks. As shown in Figure 19, 53 percent of respondents say they use anti-virus/anti-malware. This is followed by patch & vulnerability management (52 percent of respondents) and multi-factor authentication (49 percent of respondents). Technologies such as DMARC, AI/ML, threat intelligence and email DLP did not rank in the top five.

More than one response permitted

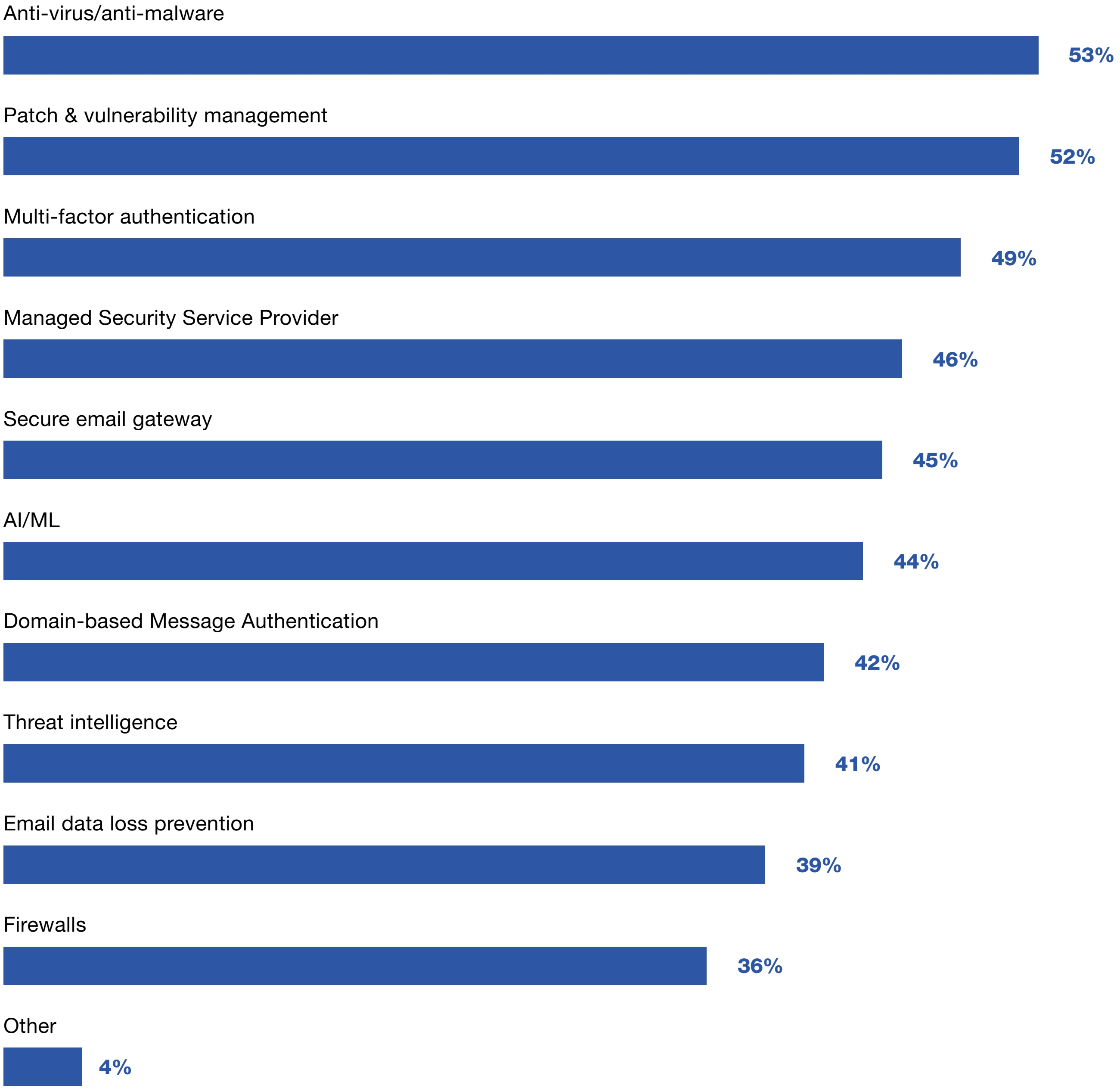


FIGURE 20.

Encryption is mostly used to prevent data loss or an exfiltration incident.

Respondents were asked what security methods and technologies their organizations implemented to prevent data loss or an exfiltration incident. According to Figure 20, 46 percent of respondents say encryption for data in transit and 44 percent of respondents say cloud security tools are used to prevent data loss or an exfiltration incident. As discussed previously, organizations are vulnerable or very vulnerable to cloud/account compromises attacks.

