

proofpoint®

REPORT

2026 Study on Cyber Insecurity in Healthcare

The Cost and Impact on
Patient Safety and Care



Table of contents

- 03 Key Findings
- 07 Part 1. Executive Summary
- 14 Part 2. Detailed Analysis
- 34 Part 3. Methodology
- 37 Part 4. Caveats to this report
- 38 Part 5. Appendix with the detailed audited findings

Key Findings

More Attacks,
Higher Costs,
Greater
Disruption

97%

of organizations experienced at least one cyberattack, averaging 51 in the past 12 months, up from 43 in 2025



74%

report disruption to patient care



\$4.2M

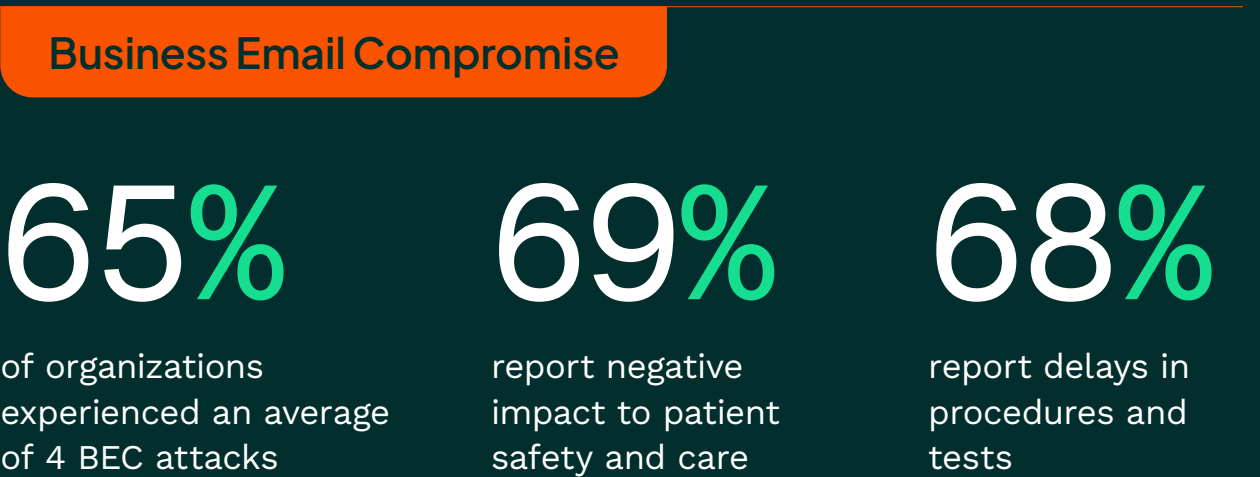
average total cost of the most expensive cyberattack, up from \$3.9M in 2025



\$1.39M

cost of disruption to healthcare operations, which was the single most expensive cost category

Cyberattacks
Are Directly
Affecting
Patient Care



AI Adoption Is Accelerating Faster Than Governance

✦✦ 45%
have embedded AI

24%
in cybersecurity operations

and

21%
in both cybersecurity and patient care



But gaps remain:

60%
lack controls governing sensitive data used in AI systems

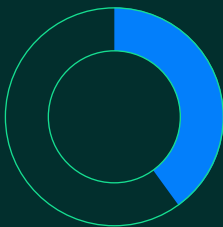
Only 42%
use security measures designed for AI usage

Only 32%
have full visibility into unsanctioned AI tool usage

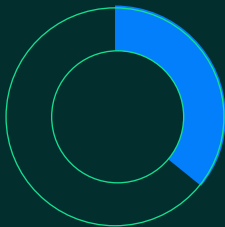
Top AI-specific risks:



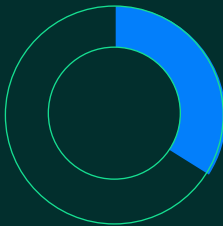
40%
Supply chain risk from AI vendors



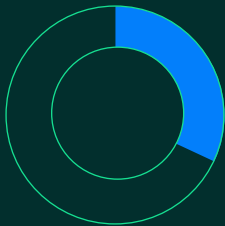
36%
Data leakage through prompts



34%
AI-generated phishing and social engineering



32%
Malicious or biased outputs affecting care decisions



Insider Risk
Remains a
Patient Safety
Threat



of organizations

experienced **21 data loss or exfiltration incidents**, on average, involving sensitive health information



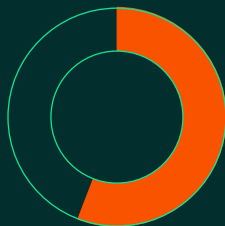
54%

say these incidents impacted patient care



56%

report increased mortality rates

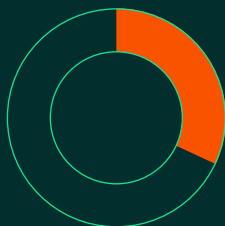


Leading causes of data loss:



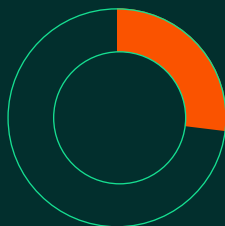
32%

Employee negligence



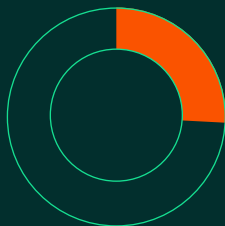
27%

Privileged access abuse



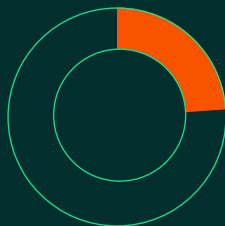
26%

Accidental data loss



24%

AI agents without guardrails



Security awareness programs remain essential



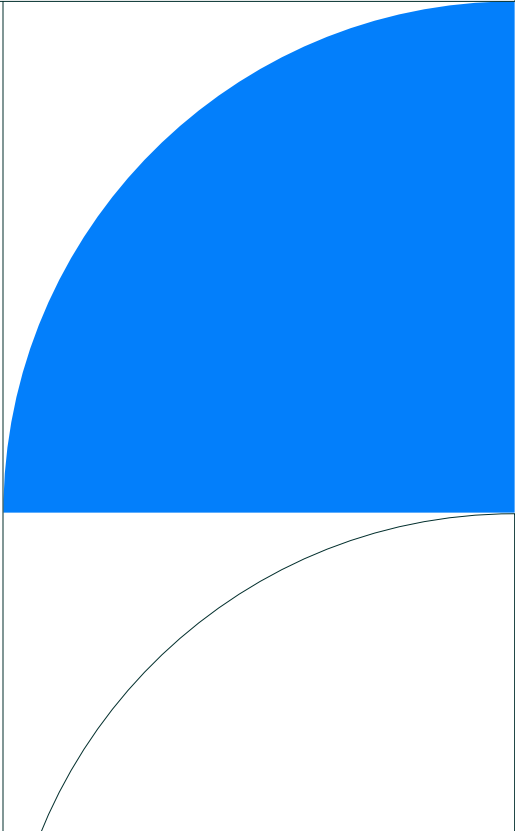
75%

are taking steps to address employee cybersecurity awareness



36%

educate employees about AI-related threats (e.g., deepfakes, AI-generated phishing)



97%

of organizations experienced an average number of 51 cyberattacks in the past 12 months

74%

reported disruption to patient care

\$4.2M

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

PART 1: EXECUTIVE SUMMARY

2026 Study on Cyber Insecurity in Healthcare:

The Cost and Impact on Patient Safety and Care

Cybersecurity incidents are increasingly disrupting clinical operations, consuming organizational resources and affecting patient care delivery.

According to the research, 97 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 51, an 8-point increase from 43 in 2025.

This fifth annual report was conducted to determine the healthcare industry’s effectiveness in reducing human-targeted cybersecurity risks and disruptions to patient care. With sponsorship from Proofpoint, Ponemon Institute surveyed 705 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.

The cyberattacks analyzed that took place over a two-year period in this research are cloud/account compromises, supply chain attacks, ransomware and business email compromise (BEC)/spoofing/impersonation. Among the organizations that experienced the four types of cyberattacks, an average of 74 percent reported disruption to patient care, a 2-point increase from 72 percent in 2025.

Cyberattack costs and consequences

Cyberattacks are increasing in frequency, cost and operational impact. We asked the 97 percent of respondents that had at least one cyberattack 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 \$4.2 million, an increase from \$3.9 million in 2025. This includes all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunities.

Healthcare organizations report that the greatest impact comes from operational disruption, downtime and the effort required to restore patient services. These findings underscore the growing importance of cyber resilience and organizations’ ability to maintain and restore clinical operations following a cyberattack.

The following is a breakdown of the five cybersecurity cost categories for the single most expensive cyberattack as well as their average cost:

- **Disruption to normal healthcare operations** cost an average of \$1,387,518 in 2026, **an increase** from \$1,210,172 in 2025. Costs stemmed from system availability problems, which continue to be the most expensive consequence from the cyberattack.
- **Users’ idle time and lost productivity** cost an average of \$1,051,150 in 2026, **an increase** from \$858,832 in 2025. These costs were due to downtime or system performance delays.
- **The cost of the time required to ensure the impact on patient care increased** to \$714,782 in 2026 from \$702,680 in 2025.
- **The damage or theft of IT assets and infrastructure** is \$546,598 in 2026, **a decrease** from \$624,605 in 2025.
- **Remediation and technical support activities**, including forensic investigations, incident response activities, help desk and delivery of services to patients is \$504,522 in 2026, **a slight decrease** from \$507,491 in 2025.

AI adoption is outpacing governance

Healthcare organizations are rapidly adopting AI technologies, but governance, visibility and security controls are lagging behind.

This year’s research takes a deeper look into the impact AI is having on cybersecurity in healthcare. As organizations increasingly adopt AI to improve operational efficiency, support patient care and enhance cybersecurity programs, they also are introducing new risks related to data protection, governance, visibility and third-party dependencies.

AI has become, or will become, a part of patient care and prevention of cyberattacks in most healthcare organizations. Forty-five percent of respondents say their organizations have embedded AI in cybersecurity (24 percent) or embedded in both cybersecurity and patient care (21 percent). Thirty percent plan to adopt AI in the future. Twenty-five percent say there are no plans to adopt AI.

Of the 45 percent of respondents currently using AI, the tasks and applications most often used are administrative automation (63 percent), medical imaging and diagnostics (62 percent) and virtual nursing/patient monitoring (48 percent).

60%

of healthcare organizations do not have controls in place to govern sensitive data use in AI systems

79%

respondents say they have or eventually will move clinical applications to the cloud

The AI-specific risk of greatest concern is supply chain risk from AI vendors (40 percent of respondents). Other risks of most concern are data leakage via prompts (36 percent) and AI-generated phishing/social engineering (34 percent). Only 14 percent of respondents say inadequate privacy protections are a serious risk, and only 11 percent say non-compliant tools are a serious risk.

Only 42 percent of respondents say their organizations use security measures to protect AI systems, agents and generative AI usage. The measures most often used are AI data governance and access controls (50 percent of respondents), AI data protection and data loss prevention (DLP) (45 percent of respondents) and AI usage discovery and visibility controls (33 percent of respondents).

Most organizations (60 percent) do not have controls in place to govern sensitive data used in AI systems. Of the 40 percent that have controls, strong encryption and data access controls for AI training is the number one control (52 percent) followed by professionals monitoring all AI outputs to prevent mistakes and access controls (both 46 percent).

Interoperability issues among AI technologies continue to be the top challenge to the effectiveness of AI-based security technologies (32 percent of respondents). However, errors and inaccuracies in AI decision rules increased significantly from 21 percent of respondents in 2025 to 30 percent in 2026. Only 29 percent of respondents say the lack of mature and/or stable AI technologies is a challenge.

Seventy-four percent of organizations have either full visibility into employees’ use of unsanctioned AI tools (32 percent) or partial (42 percent). Forty-six percent of respondents use generative AI tools approved or unapproved with governance (23 percent) or without governance (23 percent).

Securing clinical operations in the cloud

For the second year, the research includes healthcare organizations’ plans to secure clinical operations in the cloud.

More organizations are moving clinical applications to the cloud. In this year’s research, 35 percent of respondents say their organizations have moved clinical applications to the cloud, an increase from 30 percent in 2025. In 2026, 61 percent of respondents say their organizations are very or highly effective in securing clinical applications in the cloud, a significant increase from 54 percent in 2025.

76%

of organizations experienced 20 cloud/account compromises, on average

\$1.1M

Average total cost for the highest ransom payment



Concerns about BEC/spoofing/impersonation attacks increased, 48% (2026) vs. 40% (2025)

Forty-four percent say their organizations will move clinical applications to the cloud in the next six months (12 percent), within the next year (9 percent), in the next one to two years (14 percent) or eventually (9 percent). This accelerating shift toward cloud-hosted clinical systems underscores the urgency of addressing cloud/account compromise risks, given the potential impact on patient care and service continuity.

The cyberattack landscape

The report analyzes four types of cyberattacks that occurred over the past two years and their impact on healthcare organizations, patient safety and patient care delivery.

For the fifth consecutive year frequent attacks against the cloud make it the top cybersecurity threat and concern. Seventy-six percent say their organizations have experienced an average of 20 cloud/account compromises in 2026, an increase from 72 percent in 2025.

Cloud/account compromises remain healthcare’s most significant cybersecurity concern, an increase from 49 percent of respondents in 2025 to 54 percent in 2026.

Supply chain attacks increase. Fifty percent of respondents say their organizations experienced an attack against their supply chain, a significant increase from 44 percent in 2025. Of these organizations, on average they experienced four successful supply chain attacks in the past two years.

Fewer organizations are paying a ransom (31 percent vs. 33 percent in 2025) and the average amount decreased slightly. The average costliest ransom paid was \$1.1 million, down from \$1.2 million in 2025. In the past two years, organizations that had ransomware attacks (63 percent) experienced an average of 5 such attacks.

Awareness about BEC/spoofing/impersonation attacks is growing. Concerns about these attacks have increased significantly from 40 percent in 2025 to 48 percent in 2026. Sixty-five percent of respondents say their organizations experienced BEC attacks, up from 62 percent in 2025, and had an average of four attacks in the past two years.

From breach to bedside: the persistent link between cyberattacks and patient safety

The impact of cyberattacks increasingly extends beyond technology systems and into clinical operations, care delivery and patient outcomes.

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 74 percent report disruption to patient care, a slight increase from 72 percent in 2025.

Table 1. Percentage of poor outcomes for 4 types of cyberattacks

As shown in Table 1, an average of 53 percent report poor patient outcomes due to increases in medical procedure complications. An average of 52 percent saw an increase in a longer length of stay and delays in tests and procedures.

	Increased complications from medical procedures	Longer length of stay	Delay in tests/ procedures	Increase in patients transferred or diverted to other facilities	Increase in mortality rates
Ransomware	49%	70%	53%	51%	25%
BEC	52%	50%	68%	44%	26%
Supply Chain	53%	39%	47%	30%	35%
Cloud/Account Compromise	59%	50%	40%	44%	35%
2026 Average Percentage	53%	52%	52%	39%	30%



More organizations in this year’s research had a supply chain attack, 50% (2026) vs. 44% (2025)

90%

Say it disrupted patient care

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

- **Supply chain attacks continue to be the most likely to affect patient care.** More organizations in this year’s research had a supply chain attack (50 percent in 2026 vs. 44 percent in 2025). Ninety percent of those respondents say it disrupted patient care, an increase from 87 percent in 2025. Patients were primarily impacted by an increase in complications from medical procedures (53 percent). Mortality rates increased from 32 percent in 2025 to 35 percent in 2026.
- **BEC/spoofing/impersonation attacks cause delays in procedures and tests.** Sixty-five percent of respondents say their organizations experienced a BEC/spoofing/impersonation incident and had an average of four attacks. Of these respondents, 69 percent say a BEC/spoofing/impersonation attack against their organizations disrupted patient care. Sixty-eight percent of respondents say the attacks caused delays in procedures and tests that have resulted in poor outcomes and 52 percent say it increased complications from medical procedures.
- **Ransomware attacks cause delays in patient care.** Sixty-three percent of respondents say their organizations experienced an average of 5 successful ransomware attacks. Seventy-two percent of respondents say ransomware attacks had a negative impact on patient care, an increase from 67 percent in 2025. Of these respondents, 70 percent say it resulted in longer lengths of stay, which affects organizations’ ability to care for patients. Fifty-three percent say it resulted in delays in procedures and tests that resulted in a disruption to patient care.