More than one response permitted

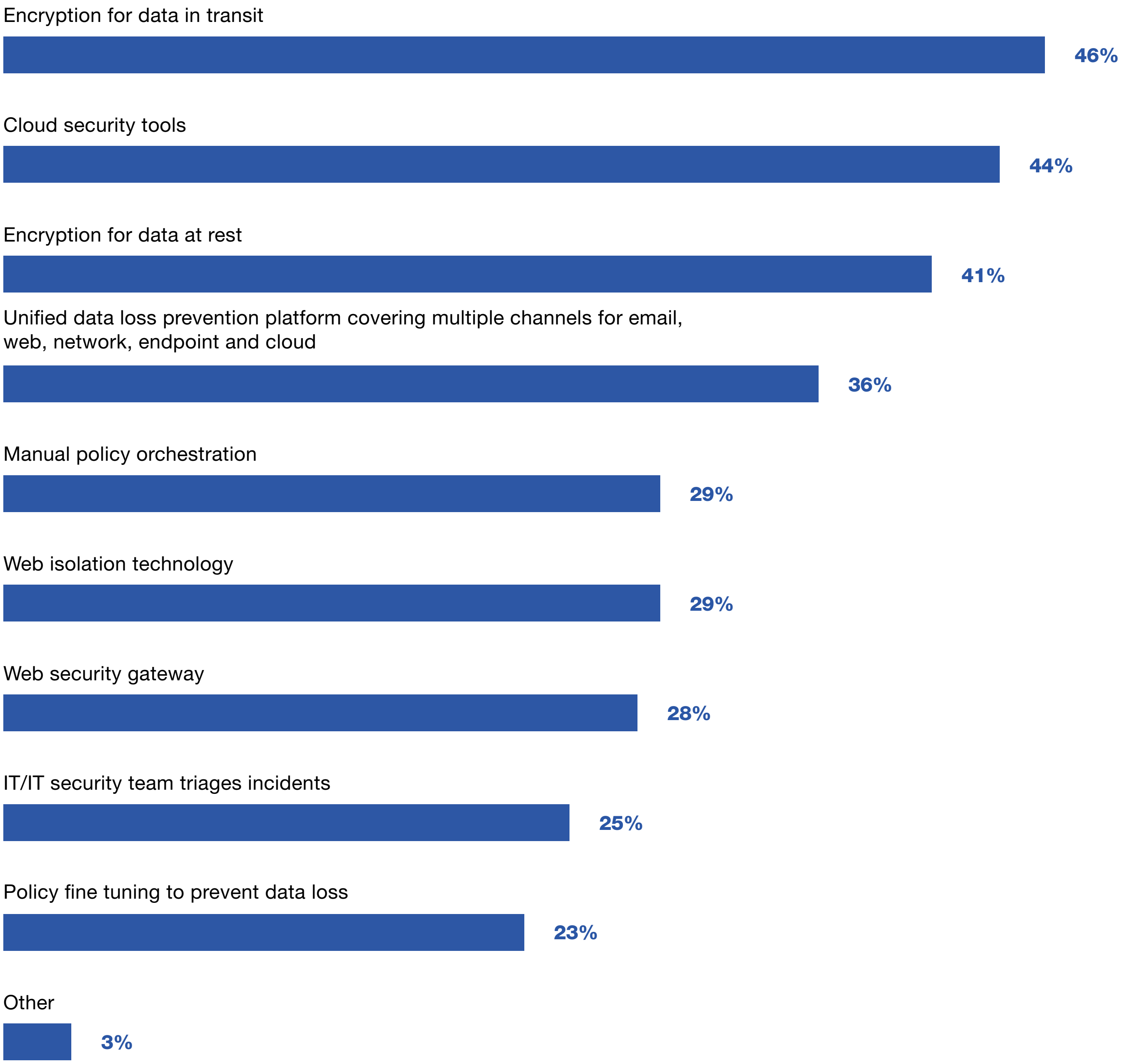
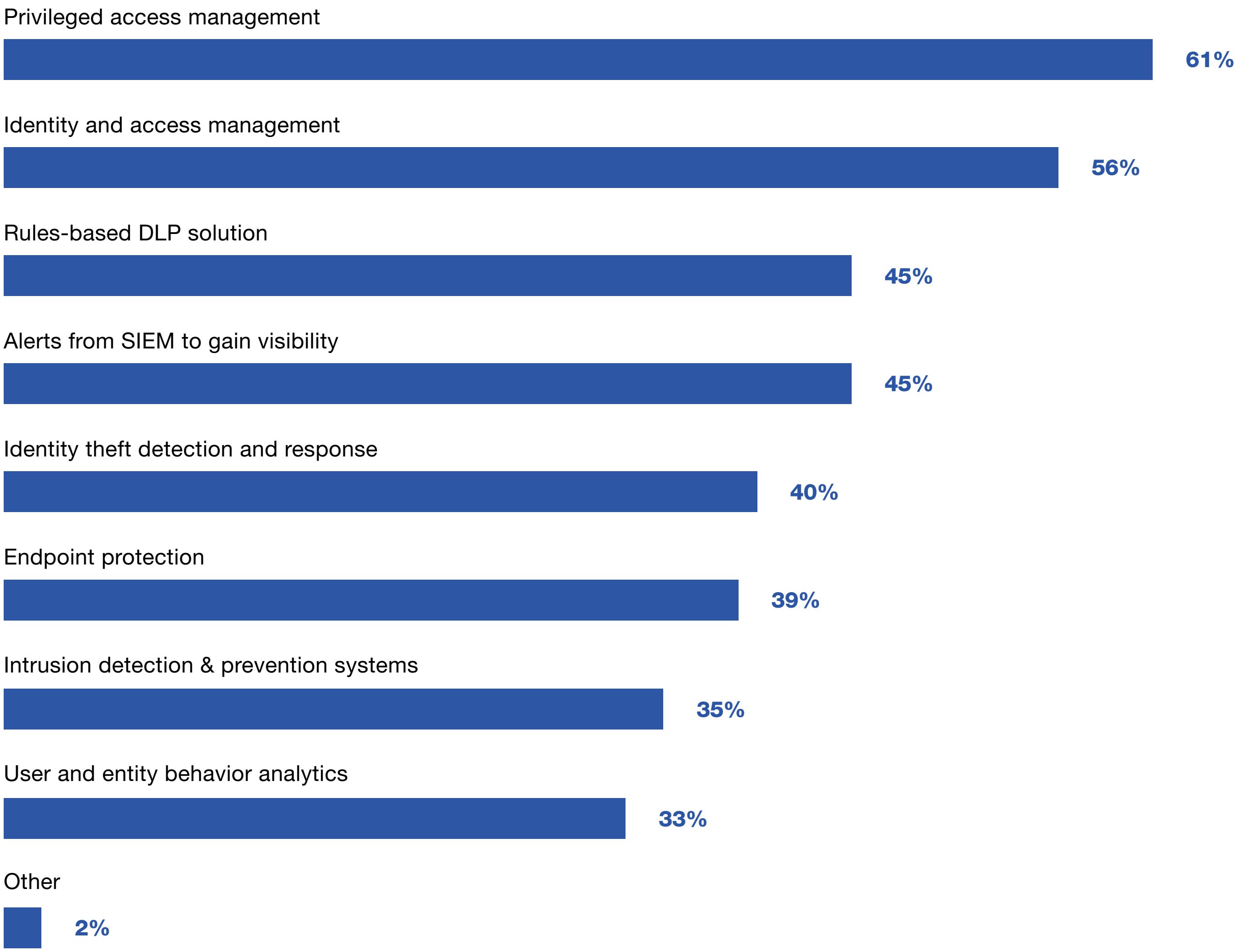


FIGURE 21.

Privileged access management and identity and access management are primarily used to prevent identity risk and lateral movement in their networks.

Respondents were asked what other technologies are implemented to prevent identity risk and lateral movement in their networks. Figure 21 presents the technologies healthcare organizations are implementing to prevent identity risk and lateral movement in its network. Most frequently implemented are privileged access management (61 percent of respondents), identity and access management (56 percent of respondents), a rules-based DLP solution (45 percent of respondents) and alerts from SIEM to gain visibility (45 percent of respondents).

More than one response permitted



OUR FINAL SAMPLE CONSISTED OF 648 SURVEYS OR A 3.6 PERCENT RESPONSE RATE.

A sampling frame of 18,015 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 3 shows 732 total returns. Screening and reliability checks required the removal of 84 surveys. Our final sample consisted of 648 surveys or a 3.6 percent response rate.

TABLE 3.

SAMPLE RESPONSE	FREQUENCY	PERCENTAGE
Sampling frame	18,015	100%
Total returns	732	4.1%
Rejected or screened surveys	84	0.5%
Final sample	648	3.6%

FIGURE 22.

Type of organization

Figure 22 reports the respondent's type of organizations. Twenty-two percent of respondents are from organizations that are private healthcare providers. This is followed by public healthcare provider (21 percent), healthcare insurer (19 percent), healthcare insurance (12 percent of, payer and pharma (each at 8 percent).