58%

report attacks against Teams, Slack and Office platforms, up from 43% in 2025

- **Cloud-based user accounts/collaboration tools that enable productivity are most often attacked.** Seventy-six percent of respondents say their organizations experienced an average of 20 cloud/account compromises. In this year’s study, 65 percent say the cloud/account compromises resulted in disruption in patient care, an increase from 61 percent in 2025.

Fifty-nine percent say cloud/account compromises increased complications from medical procedures and 50 percent say it resulted in longer length of stay. The tools most often attacked are text messaging (64 percent) and Zoom/Skype/Videoconferencing (56 percent). Attacks against Teams/Slack/Office increased significantly from 43 percent of respondents in 2025 to 58 percent in 2026.

Human risk and data loss continue to threaten patient care

Employee mistakes, misuse of privileged access and data handling errors continue to contribute to security incidents, data loss and disruptions to patient care. This year’s findings suggest organizations must also address human behavior, awareness, governance and insider risk to strengthen their cybersecurity posture and reduce the impact of cyber incidents.

- **The top barrier to achieving a strong cybersecurity posture continues to be a lack of in-house expertise.** Forty-six percent of respondents cite insufficient in-house expertise, while 42 percent point to insufficient budget, a significant increase from 37 percent in 2025.

Although annual IT budgets increased from \$65 million in 2025 to \$69 million in 2026, many organizations continue to report resource constraints that limit their ability to strengthen cybersecurity programs. Of that \$69 million, 22 percent is allocated to information security.

- **Negligent employees pose significant risk.** Ninety-seven percent of organizations in this research had at least two data loss or exfiltration incidents involving sensitive and confidential healthcare data in the past two years. Employee negligence because of not following policies (32 percent of respondents), privileged access abuse (27 percent of respondents) and accidental data loss (26 percent of respondents) are the leading causes of the incident.
- **Data loss or exfiltration disrupts patient care and can increase mortality rates.** On average, organizations experienced 21 such incidents in the past two years and 54 percent of respondents say they impacted patient care. Of these respondents, 56 percent say it increased the mortality rate, 35 percent say it increased complications from medical procedures and 34 percent say it caused delays in procedures and tests that resulted in poor outcomes.

97%

Of organizations had at least 2 data loss or exfiltration incidents

21 Average number of such incidents

54% Say they impacted patient care

Of this group:

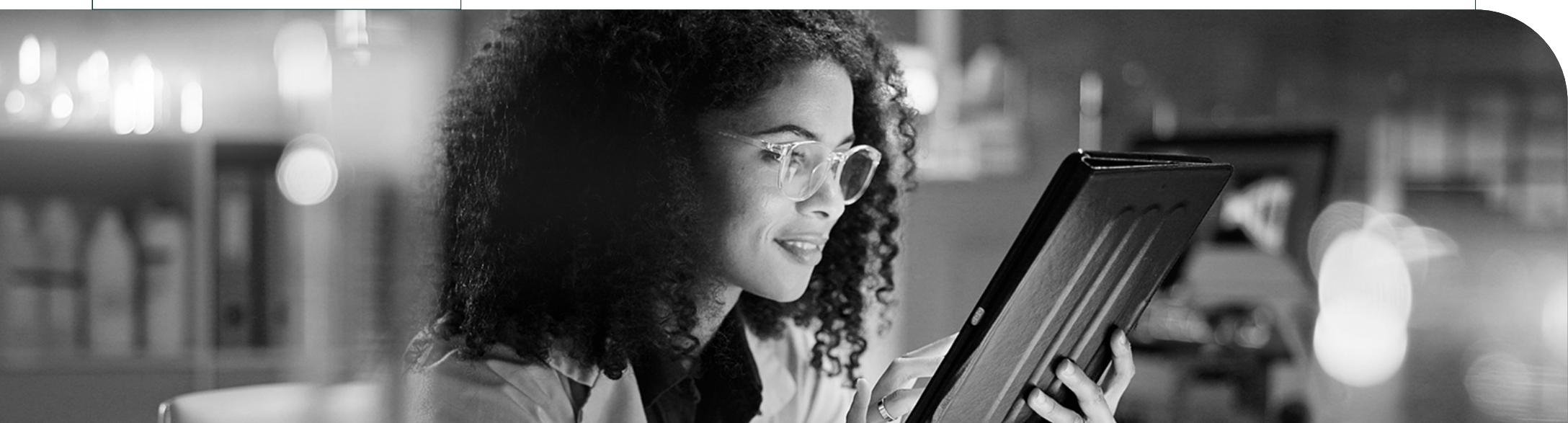
56%

Say these incidents increased mortality rates

- **More organizations are using simulations of phishing attacks to increase employees' awareness of cybersecurity threats.** Seventy-five percent of respondents in 2026 are taking steps to address the risk of employees' lack of awareness about cybersecurity threats. While regular training and awareness programs are still the number one step taken (65 percent), simulations of phishing attacks increased significantly from 47 percent of respondents in 2025 to 56 percent of respondents in 2026.

Thirty-six percent specifically educate employees about AI-related threats such as deepfakes and AI-generated phishing. Sixty-four percent of respondents rate the importance of understanding human behavior to protecting email as high or very high.

- **Anti-virus/anti-malware is the number one technology to reduce phishing and other email-based attacks; however, the use of AI/ML increased significantly.** Fifty-four percent of respondents say anti-virus/anti-malware is used to reduce phishing and other email-based attacks. Forty-seven percent of respondents say AI/ML is used, an increase from 41 percent in 2025 and email data loss prevention increased from 36 percent to 41 percent in 2026.



Cybersecurity incidents are increasingly becoming patient care events and multimillion-dollar operational disruptions. The healthcare organizations that will be most successful in the years ahead will be those that combine cyber resilience, identity security, human risk management, supply chain security and AI governance into a unified strategy focused on protecting both operations and patient outcomes.

PART 2

Detailed Analysis

In this section, we provide a deeper dive into the fifth annual findings. When applicable, this year's results are compared to previous studies. The objective of this comparison is to identify key trends and important changes in the healthcare cybersecurity landscape. Complete audited findings are presented in the Appendix of the report. The report is organized according to the following topics:

- Cybersecurity threats in healthcare: cloud/account compromise, ransomware, supply chain and 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 BEC/spoofing/impersonation

Figure 1. Cloud account compromises, Insecure mobile apps (eHealth) and insecure medical devices are considered the greatest cyber threats to healthcare organizations.

Respondents were asked to select the threats of greatest concern. As shown in Figure 1, concerns about cloud/account compromises increased from 49 percent of respondents in 2025 to 54 percent of respondents in 2026. Organizations are less worried about Employee negligence or error, a decrease from 47 percent in 2025 to 41 percent of respondents in 2026 and supply chain risks, a decrease from 42 percent in 2025 to 37 percent of respondents in 2026.

Six choices permitted

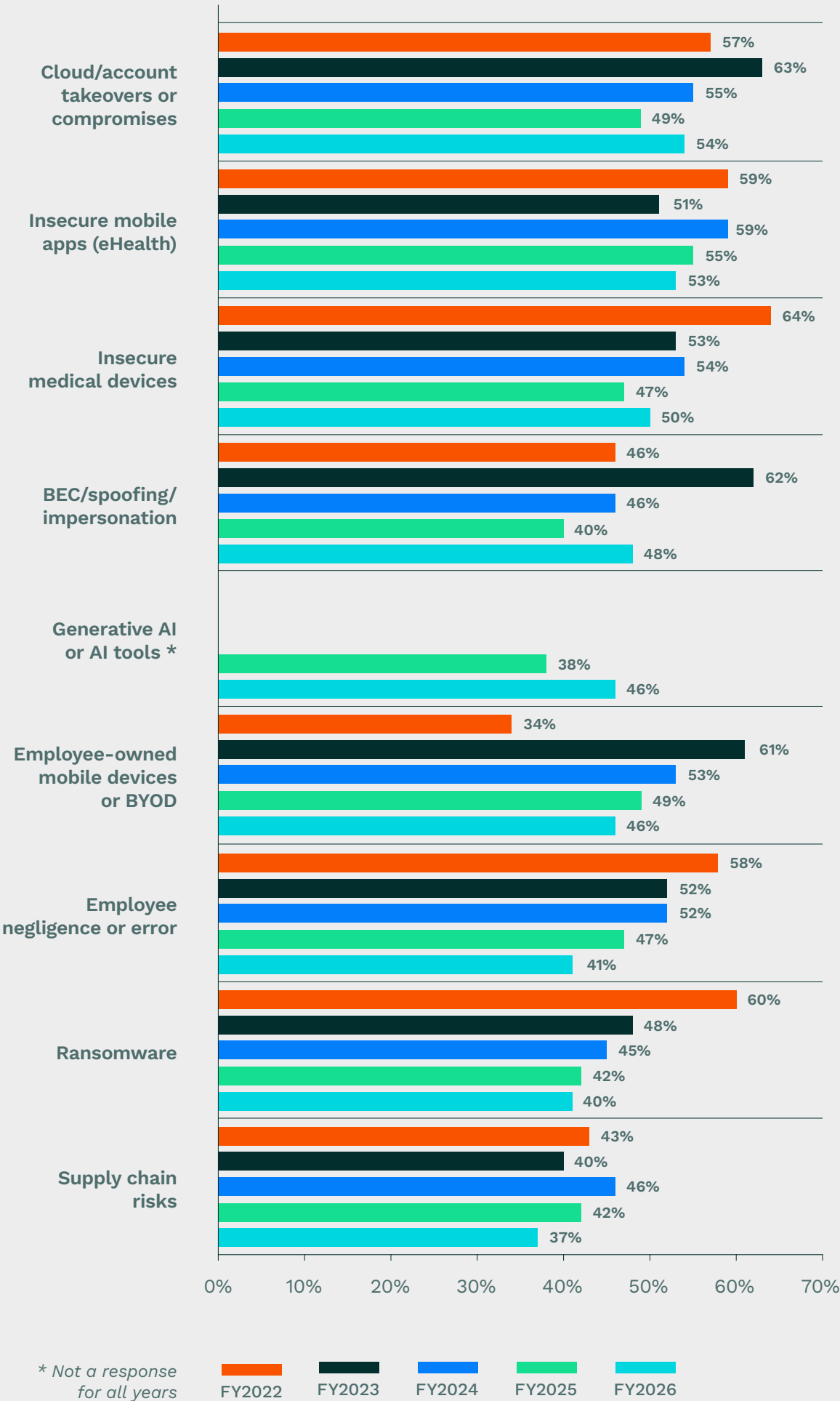


Figure 2. Healthcare organizations continue to be more prone to successful cloud/account compromises and BEC/spoofing/impersonation attacks.

Figure 2 presents the percentage of organizations that experienced four different types of cyberattacks. For the third year, more organizations say they have experienced a cloud/account compromise (69 percent in 2024 vs 72 percent in 2025 vs.76 percent in 2026).

BEC/spoofing/impersonation attacks increased from 62 percent in 2025 to 65 percent in 2026. Sixty-three percent of organizations had a ransomware attack. Supply chain attacks increased significantly from 44 percent to 50 percent in 2026.

Yes responses presented

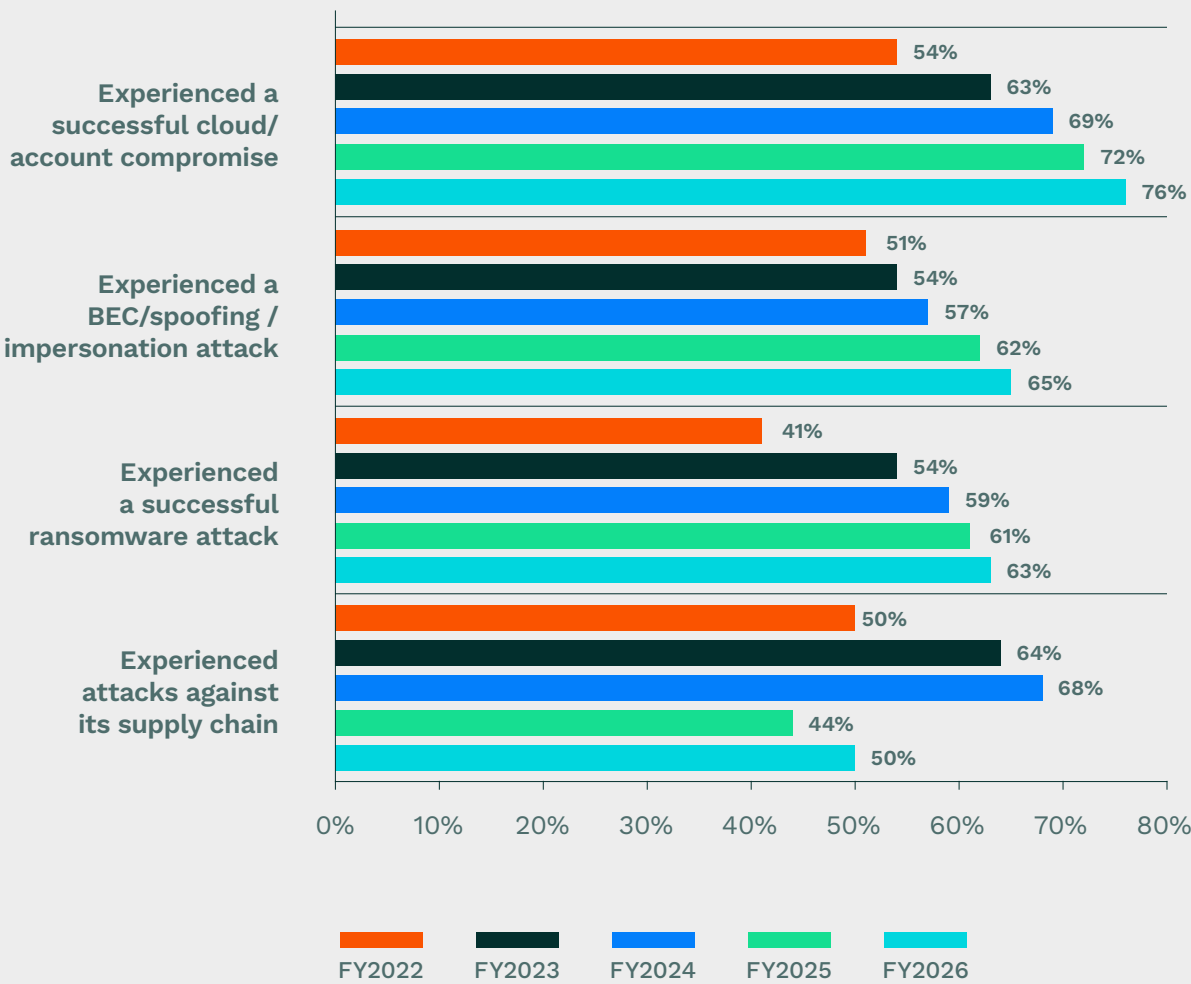


Figure 3. By far, the most cyberattacks involved cloud-based user accounts.