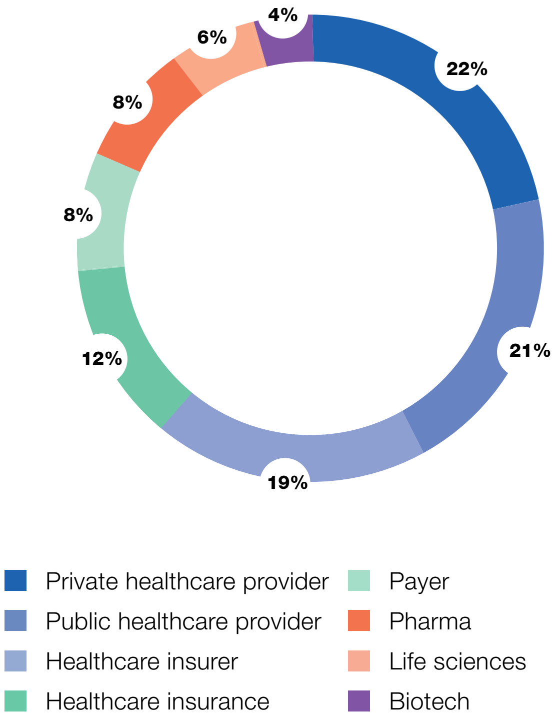


FIGURE 23.

Current position within the organization

Figure 23 reports the respondent's organizational level within participating organizations. By design, more than half (69 percent) are at or above the supervisory levels. The largest category is manager (27 percent).

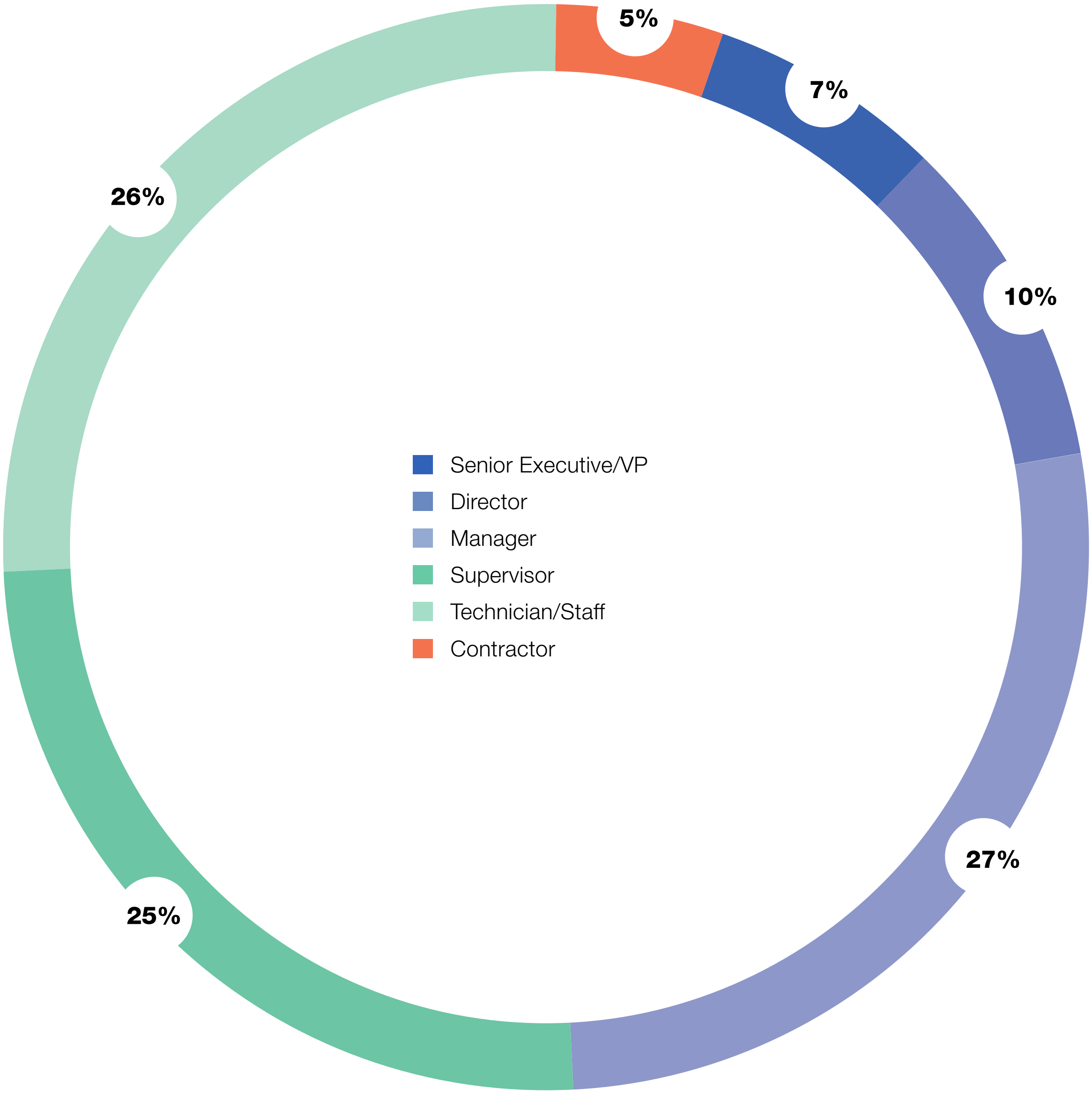


FIGURE 24.

Direct reporting channel

As shown in Figure 24, 21 percent of respondents report to the chief information security officer, 18 percent report to the chief information officer, 13 percent report to cloud administration, 9 percent report to the compliance officer and 8 percent report to data center management and chief risk officer.