Responding organizations that experienced one of the four types of cyberattacks were asked about the frequency of those attacks over the past two years. Figure 3 shows the average number of the four cyberattacks. Organizations experienced an average of 20 attacks against the cloud in 2026, which explains the previous finding that most organizations believe they pose the greatest concern. In contrast, only an average of 5 ransomware attacks, 4 supply chain attacks and 4 BEC/spoofing/impersonation attacks were experienced in the past two years

Extrapolated averages presented

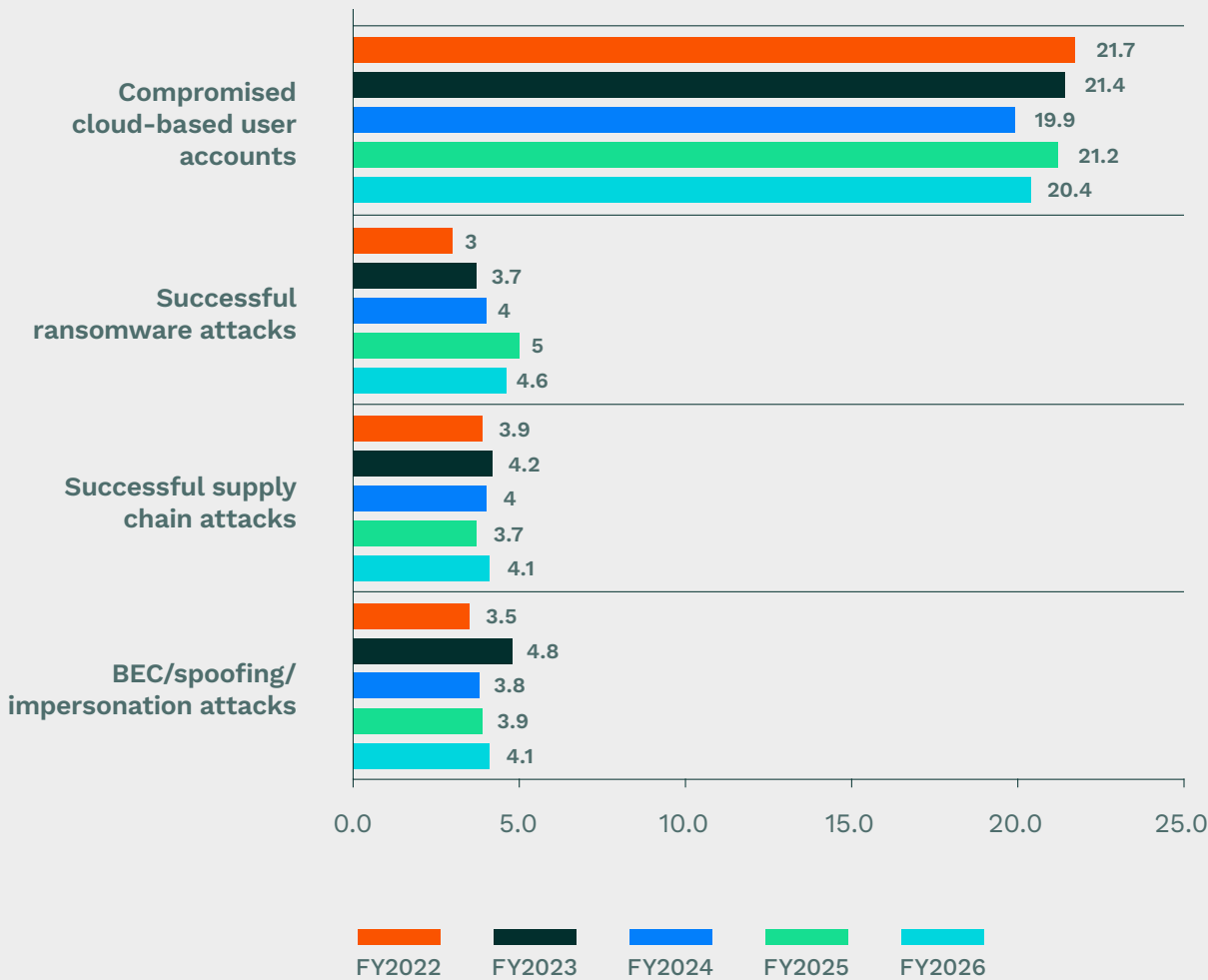


Figure 4. Text messaging, Teams/Slack/Office collaboration tools and Zoom/Skype/Videoconferencing were the most attacked cloud-based user accounts/collaboration tools.

Seventy-six 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 4, cloud-based user accounts/collaboration tools that enable productivity were most often attacked. The tool most often attacked continues to be text messaging (64 percent of respondents).

However, attacks on Teams/Slack/Office increased significantly from 43 percent to 58 percent of respondents. Fifty-six percent of respondents say Zoom/Skype/Videoconferencing is the third greatest target. Attacks on email accounts increased from 45 percent in 2025 to 50 percent and is one of the top four most targeted collaboration tools.

More than one response permitted

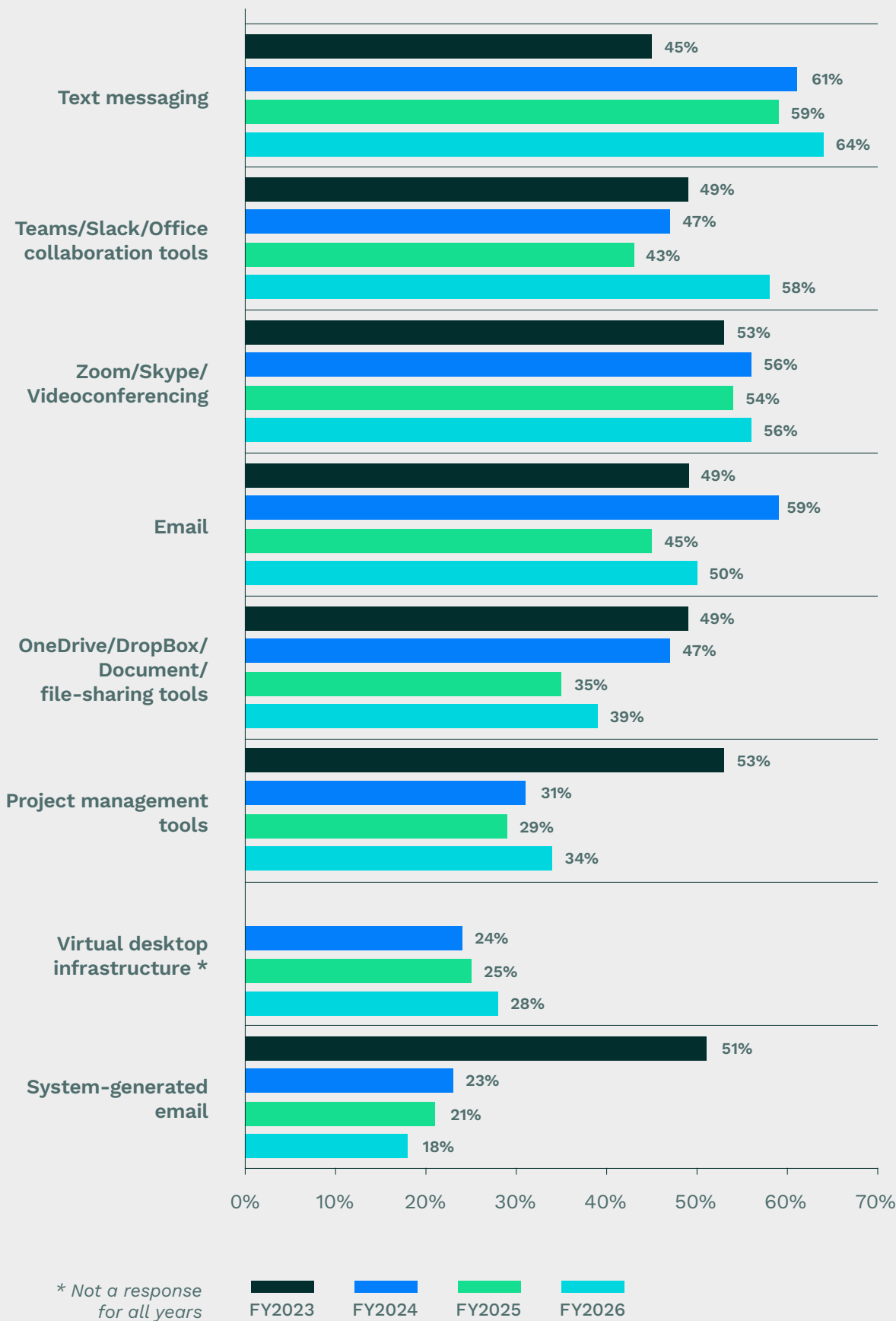


Figure 5. For the second time, this year’s study examined plans to secure clinical operations in the cloud.

As shown in Figure 5, 35 percent of respondents say their organizations have moved clinical applications to the cloud. Of this group, 61 percent, an increase from 54 percent, rate their ability to secure clinical applications in the cloud as very effective.

Forty-four percent say their organizations will move clinical applications to the cloud in the next six months (12 percent) within the next year (9 percent), in the next one to two years (14 percent) or eventually (9 percent). This accelerating shift toward cloud-hosted clinical systems underscores the urgency of addressing cloud/account compromise risks, given the potential impact on patient care and service continuity.

One choice permitted

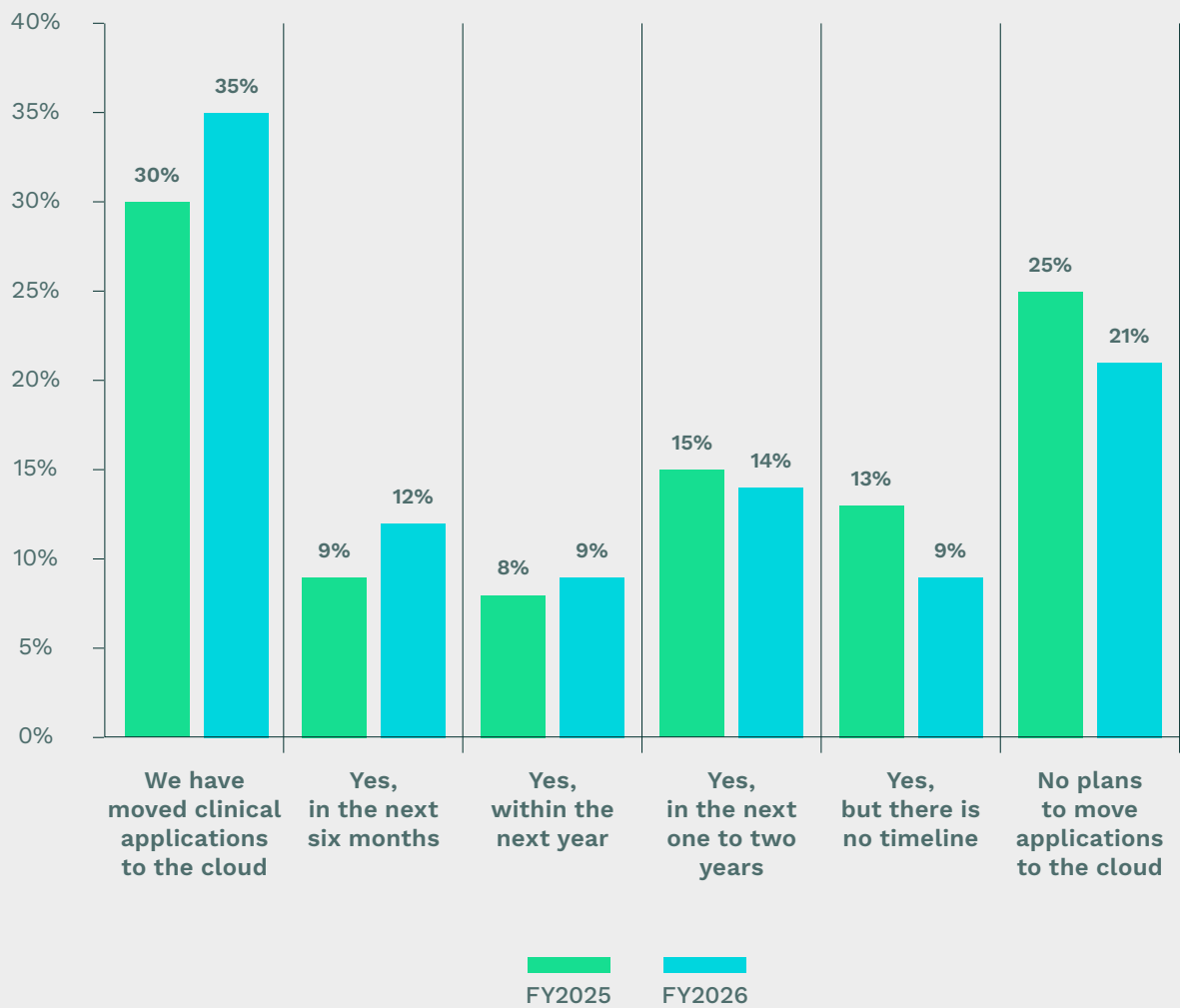
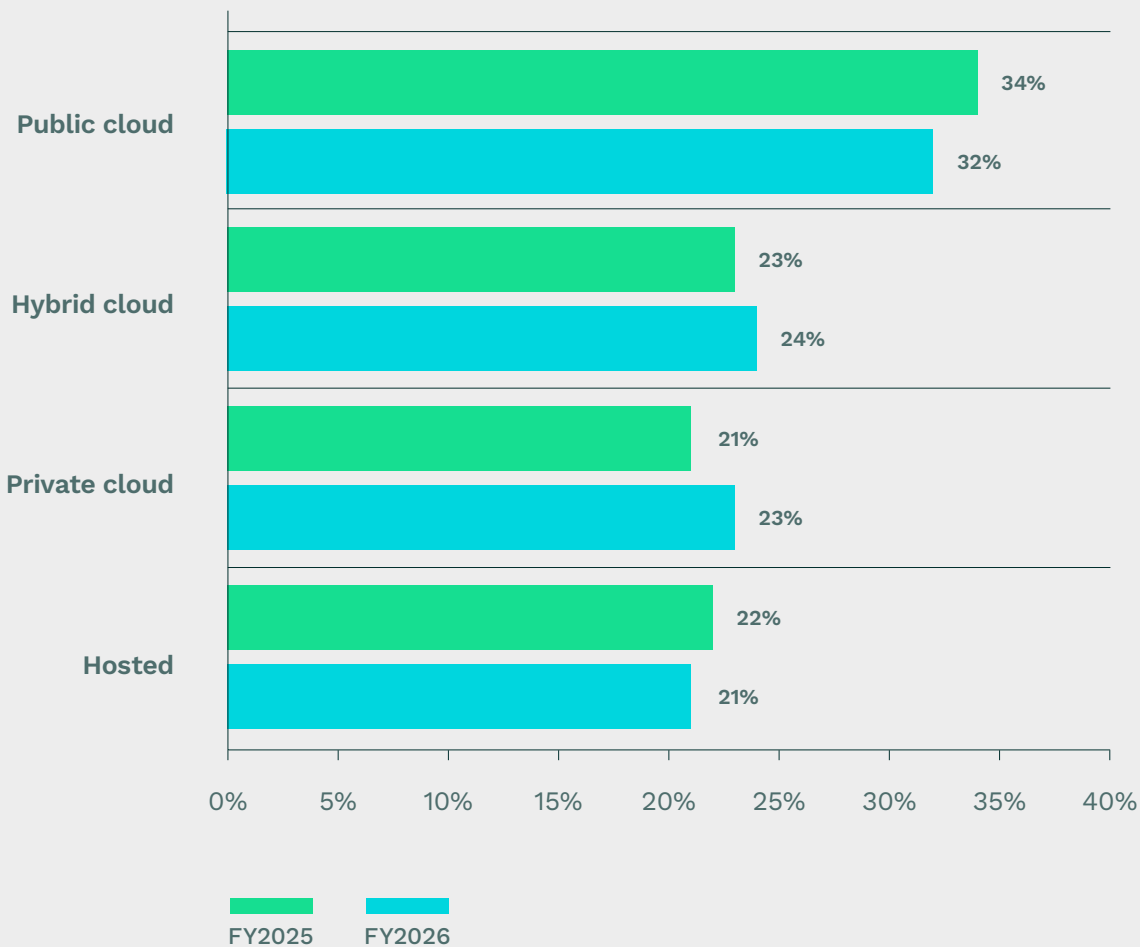


Figure 6. The cloud environment most favored for clinical applications is the public cloud.

As shown in Figure 6, 32 percent of organizations say clinical applications will be moved to the public cloud. This includes 35 percent that have already migrated and 44 percent that are planning to do so.

One choice permitted



The impact of cyberattacks on patient care

Figure 7. Cyberattacks continue to disrupt patient care, increasing the risk to patients.

Among the organizations that suffered the four types of attacks in the study, an average of 74 percent reported disruption to patient care. Specifically, attacks against the supply chain continue to have the most impact on patient care. Figure 7 shows the four types of cyberattacks featured in this research and the percentage of respondents who say it impacted patient safety and delivery of care.

Fifty percent of respondents say their organizations had a supply chain attack. Of these respondents, 90 percent say it resulted in a disruption in patient care, an increase from 87 percent in 2025 and 82 percent in 2024.

Sixty-three percent say their organizations had a ransomware attack, and 72 percent of these respondents say it disrupted patient care. Seventy-six percent of organizations had cloud/account compromises, which are becoming more impactful on patient care, increasing from 61 percent in 2025 to 65 percent in 2026. Sixty-five percent of organizations had a BEC/spoofing/impersonation attack, and 69 percent of respondents say it impacted patient care.

Yes responses presented

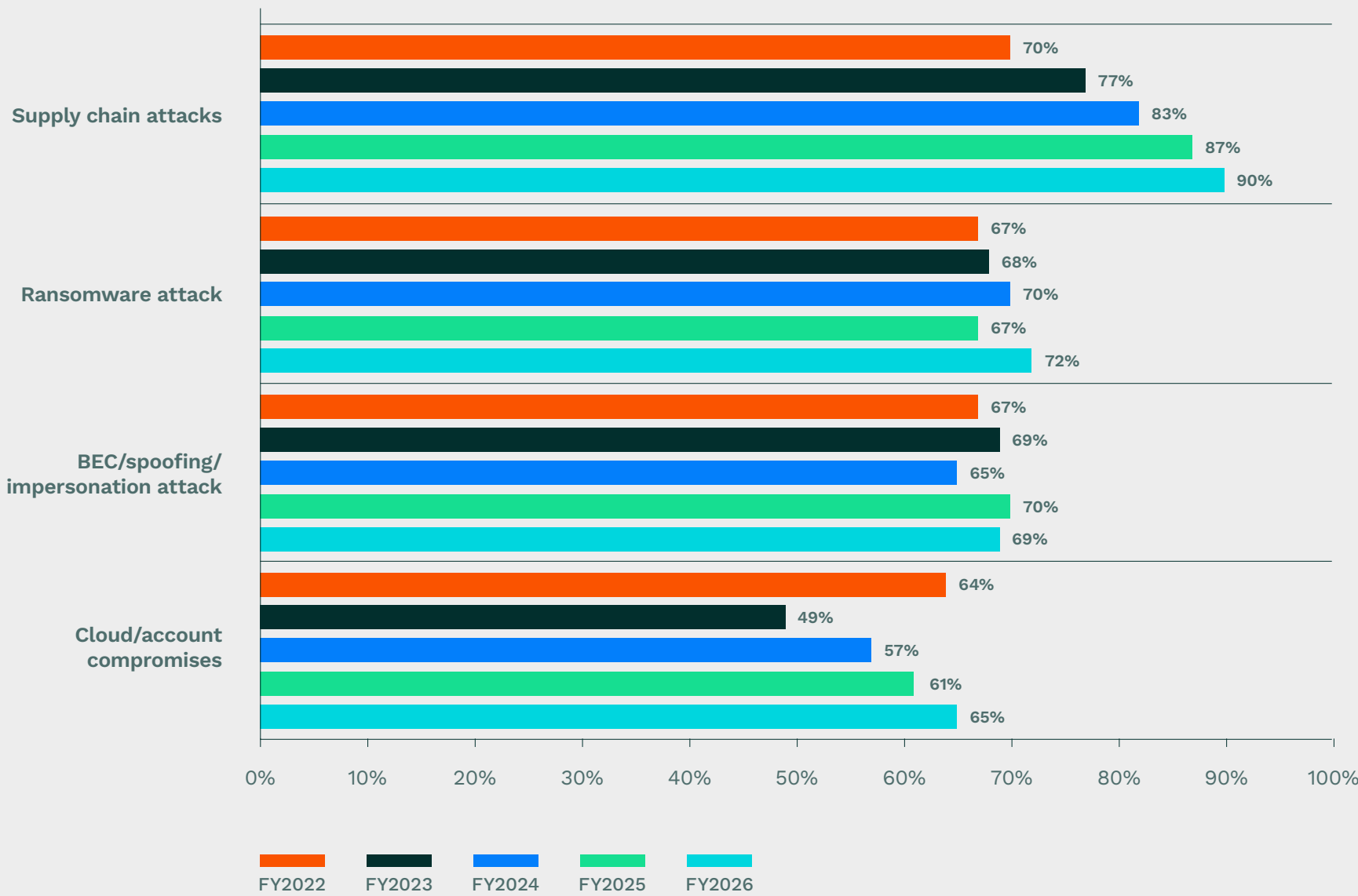
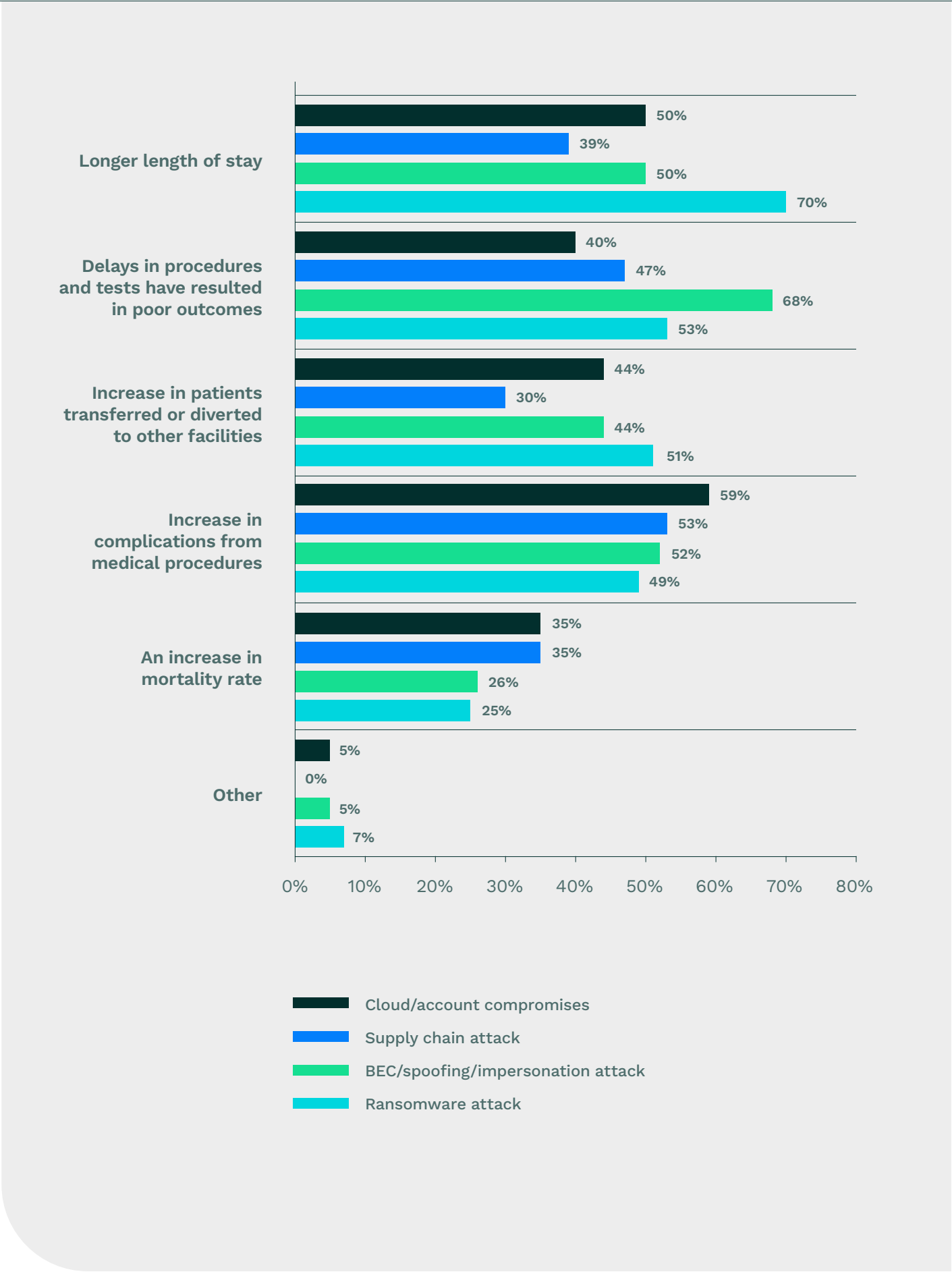


Figure 8. Ransomware attacks continue to be the most likely to result in prolonged patient length of stay, due to widespread disruption to clinical systems and care delivery.

According to Figure 8, 70 percent of respondents say ransomware attacks have resulted in longer lengths of stay. This is followed by 68 percent who say BEC/spoofing/impersonation attacks have caused delays in procedures and tests and have resulted in poor outcomes. Cloud/account compromises and supply chain attacks are most likely to result in an increase in mortality rate (both 35 percent).

More than one response permitted



The cost of cyber insecurity

Table 2. System availability problems and downtime continue to be the most significant financial consequences from a cybersecurity compromise.

Table 2 shows the five average costs of a healthcare cybersecurity compromise. According to the research, 97 percent of respondents say their organizations experienced at least one cyberattack in the past 12 months. The average number of attacks was 51. The average total cost for the **single most expensive cyberattack was \$4,204,600**, an increase from \$3,903,780 in 2025. This includes all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunities.

The average cost of damage or theft of IT assets and infrastructure continues to decrease. Respondents estimate that the average highest cost caused by damage or theft of IT assets and infrastructure decreased from \$624,605 in 2025 to \$546,598 in 2026.

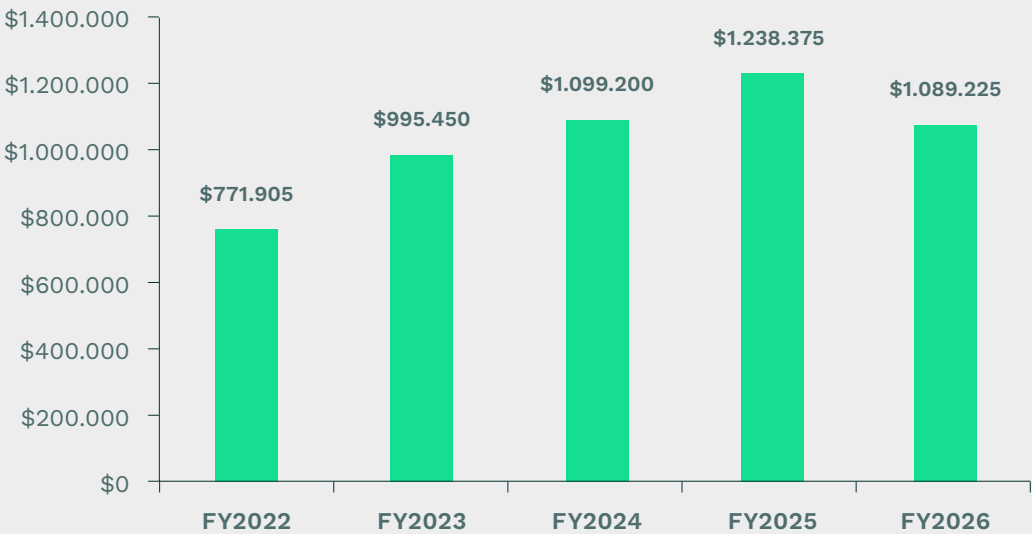
The following costs increased. Disruption to normal healthcare operations because of system availability problems increased from \$1,210,172 in 2025 to \$1,387,518 in 2026. The cost due to users’ idle time and lost productivity because of downtime or system performance delays increased from an average of \$858,832 in 2025 to \$1,051,150 in 2026. The time required to ensure the impact on patient care is corrected increased from \$702,680 in 2025 to \$714,782 in 2026.

Table 2. Five average costs of a healthcare cybersecurity compromise	2026 Average cost	2025 Average cost	2024 Average cost	2023 Average cost
Disruption to normal healthcare operations because of system availability problems	\$1,387,518	\$1,210,172	\$1,469,524	\$1,297,790
Users’ idle time and lost productivity because of downtime or system performance delays	\$1,051,150	\$858,832	\$995,484	\$1,148,045
Time required to ensure impact on patient care is corrected	\$714,782	\$702,680	\$853,272	\$1,048,215
Damage or theft of IT assets and infrastructure	\$546,598	\$624,605	\$711,060	\$748,725
Remediation & technical support activities, including forensic investigations, incident response activities, help desk and delivery of services to patients	\$504,522	\$507,491	\$711,060	\$748,725
Total	\$4,204,600	\$3,903,780	\$4,740,400	\$4,991,500

Figure 9. Healthcare organizations are making fewer and lower ransomware payments.

Sixty-three percent of respondents say their organizations had a ransomware attack. Of these respondents, 31 percent say their organizations paid the ransomware, a slight decrease from 33 percent in 2025. Fewer respondents say their organizations are paying the ransom, and the average total cost decreased, from \$1,238,375 in 2025 to \$1,089,225 in 2026, as shown in Figure 9.

Extrapolated average presented



The insider risk to sensitive data and patient safety

Figure 10. Careless users are a top root cause of data loss and exfiltration incidents.

Organizations had an average of 21 data loss and exfiltration incidents in the past two years, a slight increase from 18. Respondents were asked to identify the root causes of the data loss and exfiltration. Their responses are shown in Figure 10. Ninety-seven percent of organizations had at least two data loss or exfiltration incidents involving sensitive and confidential healthcare data in the past two years.

According to the research, employees continue to be the primary root cause of the data loss and exfiltration incident because of not following policies (32 percent). Twenty-seven percent of respondents say the cause was privilege access abuse and 26 percent of respondents say it was unintentional. The use of stolen credentials increased significantly from 15 percent of respondents to 21 percent of respondents.

More than one response permitted

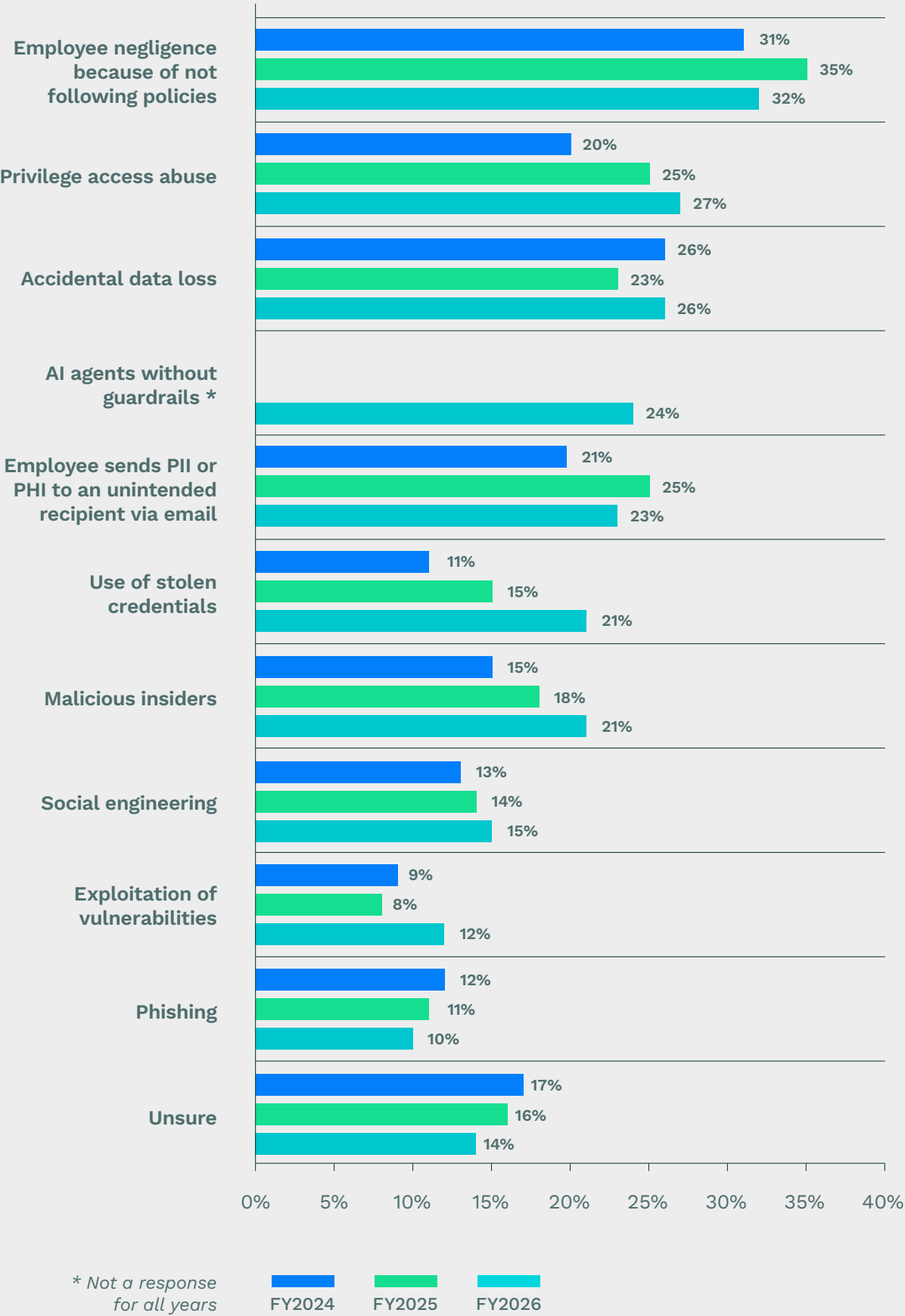


Figure 11. Data loss or exfiltration can increase patient mortality.

Respondents were asked what impact the data loss or exfiltration incident had on patient care. Fifty-four 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 11, 56 percent say it increased the mortality rate, 35 percent say it increased complications from medical procedures and 34 percent say it caused delays in procedures and tests that resulted in poor outcomes.