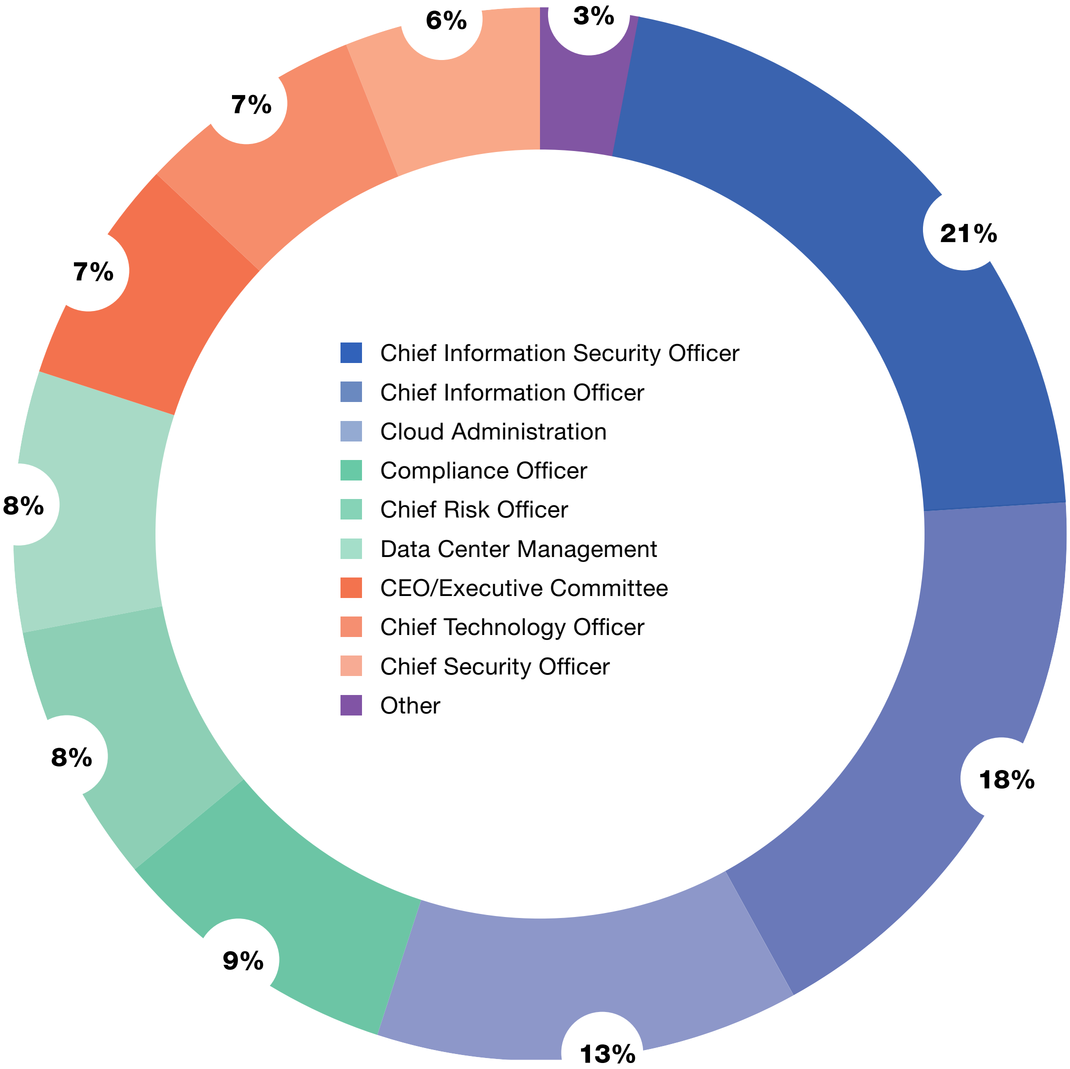
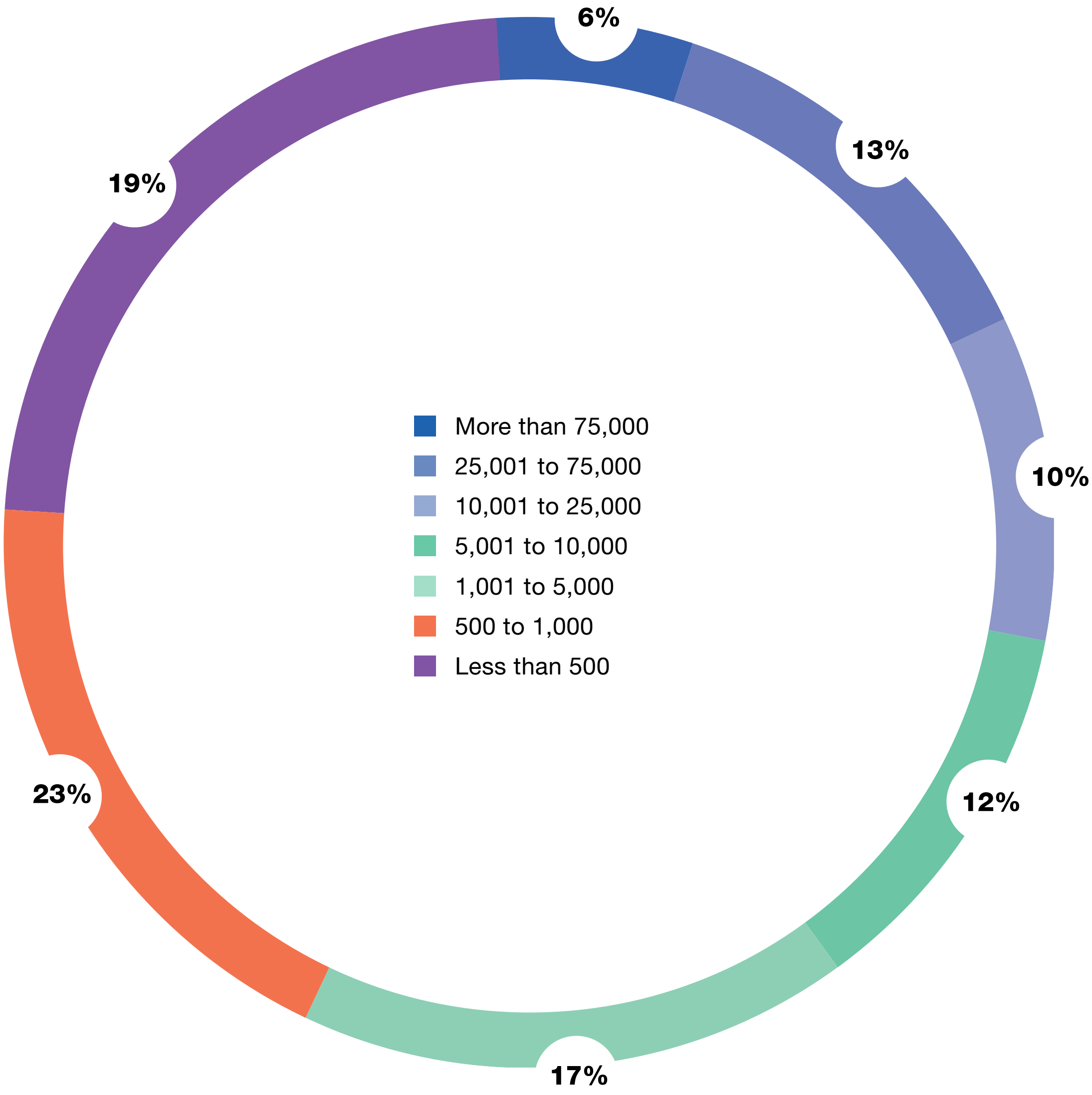


FIGURE 25.

Global 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 and April 2024.