More than one choice permitted

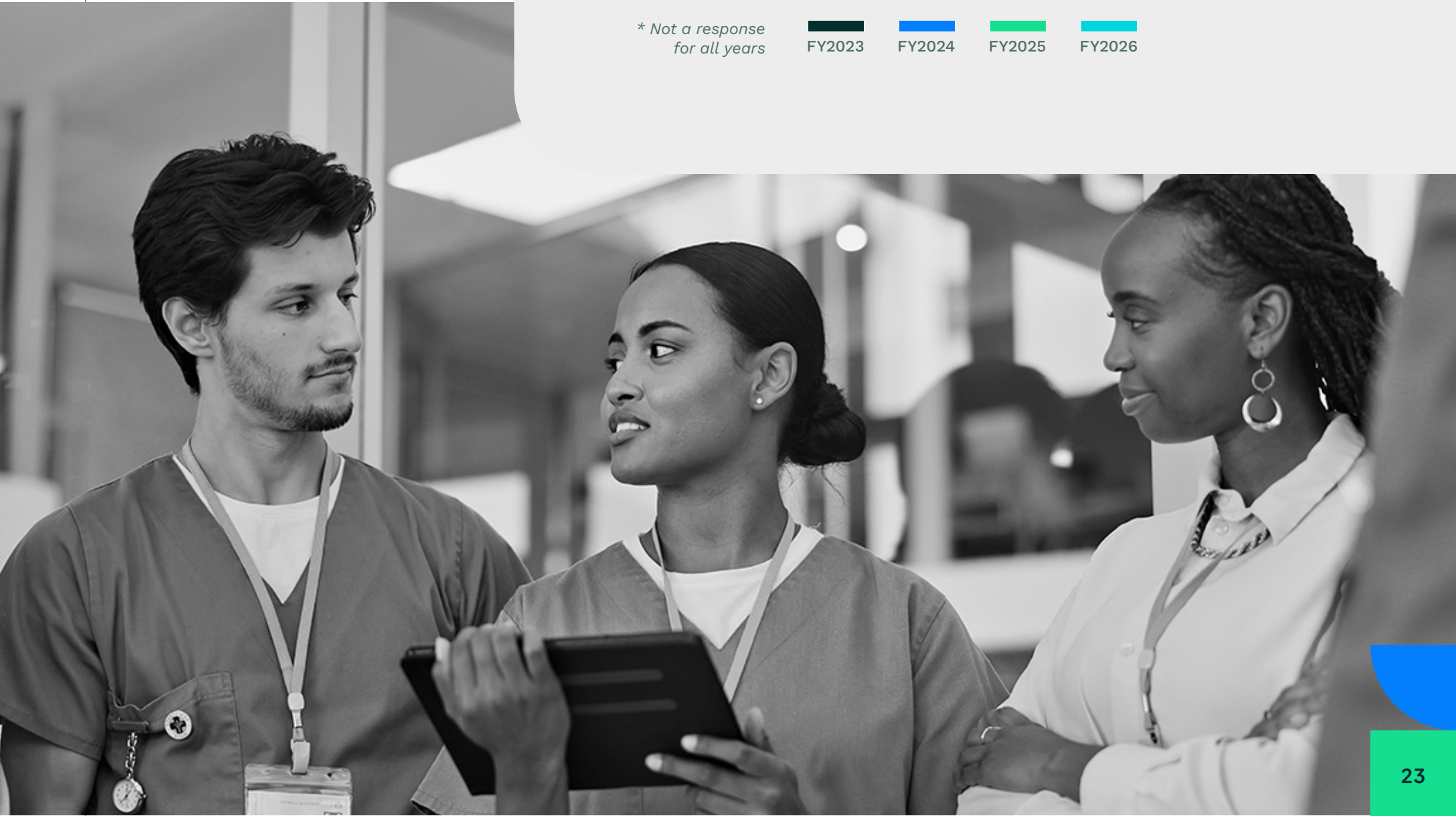
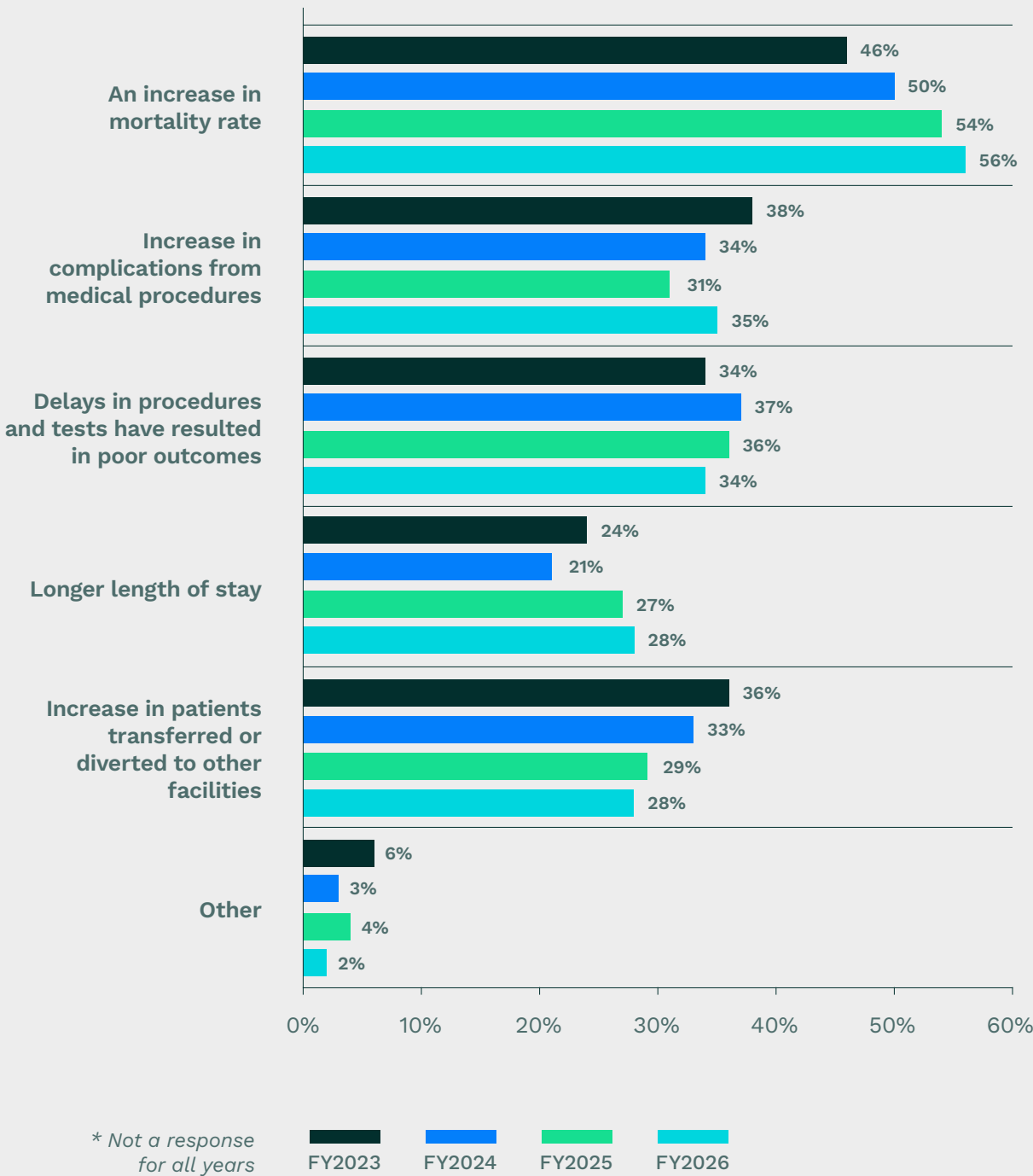


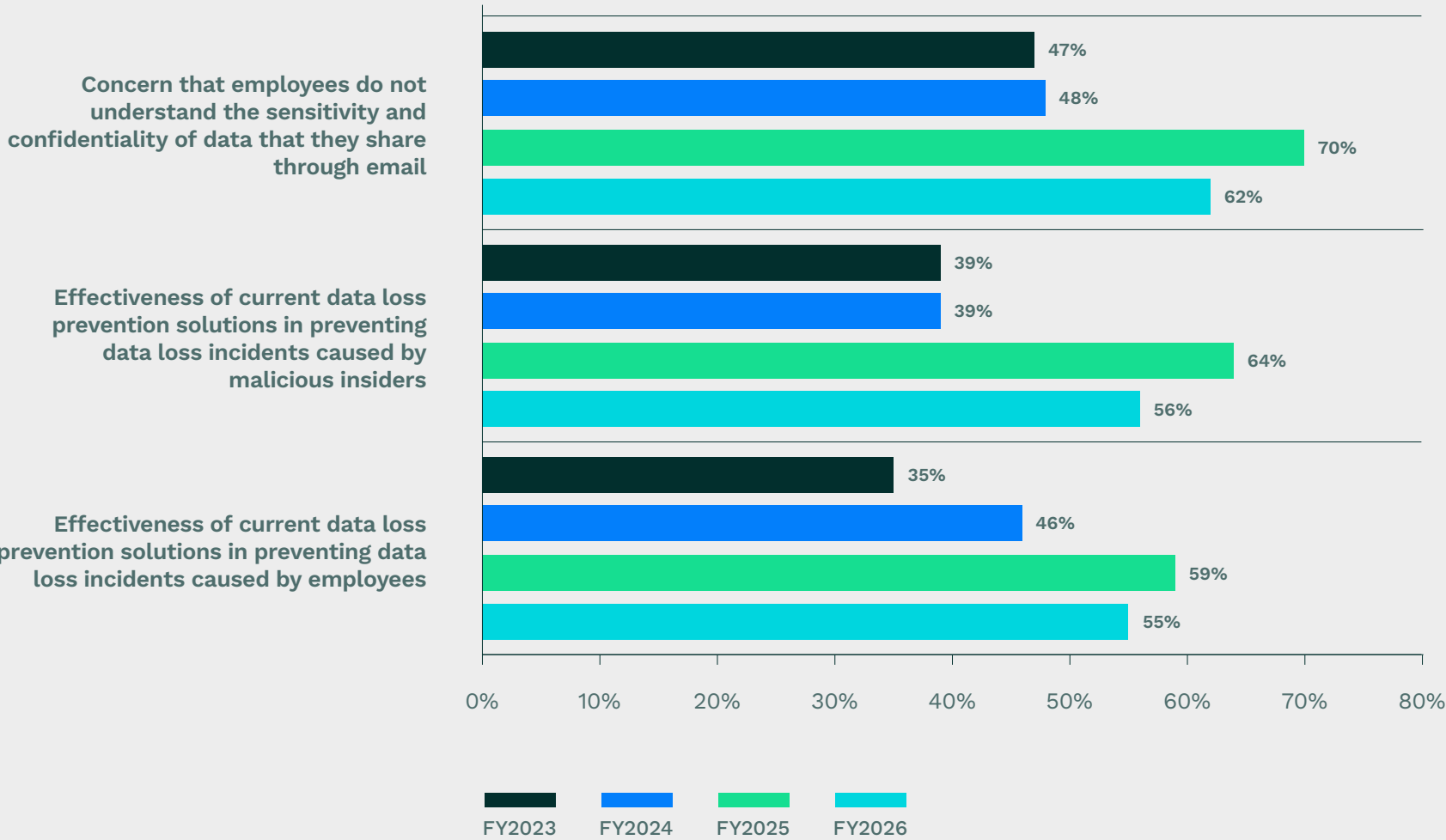
Figure 12. Concerns that employees do not understand the sensitivity and confidentiality of data shared by email decreased significantly from 70 percent in 2025 to 62 percent of respondents in 2026.

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. To determine the level of concern, respondents were asked to rate their concern about employees' awareness on a scale from 1 = not concerned to 10 = very concerned.

Figure 12 presents the very effective responses (7+ on the 10-point scale). As shown, organizations are less positive about the solutions to prevent data loss incidents caused by malicious insiders (a decrease from 64 percent to 56 percent) and data loss prevention solutions to prevent data loss incidents caused by employees (a decrease from 59 percent to 55 percent). However, concerns that employees do not understand the sensitivity and confidentiality of data shared through email decreased from 70 percent to 62 percent.

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



AI and machine learning in healthcare

Figure 13. AI is becoming a critical component of healthcare’s cybersecurity strategies.

For the third consecutive year, the research explores both the benefits and risks of using AI in healthcare, reflecting its growing impact across the industry. Respondents were asked if their organizations adopted AI. As shown in Figure 13, 45 percent of respondents say their organizations have embedded AI in cybersecurity (24 percent) or embedded in both cybersecurity and patient care (21 percent).

One choice is permitted

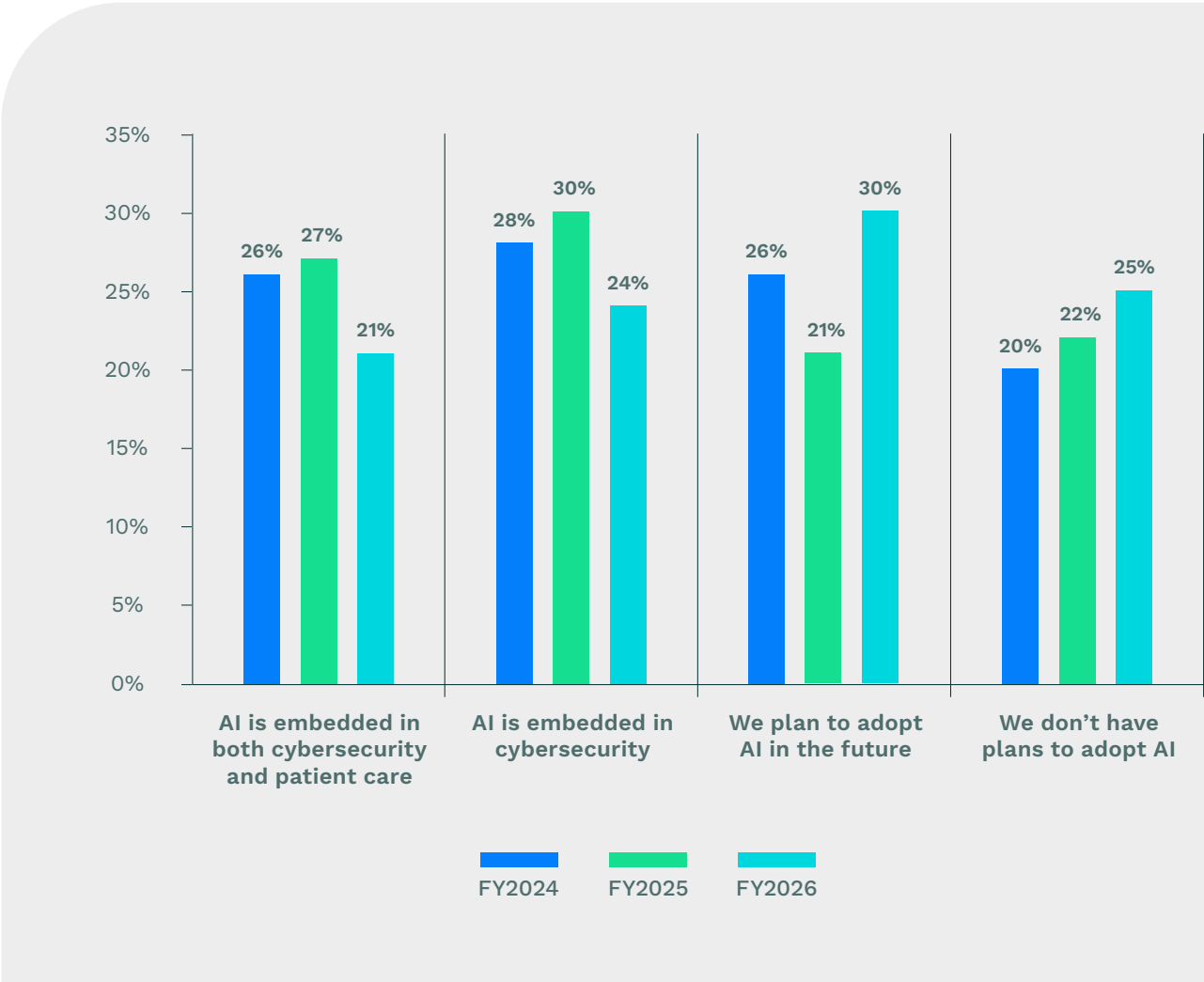


Figure 14. The most common AI tasks in healthcare are administrative, medical imaging and diagnostics. Adoption of robotic surgery may take time.

Respondents were asked what AI tasks and applications does their organization use. As shown in Figure 14, 63 percent of respondents say AI automation of administrative tasks is a priority and 62 percent say AI is used in medical imaging and diagnostics. Few organizations are using AI for surgery and clinical decisions (12 percent and 19 percent of respondents).

More than one choice permitted

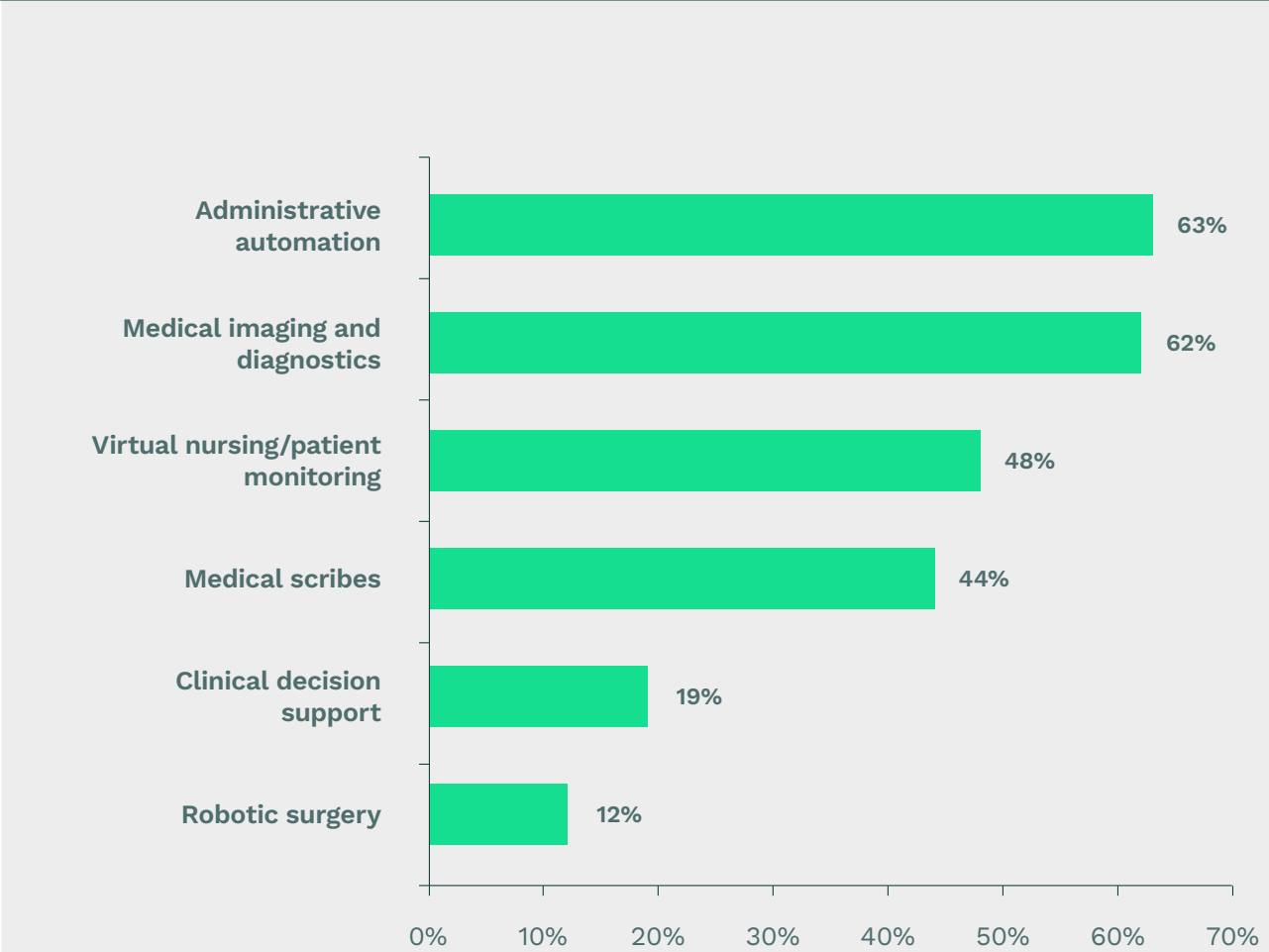


Figure 15. Most organizations do not have controls in place to govern sensitive data used in AI systems.

Respondents were asked what controls are in place to govern sensitive data use in AI systems. Only 40 percent of respondents say their organizations have controls in place to govern sensitive data used in AI systems, suggesting AI data governance remains in the early stages for many organizations. Among those implementing safeguards, 52 percent of respondents say a priority is to protect AI training data with strong encryption and data access controls, as shown in Figure 15. Forty-six percent of respondents say all AI outputs are monitored by professionals to prevent mistakes. Another 46 percent of respondents say access controls are used.

More than one choice permitted

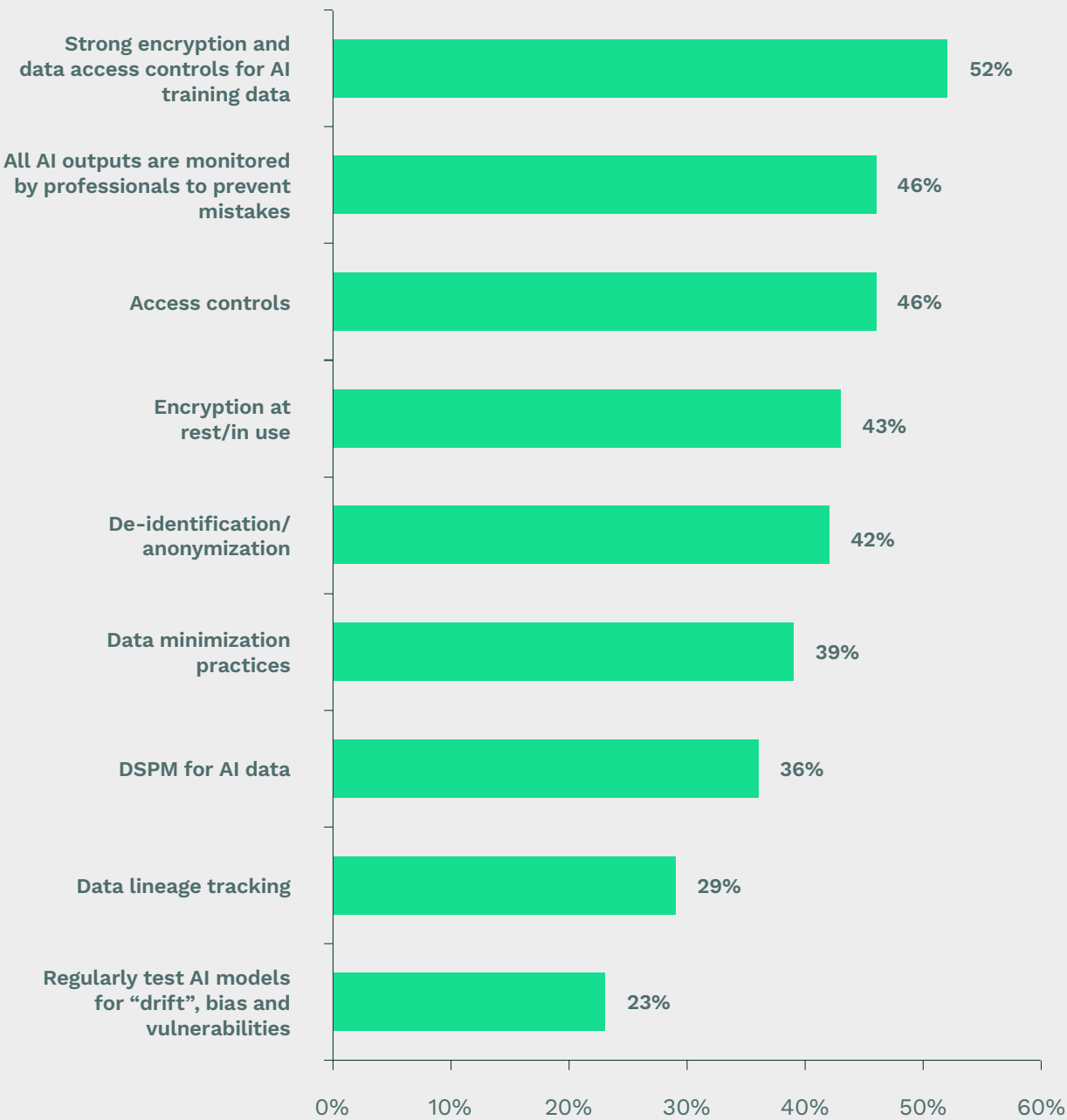


Figure 16. Healthcare organizations remain cautious about generative AI adoption.

Generative AI can introduce risks such as the inadvertent disclosure of sensitive data, the creation of deceptive content, deep fakes, synthetic identities, and counterfeit data. These risks can lead to fraud, misinformation and other malicious activities. As a result, many organizations continue to limit or prohibit the use of public generative AI tools.

According to Figure 16, only 23 percent of respondents say generative AI tools are widely used with governance. Fifty-one percent say they limit use (31 percent) or these tools are not used (20 percent).

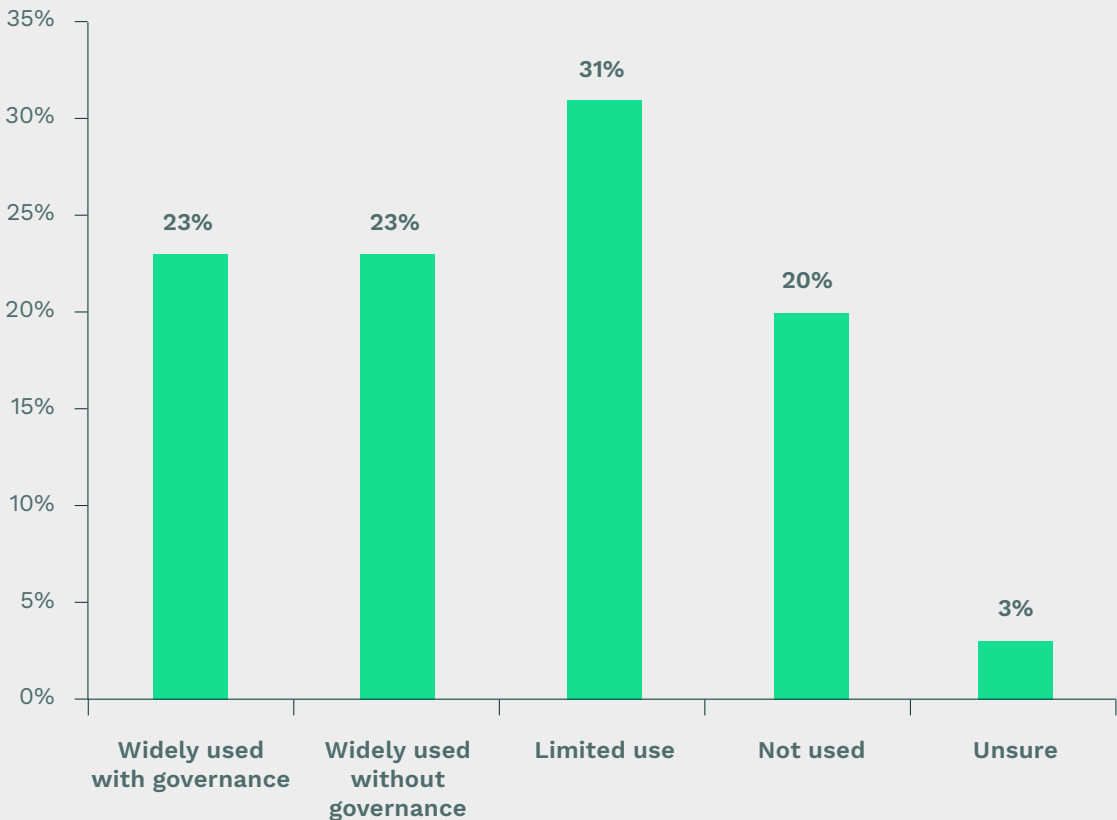


Figure 17. Visibility into AI tools is critical to mitigating security risks and maintaining regulatory compliance. Visibility empowers organizations to track how AI models use their data and secure internal operations against unauthorized use.

Respondents were asked if their organizations have visibility into employee use of unsanctioned AI tools. As shown in Figure 17, 74 percent of respondents say their organizations have either full visibility (32 percent) or partial visibility (42 percent).

One response permitted

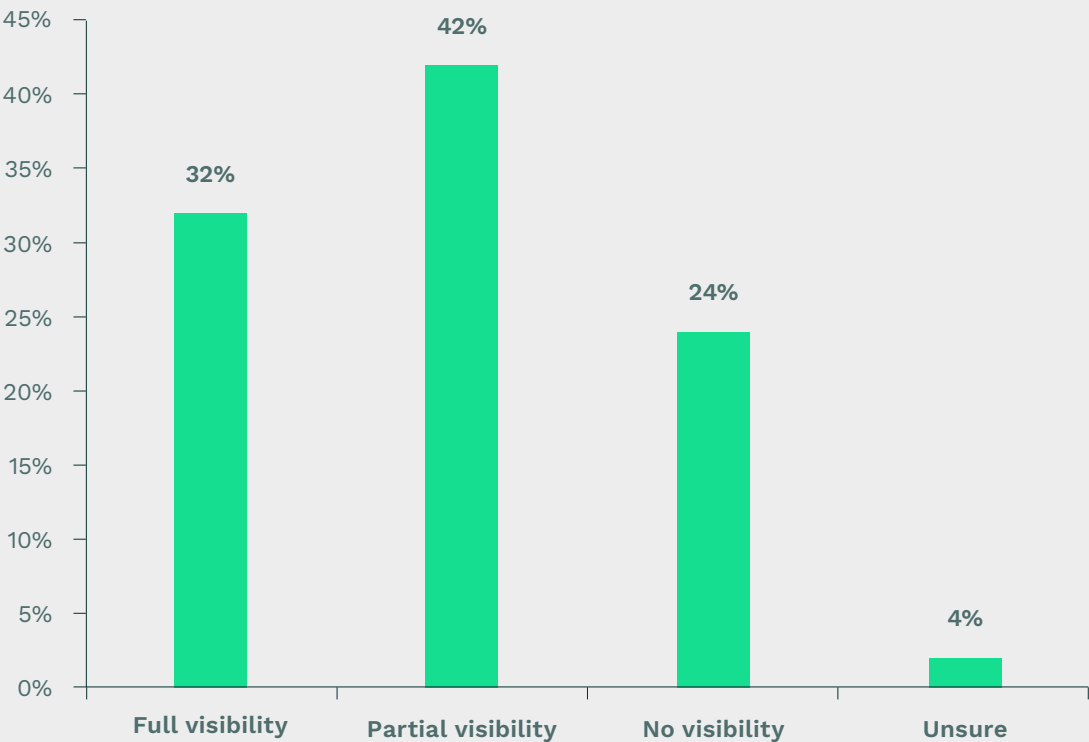


Figure 18. The supply chain seems to be the weakest link in AI security in healthcare.

Respondents were asked to identify AI-specific risks they are most concerned about. As shown in Figure 18, AI vendors within the supply chain are the leading concern, cited by 40% of respondents. Other top risks include data leakage through AI prompts (36%) and AI-generated phishing and social engineering attacks (34%), underscoring the expanding AI threat landscape.