SURVEY RESPONSE	FY2024	FY2023	FY2022
Total sampling frame	18015	17,085	16,451
Total returns	732	715	698
Rejected returns	84	62	57
Total sample	648	653	641
Response rate	3.6%	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)	FY2024	FY2023	FY2022
	Setting IT cybersecurity priorities	49%	51%	46%
	Managing IT security budgets	43%	45%	42%
	Selecting vendors and contractors	47%	49%	47%
	Participating in IT cybersecurity strategies	52%	51%	51%
	Evaluating and measuring effectiveness of cybersecurity strategies	36%	36%	34%
	Managing cybersecurity risk	40%	34%	36%
	Overseeing governance and compliance	28%	27%	29%
	None of the above [Stop]	0%	0%	0%

PART 1. CYBERSECURITY THREATS TO HEALTHCARE

Q1	WHAT CYBERSECURITY THREATS IS YOUR ORGANIZATION MOST CONCERNED ABOUT? (Please select the top six)	FY2024	FY2023	FY2022
	BEC/spoof phishing	46%	62%	46%
	Cloud/account compromises	55%	63%	57%
	Employee negligence or error	52%	52%	58%
	Employee-owned mobile devices or BYOD	53%	61%	34%
	Insecure medical devices	54%	53%	64%
	Insecure mobile apps (eHealth)	59%	51%	59%
	Malicious insiders	42%	45%	37%
	Nation state attacks	21%	19%	17%
	Process failures	31%	31%	36%
	Ransomware	45%	48%	60%
	Supply chain risks	46%	40%	43%
	System failures	44%	35%	36%
	Third-party misuse of patient data	31%	26%	33%
	Use of public cloud services	17%	11%	18%
	Other (please specify)	4%	3%	2%
	Total	600%	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)	FY2024	FY2023	FY2022
	Attacks to medical devices	48%	47%	51%
	Attacks to the supply chain	41%	45%	44%
	BEC/spoof phishing	44%	45%	48%
	Cloud/account compromises	67%	69%	63%
	Malicious insiders	33%	32%	29%
	Careless insiders	45%	44%	37%
	Ransomware	65%	66%	62%
	None of the above	9%	7%	
	Total	352%	355%	334%

Q3	**WHAT CHALLENGES KEEP YOUR ORGANIZATION'S CYBERSECURITY POSTURE FROM BEING FULLY EFFECTIVE?** (Please select the top three challenges)	FY2024	FY2023	FY2022
	Insufficient budget (money)	40%	47%	41%
	Insufficient staffing	42%	50%	46%
	Lack of in-house expertise	55%	58%	53%
	Lack of clear leadership	49%	14%	19%
	No understanding how to protect against cyberattacks	32%	38%	35%
	Management does not see cyberattacks as a significant risk	21%	17%	16%
	Lack of collaboration with other functions	32%	43%	50%
	Not considered a priority	29%	33%	40%
	Total	300%	300%	300%

Q4	**USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO BEC/SPOOFING/IMPERSONATION** (From 1 = not vulnerable to 10 = highly vulnerable)	FY2024	FY2023	FY2022
	1 or 2	13%	8%	11%
	3 or 4	16%	16%	13%
	5 or 6	19%	15%	12%
	7 or 8	21%	25%	24%
	9 or 10	31%	36%	40%
	Total	100%	100%	100%
	Extrapolated value	6.3	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)	FY2024	FY2023	FY2022
	1 or 2	2%	2%	5%
	3 or 4	18%	11%	8%
	5 or 6	20%	24%	16%
	7 or 8	24%	23%	23%
	9 or 10	36%	40%	48%
	Total	100%	100%	100%
	Extrapolated value	7.0	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)	FY2024	FY2023	FY2022
	1 or 2	14%	5%	6%
	3 or 4	15%	10%	9%
	5 or 6	17%	21%	13%
	7 or 8	30%	26%	25%
	9 or 10	24%	38%	47%
	Total	100%	100%	100%
	Extrapolated value	6.2	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)	FY2024	FY2023	FY2022
	1 or 2	8%	5%	0%
	3 or 4	9%	6%	9%
	5 or 6	20%	15%	16%
	7 or 8	34%	40%	30%
	9 or 10	29%	34%	45%
	Total	100%	100%	100%
	Extrapolated value	6.8	7.3	7.7

Q8	DID YOUR ORGANIZATION EVER EXPERIENCE A SUCCESSFUL RANSOMWARE ATTACK?	FY2024	FY2023	FY2022
	Yes	59%	54%	41%
	No (please skip to Q12a)	33%	44%	52%
	Unsure (please skip to Q12a)	8%	2%	7%
	Total	100%	100%	100%

Q9	HOW MANY SUCCESSFUL RANSOMWARE INCIDENTS DID YOUR ORGANIZATION EXPERIENCE OVER THE PAST TWO YEARS?	FY2024	FY2023	FY2022
	One	37%	43%	53%
	Two to five	36%	34%	33%
	Six to 10	21%	16%	9%
	More than 10	6%	7%	5%
	Total	100%	100%	100%
	Extrapolated value	4.0	3.7	3.0

Q10A	DID YOUR ORGANIZATION PAY THE RANSOM?	FY2024	FY2023	FY2022
	Yes	36%	40%	51%
	No	64%	60%	49%
	Total	100%	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)	FY2024	FY2023	FY2022
	Less than $10,000	0%	0%	2%
	$10,000 to $25,000	9%	13%	9%
	$25,001 to $50,000	10%	9%	7%
	$50,001 to $75,000	12%	14%	10%
	$75,001 to $100,000	19%	18%	17%
	$100,001 to $250,000	12%	11%	19%
	$250,001 to $500,000	13%	12%	18%
	$500,001 to $1,00,000	8%	9%	8%
	$1,00,001 to $5,000,000	9%	7%	5%
	$5,00,001 to $10,000,000	6%	4%	3%
	More than $10,000,000	2%	3%	2%
	Total	100%	100%	100%
	Extrapolated value	$1,099,200	$995,450	$771,905

Q11A	DID THE RANSOMWARE ATTACK RESULT IN A DISRUPTION IN PATIENT CARE?	FY2024	FY2023	FY2022
	Yes	70%	68%	67%
	No	25%	26%	30%
	Unsure	5%	6%	3%
	Total	100%	100%	100%

Q11B	IF YES, WHAT IMPACT DID THE RANSOMWARE ATTACK HAVE ON PATIENT CARE? (Please select all that apply)	FY2024	FY2023	FY2022
	An increase in mortality rate	29%	28%	24%
	Delays in procedures and tests have resulted in poor outcomes	61%	59%	64%
	Increase in complications from medical procedures	47%	44%	48%
	Increase in patients transferred or diverted to other facilities	52%	46%	50%
	Longer length of stay	58%	48%	59%
	Other (please specify)	5%	3%	3%
	Total	252%	228%	248%