Three choices permitted

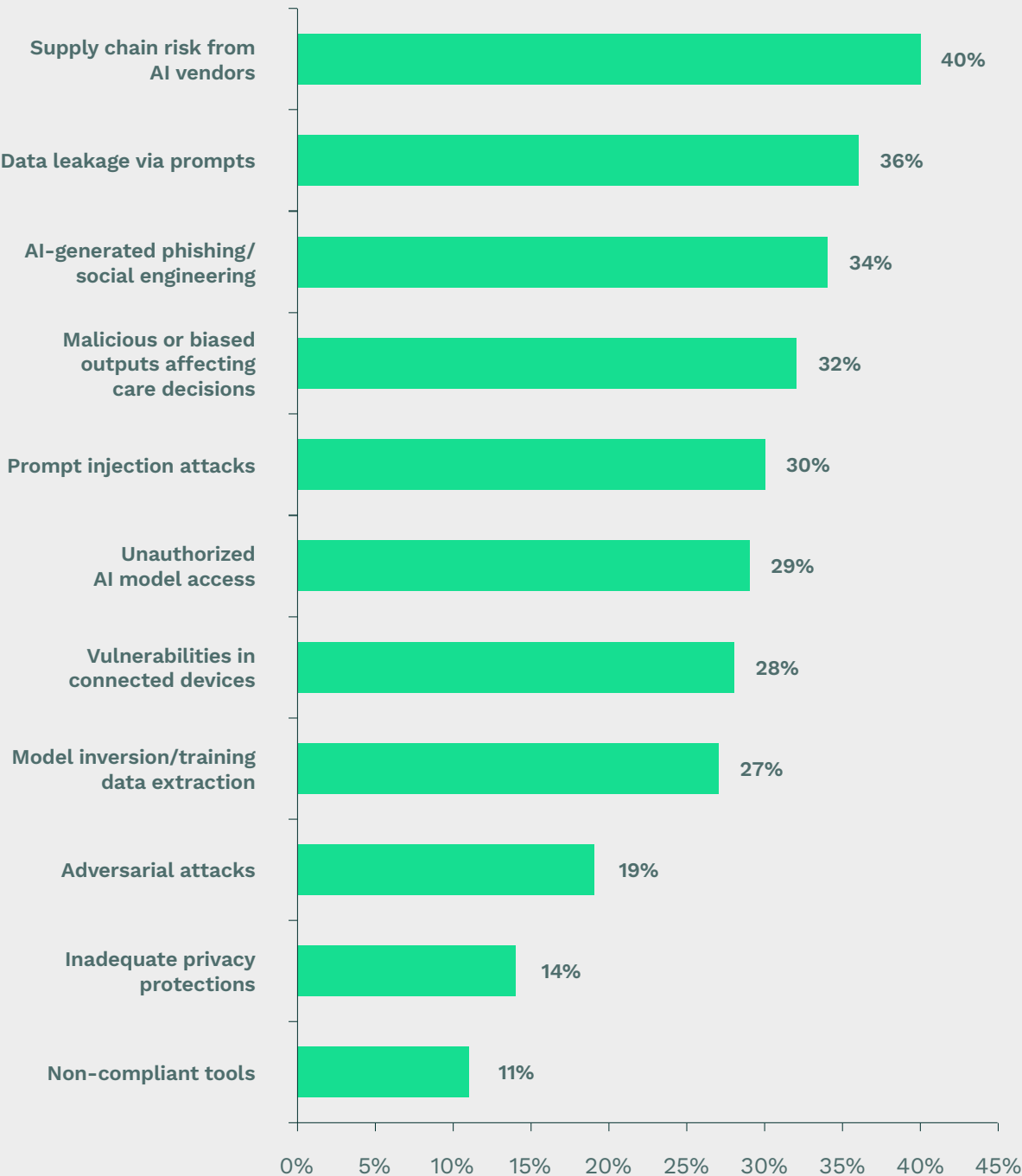


Figure 19. AI governance and data protection lead AI security measures.

Respondents were asked what security measures their organizations use to protect AI systems, AI agents, and generative AI tools. While AI-related risks such as data leakage through prompts and AI supply chain vulnerabilities are significant concerns, only 42% of respondents report having security measures in place to protect AI systems, agents, and generative AI. Among organizations implementing safeguards, AI data governance and access controls are the most common measures (50%), followed by AI data protection and data loss prevention (45%), as shown in Figure 19.

More than one choice permitted

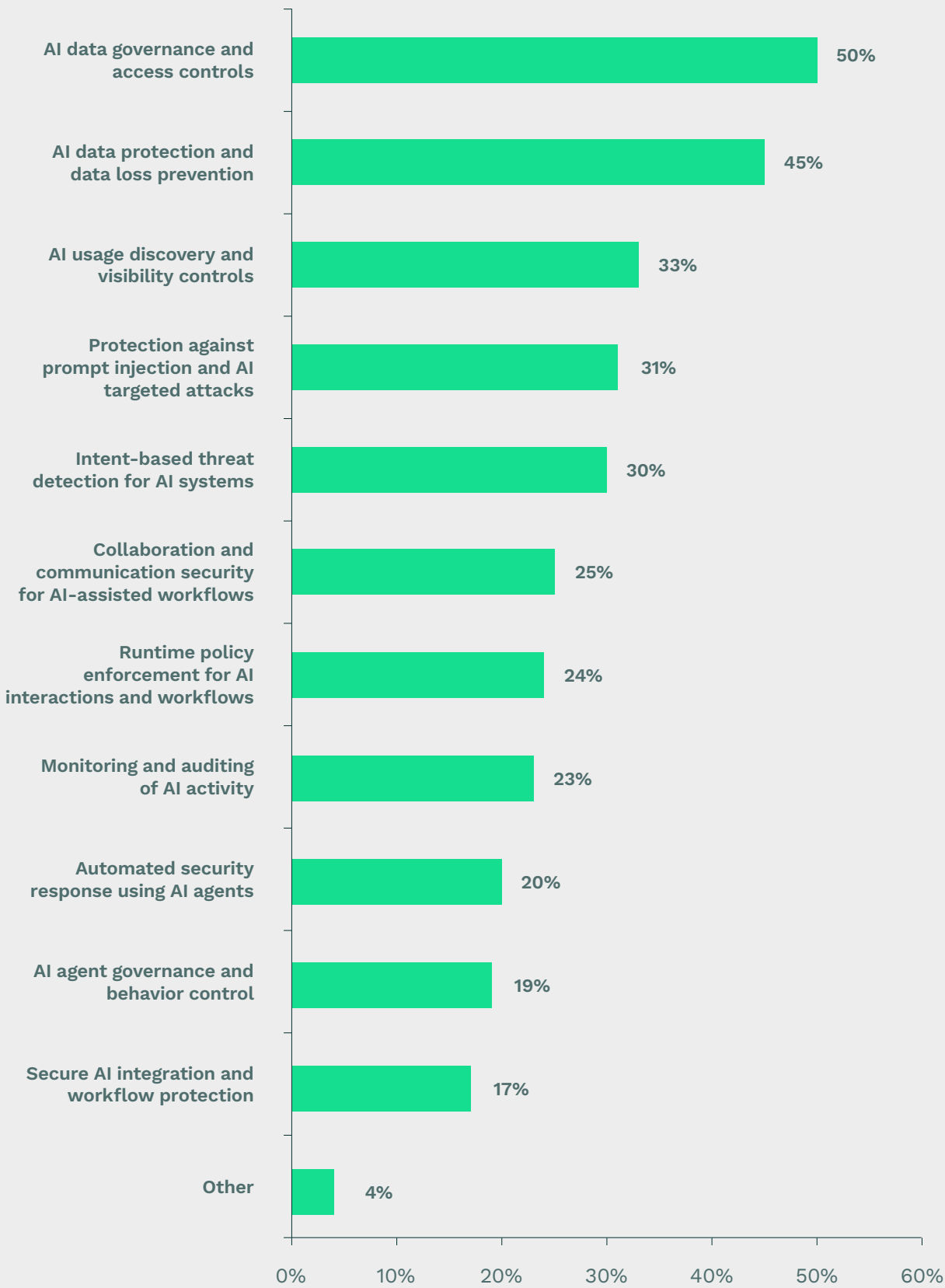
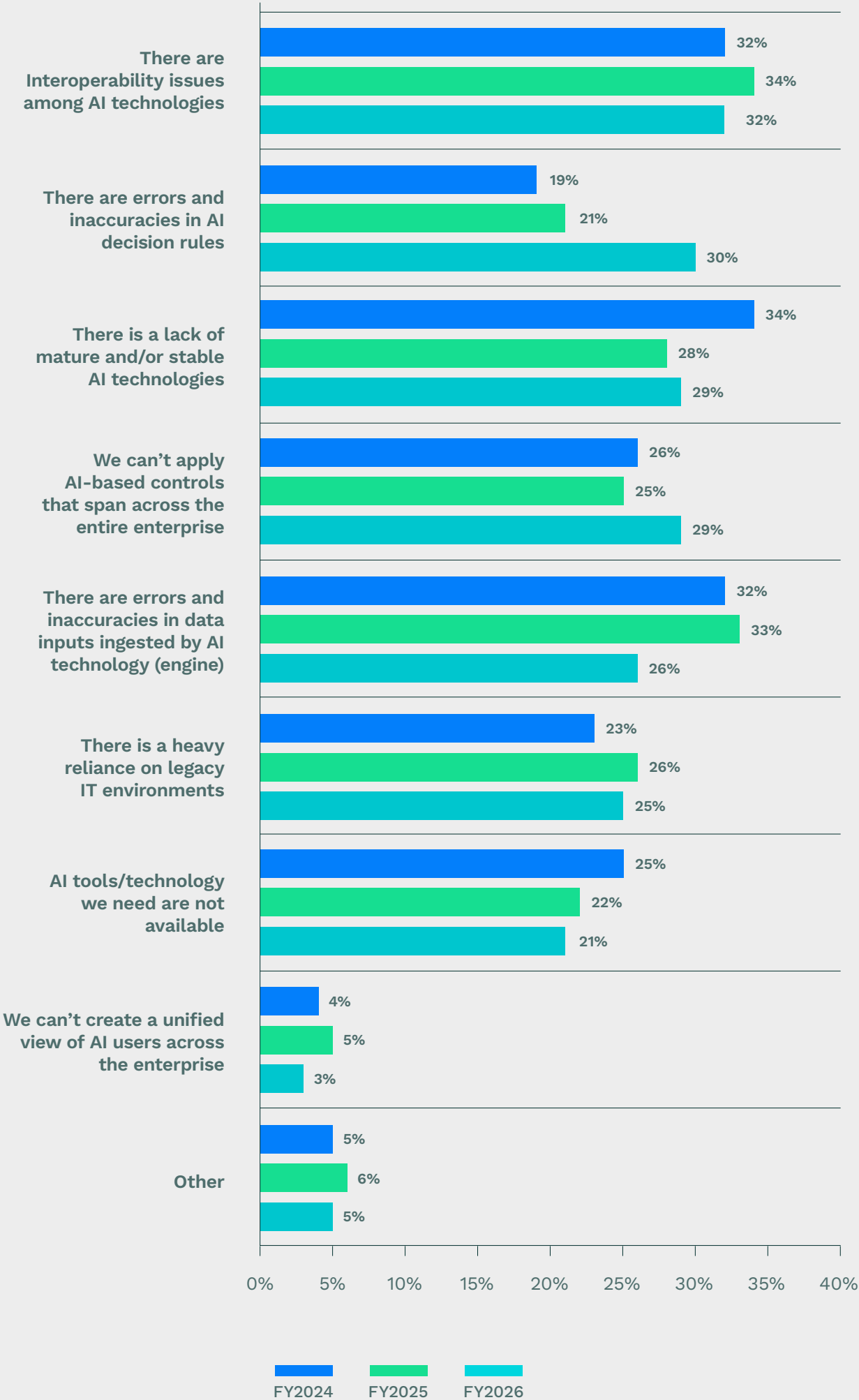


Figure 20. Interoperability remains the top challenge to AI security adoption for the second consecutive year.

Respondents were asked to identify the challenges to adopting AI-based security technologies. Figure 20 presents the issues that may delay adoption. The top challenge is interoperability among AI technologies (32 percent of respondents). Errors and inaccuracies in AI decision rules have increased significantly from 21 percent to 30 percent of respondents in 2026. Errors and inaccuracies in data inputs ingested by AI technology (engine) have decreased as a challenge from 33 percent to 26 percent of respondents in 2026.

Two choices permitted



Solutions and responses to cyber insecurity

Figure 21. The lack of in-house expertise and budget continues to be a problem and a threat to healthcare organizations’ cybersecurity posture.

While 46 percent of respondents say their organizations’ lack of in-house expertise is a primary deterrent to achieving a strong cybersecurity posture, the lack of budget is a challenge according to 42 percent, as shown in Figure 21.

The annual budget for IT has increased slightly from \$65 million in 2025 to \$69 million in 2026. Twenty-two percent of the IT budget is dedicated to information security.

Three choices permitted

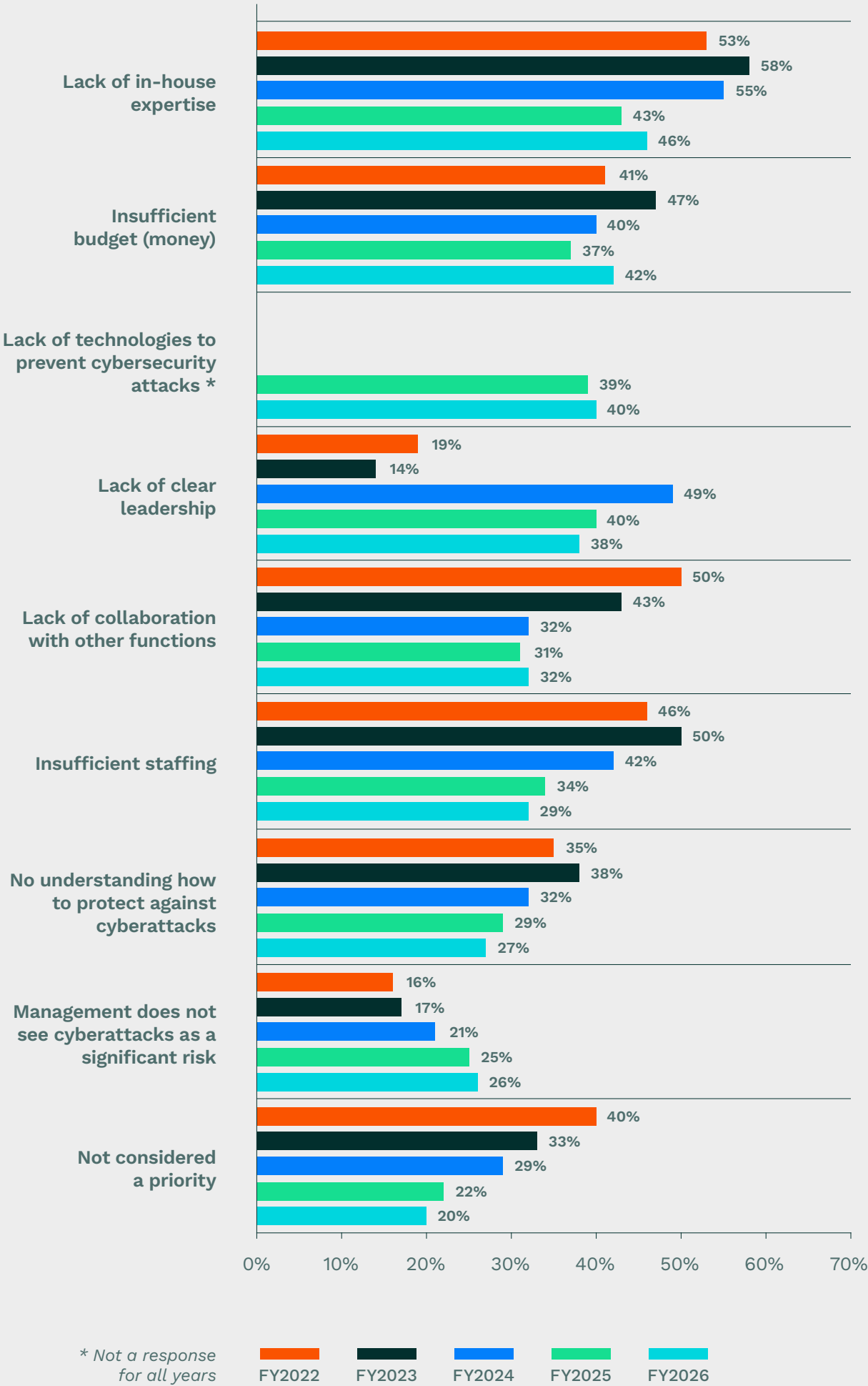


Figure 22. More organizations are using simulations of phishing attacks to create greater awareness of cybersecurity threats.

Sixty-four percent of respondents say it is very important to understand human behavior to protect sensitive and confidential data in emails.

Respondents were asked what steps are taken to address the risk of employees’ lack of awareness about cybersecurity threats. Seventy-five percent of respondents say their organizations take steps to address the risk of employees’ lack of awareness about cybersecurity threats, an increase from 71 percent in 2024.

As shown in Figure 22, 65 percent of respondents say their organizations conduct regular training and awareness programs. Simulation of phishing attacks increased significantly from 47% of respondents in 2025 to 56 percent in 2026. Fifty percent say their organizations monitor the actions of employees. More organizations are conducting audits and assessments of areas most vulnerable to employees’ lack of awareness.