Q12A	DID YOUR ORGANIZATION EVER EXPERIENCE A BEC/SPOOFING/IMPERSONATION ATTACK?	FY2024	FY2023	FY2022
	Yes	57%	54%	51%
	No (please skip to Q14a)	38%	41%	40%
	Unsure (please skip to Q14a)	5%	5%	9%
	Total	100%	100%	100%

Q12B	IF YES, HOW MANY BEC/SPOOFING/IMPERSONATION ATTACKS DID YOUR ORGANIZATION EXPERIENCE OVER THE PAST TWO YEARS?	FY2024	FY2023	FY2022
	One	53%	40%	49%
	Two to five	21%	24%	31%
	Six to 10	15%	19%	12%
	More than 10	11%	17%	8%
	Total	100%	100%	100%
	Extrapolated value	3.8	4.8	3.5

Q13A	DID THE BEC/SPOOFING/IMPERSONATION ATTACK RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?	FY2024	FY2023	FY2022
	Yes	65%	69%	67%
	No	31%	26%	30%
	Unsure	4%	5%	3%
	Total	100%	100%	100%

Q13B	IF YES, WHAT IMPACT DID THE BEC/ SPOOFING/IMPERSONATION ATTACK HAVE ON PATIENT CARE? (Please select all that apply)	FY2024	FY2023	FY2022
	An increase in mortality rate	24%	12%	21%
	Delays in procedures and tests have resulted in poor outcomes	69%	71%	60%
	Increase in complications from medical procedures	57%	56%	51%
	Increase in patients transferred or diverted to other facilities	50%	46%	45%
	Longer length of stay	52%	55%	48%
	Other (please specify)	4%	4%	2%
	Total	256%	244%	227%

Q14A	DID YOUR ORGANIZATION EVER EXPERIENCE ATTACKS AGAINST ITS SUPPLY CHAIN?	FY2024	FY2023	FY2022
	Yes	68%	64%	50%
	No (please skip to Q16a)	28%	30%	44%
	Unsure (please skip to Q16a)	4%	6%	6%
	Total	100%	100%	100%

Q14B	IF YES, HOW MANY SUPPLY CHAIN ATTACKS DID YOUR ORGANIZATION EXPERIENCE OVER THE PAST TWO YEARS?	FY2024	FY2023	FY2022
	One	46%	36%	44%
	Two to five	26%	33%	29%
	Six to 10	19%	21%	19%
	More than 10	9%	10%	8%
	Total	100%	100%	100%
	Extrapolated value	4.0	4.2	3.9

Q15A	DID THE SUPPLY CHAIN ATTACKS RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?	FY2024	FY2023	FY2022
	Yes	82%	77%	70%
	No	18%	18%	24%
	Unsure	0%	5%	6%
	Total	100%	100%	100%

Q15B	IF YES, WHAT IMPACT DID THE SUPPLY CHAIN ATTACKS HAVE ON PATIENT CARE? (Please select all that apply)	FY2024	FY2023	FY2022
	An increase in mortality rate	26%	21%	23%
	Delays in procedures and tests have resulted in poor outcomes	48%	50%	54%
	Increase in complications from medical procedures	51%	45%	48%
	Increase in patients transferred or diverted to other facilities	38%	39%	40%
	Longer length of stay	45%	48%	51%
	Other (please specify)	3%	4%	3%
	Total	211%	207%	219%

PART 2. PROTECTING THE CLOUD

Q16A	DID YOUR ORGANIZATION EVER EXPERIENCE A SUCCESSFUL CLOUD/ ACCOUNT COMPROMISE?	FY2024	FY2023	FY2022
	Yes	69%	63%	54%
	No (Please skip to Q18)	29%	33%	41%
	Unsure (Please skip to Q18)	2%	4%	5%
	Total	100%	100%	100%

Q16B	HOW MANY TIMES HAVE ATTACKERS COMPROMISED CLOUD-BASED USER ACCOUNTS WITHIN YOUR ORGANIZATION OVER THE PAST TWO YEARS?	FY2024	FY2023	FY2022
	Once	0%	0%	5%
	2 to 5	13%	12%	9%
	6 to 10	12%	14%	6%
	11 to 15	16%	10%	9%
	16 to 20	21%	21%	22%
	21 to 25	19%	19%	22%
	26 to 50	13%	16%	18%
	More than 50	6%	8%	9%
	Total	100%	100%	100%
	Extrapolated value	19.9	21.4	21.7

Q16C	WHICH CLOUD-BASED USER ACCOUNTS/COLLABORATION TOOLS WERE MOST ATTACKED IN YOUR ORGANIZATION? (Please select all that apply)	FY2024	FY2023
	Email	59%	49%
	Text messaging	61%	45%
	Zoom/Skype/Videoconferencing	56%	53%
	Teams/Slack/Office collaboration tools	47%	49%
	Project management tools	31%	53%
	OneDrive/DropBox/Document/file-sharing tools	47%	49%
	Application/system-generated email	23%	51%
	Virtual desktop infrastructure (VDI)	24%	
	Total	348%	349%

Q17A	DID THE CLOUD/ACCOUNT COMPROMISES RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?	FY2024	FY2023	FY2022
	Yes	57%	49%	64%
	No	34%	40%	32%
	Unsure	9%	11%	4%
	Total	100%	100%	100%

Q17B	IF YES, WHAT IMPACT DID THE CLOUD COMPROMISES HAVE ON PATIENT CARE? (Please select all that apply)	FY2024	FY2023	FY2022
	An increase in mortality rate	32%	29%	18%
	Delays in procedures and tests have resulted in poor outcomes	44%	47%	49%
	Increase in complications from medical procedures	56%	53%	51%
	Increase in patients transferred or diverted to other facilities	36%	37%	37%
	Longer length of stay	52%	48%	50%
	Other (please specify)	1%	3%	2%
	Total	221%	217%	207%

PART 3. DATA LOSS PROTECTION/EXFILTRATION

Q18	HOW MANY DATA LOSS AND EXFILTRATION INCIDENTS INVOLVING SENSITIVE AND CONFIDENTIAL HEALTHCARE DATA OCCURRED WITHIN YOUR ORGANIZATION OVER THE PAST TWO YEARS?	FY2024	FY2023
	Once	0%	8%
	2 to 5	8%	5%
	6 to 10	14%	12%
	11 to 15	25%	24%
	16 to 20	12%	10%
	21 to 25	25%	23%
	26 to 50	10%	13%
	More than 50	6%	5%
	Total	100%	100%
	Extrapolated value	20	19

Q19	WHAT WERE THE ROOT CAUSES OF THE DATA LOSS AND EXFILTRATION INCIDENT? (Please select all that apply)	FY2024
	Accidental data loss	26%
	Employee negligence because of not following policies	31%
	Privilege access abuse	20%
	Malicious insiders	15%
	Employee sends PII or PHI to an unintended recipient via email	21%
	Use of stolen credentials	11%
	Social engineering	13%
	Exploitation of vulnerabilities	9%
	Phishing	12%
	Uncertain	17%
	Total	175%

Q20A	DID THE DATA LOSS OR EXFILTRATION RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?	FY2024	FY2023
	Yes	51%	43%
	No (Please skip to Q21)	45%	51%
	Unsure (Please skip to Q21)	4%	6%
	Total	100%	100%

Q20B	IF YES, WHAT IMPACT DID THE DATA LOSS PROTECTION OR EXFILTRATION INCIDENT HAVE ON PATIENT CARE? (Please select all that apply)	FY2024	FY2023
	An increase in mortality rate	50%	46%
	Delays in procedures and tests have resulted in poor outcomes	37%	34%
	Increase in complications from medical procedures	34%	38%
	Increase in patients transferred or diverted to other facilities	33%	36%
	Longer length of stay	21%	24%
	Other (please specify)	3%	6%
	Total	178%	184%

Q21	WHAT SECURITY METHODS AND TECHNOLOGIES DOES YOUR ORGANIZATION USE TO REDUCE PHISHING AND OTHER EMAIL-BASED ATTACKS? (Please select all that apply)	FY2024
	Secure email gateway (SEG)	45%
	Domain-based Message Authentication (DMARC)	42%
	Email data loss prevention	39%
	Anti-virus/anti-malware	53%
	Multi-factor authentication	49%
	Patch & vulnerability management	52%
	Managed Security Service Provider (MSSP)	46%
	Firewalls	36%
	AI/ML	44%
	Threat intelligence	41%
	Other (please specify)	4%
	Total	451%

Q22	WHAT OTHER TECHNOLOGIES HAS YOUR ORGANIZATION IMPLEMENTED TO PREVENT IDENTITY RISK AND LATERAL MOVEMENT IN ITS NETWORK? (Please select all that apply)	FY2024
	Identity and access management (IAM)	56%
	Privileged access management (PAM)	61%
	Identity theft detection and response (ITDR)	40%
	Intrusion detection & prevention systems (IDPS)	35%
	User and entity behavior analytics (UEBA)	33%
	Alerts from SIEM to gain visibility	45%
	Endpoint protection	39%
	Rules-based DLP solution	45%
	Other (please specify)	2%
	Total	356%

Q23	WHAT SECURITY METHODS AND TECHNOLOGIES HAS YOUR ORGANIZATION IMPLEMENTED TO PREVENT DATA LOSS OR AN EXFILTRATION INCIDENT? (Please select all that apply)	FY2024
	Policy fine tuning to prevent data loss	23%
	Web security gateway	28%
	Cloud security tools	44%
	Web isolation technology	29%
	Encryption for data at rest	41%
	Encryption for data in transit	46%
	Unified data loss prevention platform covering multiple channels for email, web, network, endpoint and cloud	36%
	IT/IT security team triages incidents	25%
	Manual policy orchestration	29%
	Other (please specify)	3%
	Total	304%

Q24A	DOES YOUR ORGANIZATION TAKE STEPS TO ADDRESS THE RISK OF EMPLOYEES' LACK OF AWARENESS ABOUT CYBERSECURITY THREATS?	FY2024	FY2023	FY2022
	Yes	71%	65%	59%
	No	29%	30%	35%
	Unsure	0%	5%	6%
	Total	100%	100%	100%

Q24B	IF YES, WHAT STEPS DOES IT TAKE? (Please select all that apply)	FY2024	FY2023	FY2022
	Regular training and awareness programs	59%	57%	63%
	Simulations of phishing attacks	45%	40%	41%
	Monitoring of employees	53%	54%	59%
	Audits and assessments of areas most vulnerable to employees' lack of awareness	39%	43%	39%
	Include user's compliance with privacy and security policies in performance evaluations	34%	36%	35%
	Other (please specify)	5%	4%	3%
	Total	235%	234%	240%

Q25	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)	FY2024	FY2023
	1 or 2	11%	18%
	3 or 4	23%	33%
	5 or 6	20%	14%
	7 or 8	26%	16%
	9 or 10	20%	19%
	Total	100%	100%
	Extrapolated value	5.92	5.20

Q26	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)	FY2024	FY2023
	1 or 2	15%	15%
	3 or 4	23%	20%
	5 or 6	23%	26%
	7 or 8	24%	25%
	9 or 10	15%	14%
	Total	100%	100%
	Extrapolated value	5.52	5.56

Q27	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)	FY2024	FY2023
	1 or 2	11%	15%
	3 or 4	18%	17%
	5 or 6	23%	21%
	7 or 8	23%	25%
	9 or 10	25%	22%
	Total	100%	100%
	Extrapolated value	6.16	5.94

PART 4. AI AND MACHINE LEARNING IN HEALTHCARE

Q28	HAS YOUR ORGANIZATION ADOPTED AI? (Please select one choice only)	FY2024
	Yes, AI is embedded in cybersecurity	28%
	Yes, AI is embedded in both cybersecurity and patient care	26%
	No, but we plan to adopt AI in the future (please skip to Part 5)	26%
	We don’t have plans to adopt AI (please skip to Part 5)	20%
	Total	100%

Q29	THE DEPLOYMENT OF AI-BASED SECURITY TECHNOLOGIES WILL INCREASE THE PRODUCTIVITY OF OUR ORGANIZATION’S IT SECURITY PERSONNEL	FY2024
	Strongly disagree	21%
	Disagree	15%
	Unsure	9%
	Agree	25%
	Strongly Agree	30%
	Total	100%

Q30	AI SIMPLIFIES PATIENT CARE AND ADMINISTRATORS’ WORK BY PERFORMING TASKS THAT ARE TYPICALLY DONE BY HUMANS BUT IN LESS TIME AND COST	FY2024
	Strongly disagree	15%
	Disagree	16%
	Unsure	21%
	Agree	23%
	Strongly Agree	25%
	Total	100%

Q31	TO PROTECT EMAIL FROM EMPLOYEES' NEGLIGENCE AND ERROR, DOES YOUR ORGANIZATION USE AI AND MACHINE LEARNING TO UNDERSTAND HUMAN BEHAVIOR?	FY2024
	Yes	36%
	No (please skip to Q33)	64%
	Total	100%

Q32	IF YES, HOW IMPORTANT IS UNDERSTANDING HUMAN BEHAVIOR TO PROTECTING EMAIL? (From 1 = not important to 10 = very important)	FY2024
	1 or 2	8%
	3 or 4	15%
	5 or 6	21%
	7 or 8	23%
	9 or 10	33%
	Total	100%

Q33	HOW EFFECTIVE IS AI IN IMPROVING THE CYBERSECURITY POSTURE OF YOUR ORGANIZATION? (From 1 = not effective to 10 = very effective)	FY2024
	1 or 2	11%
	3 or 4	13%
	5 or 6	19%
	7 or 8	25%
	9 or 10	32%
	Total	100%

Q34	HOW DIFFICULT IS IT TO SAFEGUARD CONFIDENTIAL AND SENSITIVE PATIENT DATA USED IN YOUR ORGANIZATION'S AI? (From 1 = not difficult to 10 = very difficult)	FY2024
	1 or 2	5%
	3 or 4	9%
	5 or 6	23%
	7 or 8	30%
	9 or 10	33%
	Total	100%

Q35	WHICH OF THE FOLLOWING ARE CHALLENGES TO THE EFFECTIVENESS OF AI-BASED SECURITY TECHNOLOGIES USED BY YOUR ORGANIZATION TODAY? (Please select the top two factors)	FY2024
	AI tools/technology we need are not available	25%
	We can't apply AI-based controls that span across the entire enterprise	26%
	We can't create a unified view of AI users across the enterprise	4%
	There are errors and inaccuracies in AI decision rules	19%
	There are errors and inaccuracies in data inputs ingested by AI technology (engine)	32%
	There is a heavy reliance on legacy IT environments	23%
	There are Interoperability issues among AI technologies	32%
	There is a lack of mature and/or stable AI technologies	34%
	Other (please specify)	5%
	Total	200%

PART 5. CYBERATTACK EXPERIENCE

Q36	HOW MANY CYBERATTACKS HAS YOUR ORGANIZATION EXPERIENCED OVER THE PAST 12 MONTHS?	FY2024	FY2023	FY2022
	None (please skip to Part 6)	8%	12%	11%
	1 to 5	15%	13%	12%
	6 to 10	23%	21%	15%
	11 to 25	12%	11%	13%
	26 to 50	11%	9%	11%
	51 to 100	12%	18%	23%
	More than 100	19%	16%	15%
	Total	100%	100%	100%
	Extrapolated value	40.4	40.1	43.3

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

Q37	APPROXIMATELY, HOW MUCH WAS THE TOTAL COST FROM THE ONE MOST SIGNIFICANT CYBERSECURITY ATTACK?	FY2024	FY2023	FY2022
	Less than $10,000	0%	0%	0%
	$10,001 to $50,000	3%	0%	0%
	50,001 to $100,000	6%	7%	6%
	100,001 to $250,000	10%	13%	12%
	250,001 to $500,000	14%	18%	18%
	500,001 to $1,000,000	18%	14%	16%
	1,000,001 to $5,000,000	21%	19%	21%
	5,000,001 to $10,000,000	15%	11%	13%
	10,000,001 to $25,000,000	9%	15%	12%
	More than $25,000,000	4%	3%	2%
	Total	100%	100%	100%
	Extrapolated value	$4,740,400	$4,991,500	$4,429,000

Q38	**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)	FY2024	FY2023	FY 2022
	Remediation & technical support activities, including forensic investigations, incident response activities, help desk and delivery of services to patients	15.00	15.00	16.00
	Users' idle time and lost productivity because of downtime or system performance delays	21.00	23.00	25.00
	Disruption to normal healthcare operations because of system availability problems	31.00	26.00	23.00
	Damage or theft of IT assets and infrastructure	15.00	15.00	21.00
	Time required to ensure impact on patient care is corrected	18.00	21.00	15.00
	Total Points	100.00	100.00	100.00

PART 6. SECURITY SPENDING & INVESTMENT

Q39	**WHAT IS YOUR ORGANIZATION'S APPROXIMATE ANNUAL BUDGET FOR IT?**	FY2024	FY2023	FY2022
	Less than $1,000,000	0%	2%	0%
	1,000,000 to $5,000,000	4%	3%	2%
	5,000,001 to $10,000,000	9%	8%	6%
	10,000,001 to $25,000,000	11%	11%	10%
	25,000,001 to $50,000,000	20%	25%	17%
	$50,000,001 to $100,000,000	25%	23%	28%
	$100,000,000+	31%	25%	37%
	Cannot estimate	0%	3%	0%
	Total	100%	100%	100%
	Extrapolated value	$66,170,000	$59,258,000	$75,200,000

Q40	WHAT PERCENTAGE OF YOUR ORGANIZATION'S IT BUDGET IS DEDICATED TO INFORMATION SECURITY?	FY2024	FY2023	FY2022
	Less than 5%	4%	5%	3%
	5 to 10%	9%	8%	7%
	11 to 15%	19%	21%	23%
	16 to 20%	33%	37%	35%
	21 to 30%	25%	19%	21%
	More than 30%	10%	10%	11%
	Total	100%	100%	100%
	Extrapolated value	19%	18%	19%

PART 7. YOUR ROLE AND ORGANIZATION

D1	WHAT BEST DESCRIBES YOUR ORGANIZATION?	FY2024	FY2023	FY2022
	Public healthcare provider	21%	19%	19%
	Private healthcare provider	22%	20%	22%
	Healthcare insurer	19%	18%	13%
	Payer	8%	14%	15%
	Healthcare insurance	12%	11%	9%
	Life sciences	6%	5%	8%
	Biotech	4%	4%	5%
	Pharma	8%	9%	9%
	Total	100%	100%	100%

D2	WHAT ORGANIZATIONAL LEVEL BEST DESCRIBES YOUR CURRENT POSITION?	FY2024	FY2023	FY2022
	Senior Executive/VP	7%	8%	9%
	Director	10%	17%	16%
	Manager	27%	29%	23%
	Supervisor	25%	23%	14%
	Technician/Staff	26%	19%	33%
	Contractor	5%	4%	5%
	Other (please specify)	0%	0%	0%
	Total	100%	100%	100%

D3	CHECK THE PRIMARY PERSON YOU OR YOUR IT SECURITY LEADER REPORTS TO WITHIN THE ORGANIZATION	FY2024	FY2023	FY2022
	CEO/Executive Committee	7%	9%	8%
	Chief Information Officer	18%	19%	21%
	Chief Information Security Officer	21%	20%	19%
	Chief Risk Officer	8%	7%	6%
	Chief Security Officer	6%	5%	4%
	Chief Technology Officer	7%	8%	7%
	Compliance Officer	9%	8%	9%
	Data Center Management	8%	9%	10%
	Cloud Administration	13%	11%	12%
	Other (please specify)	3%	4%	4%
	Total	100%	100%	100%

D4	WHAT IS THE HEADCOUNT OF YOUR ORGANIZATION?	FY2024	FY2023	FY2022
	Less than 500	19%	18%	16%
	500 to 1,000	23%	21%	25%
	1,001 to 5,000	17%	18%	19%
	5,001 to 10,000	12%	10%	9%
	10,001 to 25,000	10%	12%	13%
	25,001 to 75,000	13%	14%	12%
	More than 75,000	6%	7%	6%
	Total	100%	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.

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.

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.