More than one choice permitted

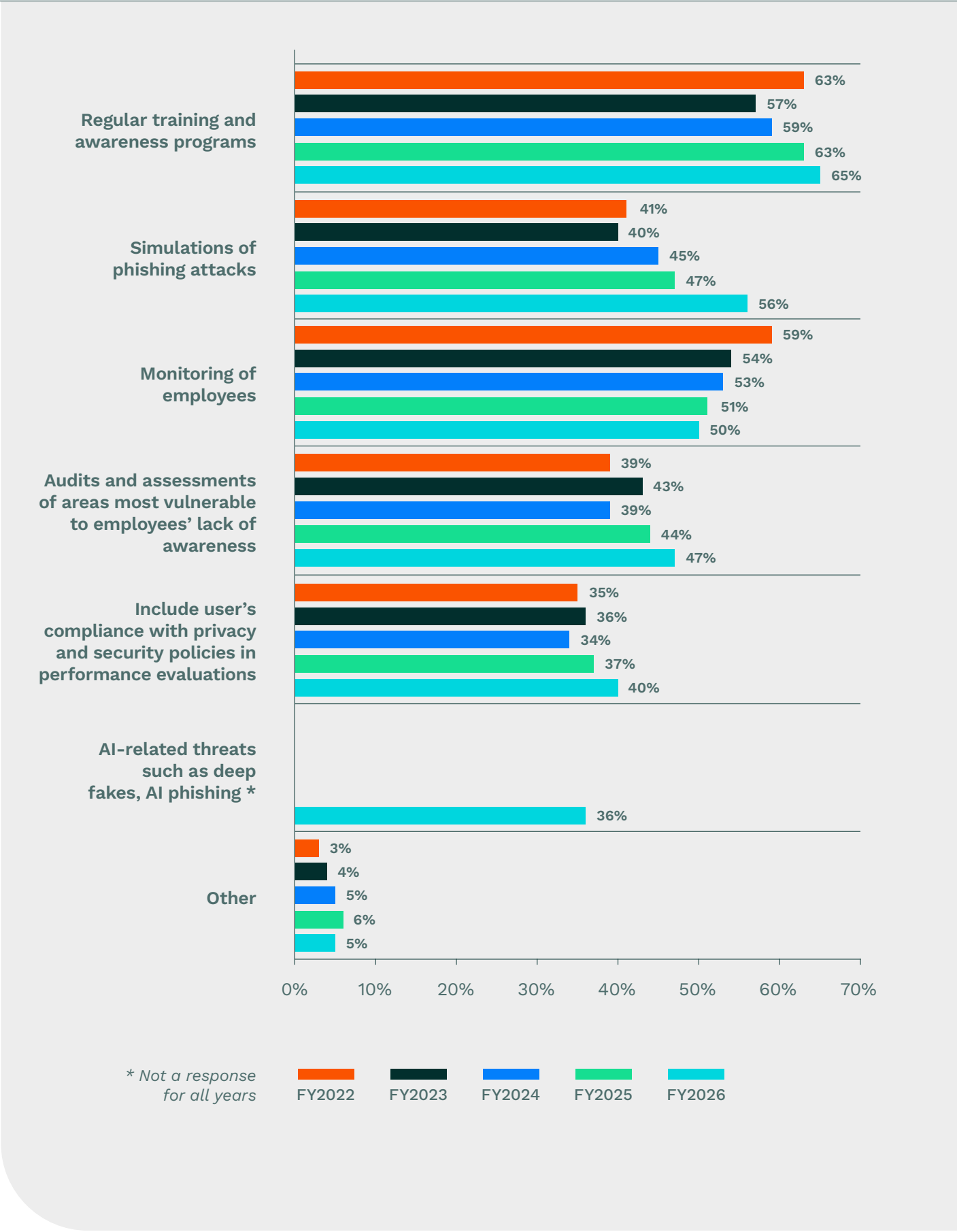


Figure 23. Email security deployment models continue to evolve.

Respondents were asked what security methods and technologies their organizations use to reduce phishing and other email-based attacks. As shown in Figure 23, the use of anti-virus/anti-malware increased significantly from 49 percent in 2025 to 54 percent in 2026. Fifty-three percent say they use a secure email gateway. New to this year’s study, API-based email security emerged as a widely adopted technology, with 51% of respondents reporting its use. Nearly half (48%) also indicated they use a combination of SEG and API-based email security, reflecting a growing trend toward multiple email security deployment models. AI/ML increased from 41 percent in 2025 to 47 percent of respondents in 2026.

More than one choice permitted

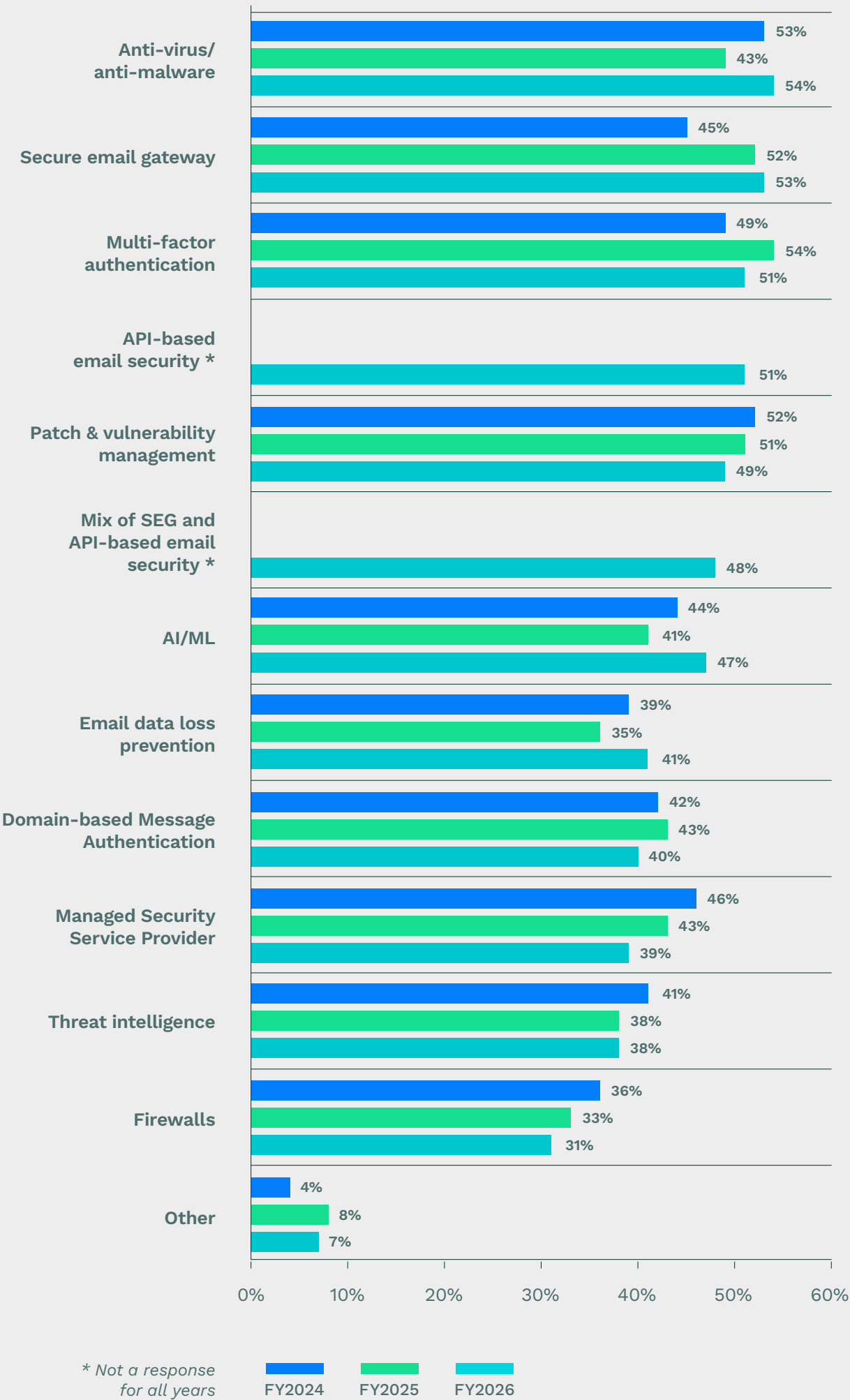
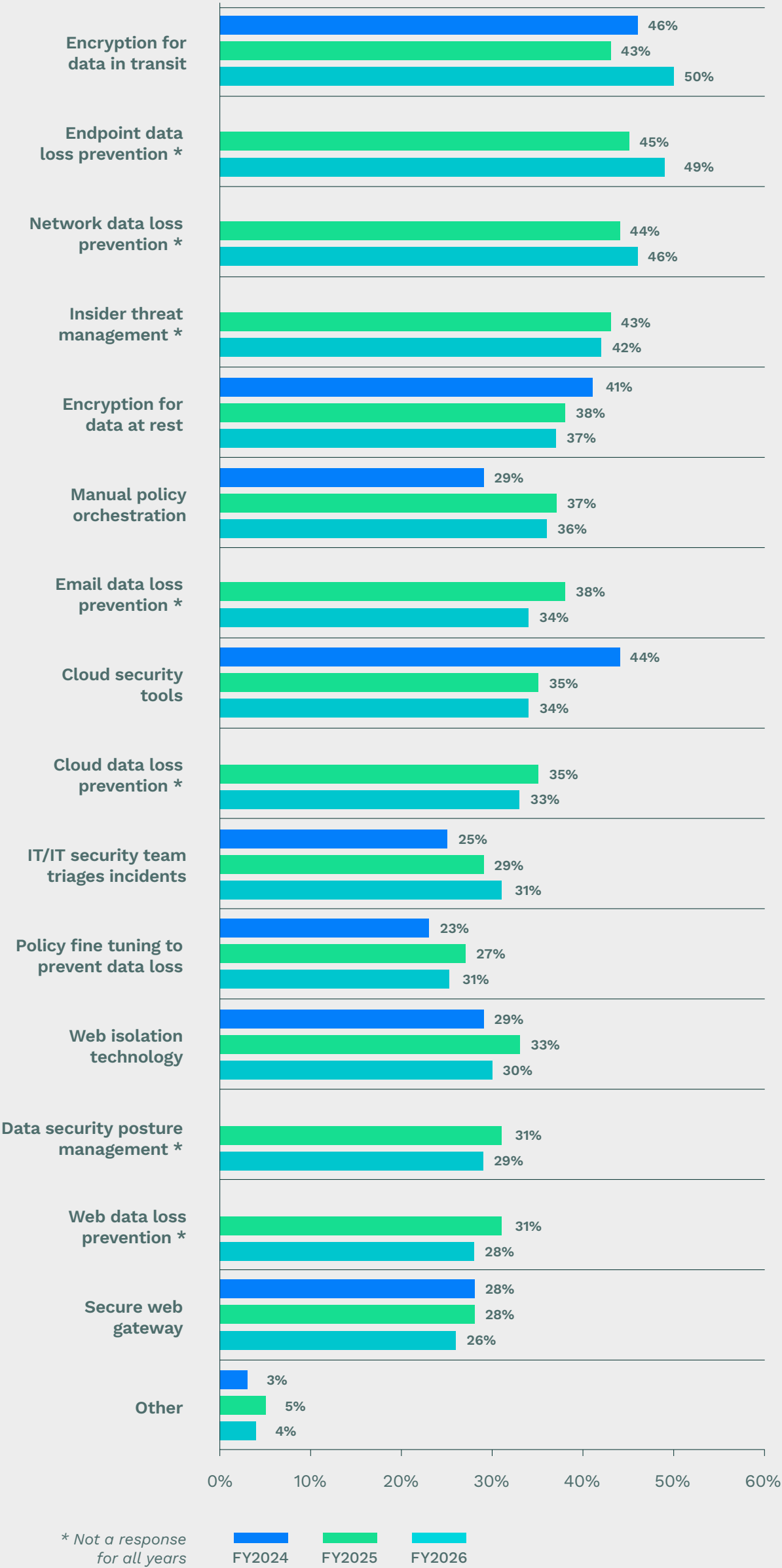


Figure 24. The use of encryption for data in transit and endpoint data loss prevention are the top two technologies used to prevent data loss or exfiltration incidents.

Respondents were asked what security methods and technologies their organizations implemented to prevent data loss or an exfiltration incident. According to Figure 24, The use of encryption for data in transit increased significantly from 43 percent in 2025 to 50 percent of respondents in 2026. Forty-nine percent of respondents say endpoint data loss prevention and 46 percent say network data loss prevention tools are used to prevent data loss or an exfiltration incident.

More than one choice permitted



PART 3

Methodology

Our final sample consisted of 705 surveys or a 3.7 percent response rate

A sampling frame of 19,005 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 788 total returns. Screening and reliability checks required the removal of 83 surveys. Our final sample consisted of 705 surveys or a 3.7 percent response rate.

Table 3. Sample response	Freq	Pct%
Sampling frame	19,005	100.0%
Total returns	788	4.1%
Rejected or screened surveys	83	0.4%
Final sample	705	3.7%



Figure 25. Type of organization.

Figure 25 reports respondents' organization types. Twenty-two percent of respondents are from organizations that are public healthcare providers. This is followed by private healthcare providers (18 percent), healthcare insurer (18 percent), payer (11 percent) and healthcare insurance (10 percent).

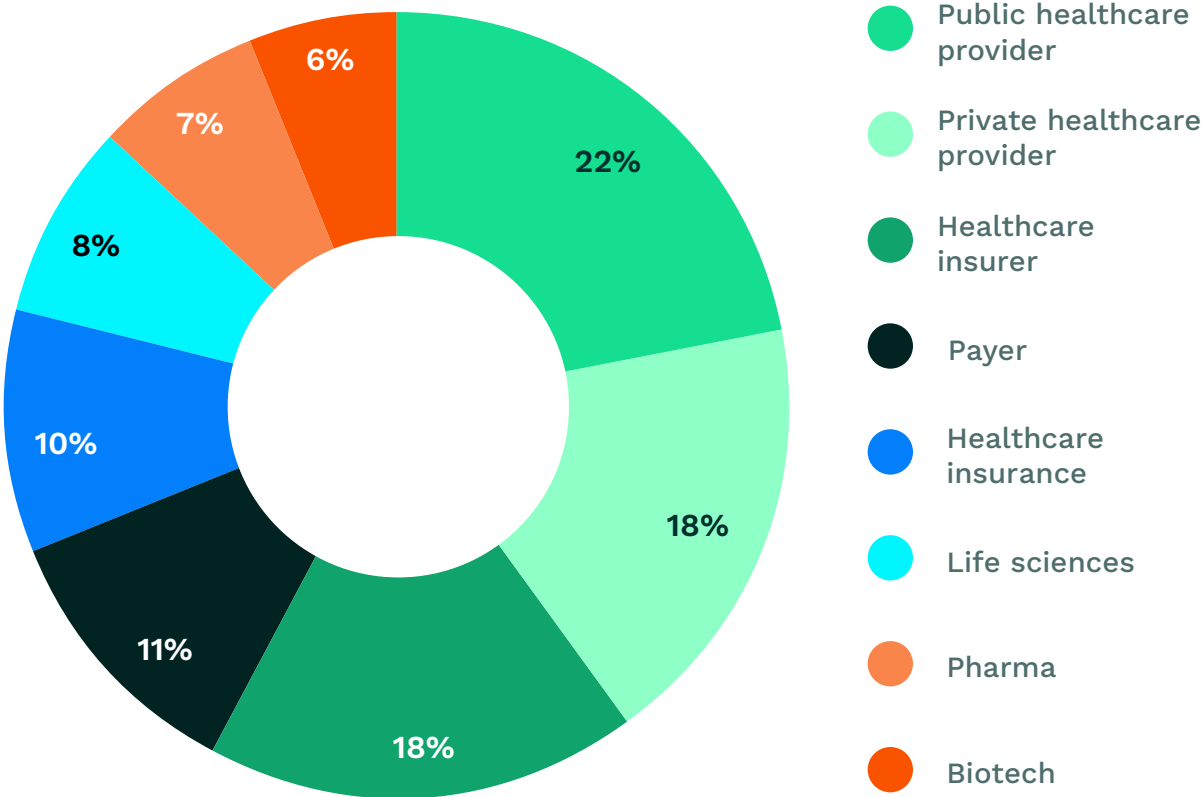


Figure 26. Current position within the organization.

Figure 26 reports the respondent's organizational level within participating organizations. By design, more than half (63 percent) are at or above the supervisory levels. The largest category is technician/staff (28 percent).

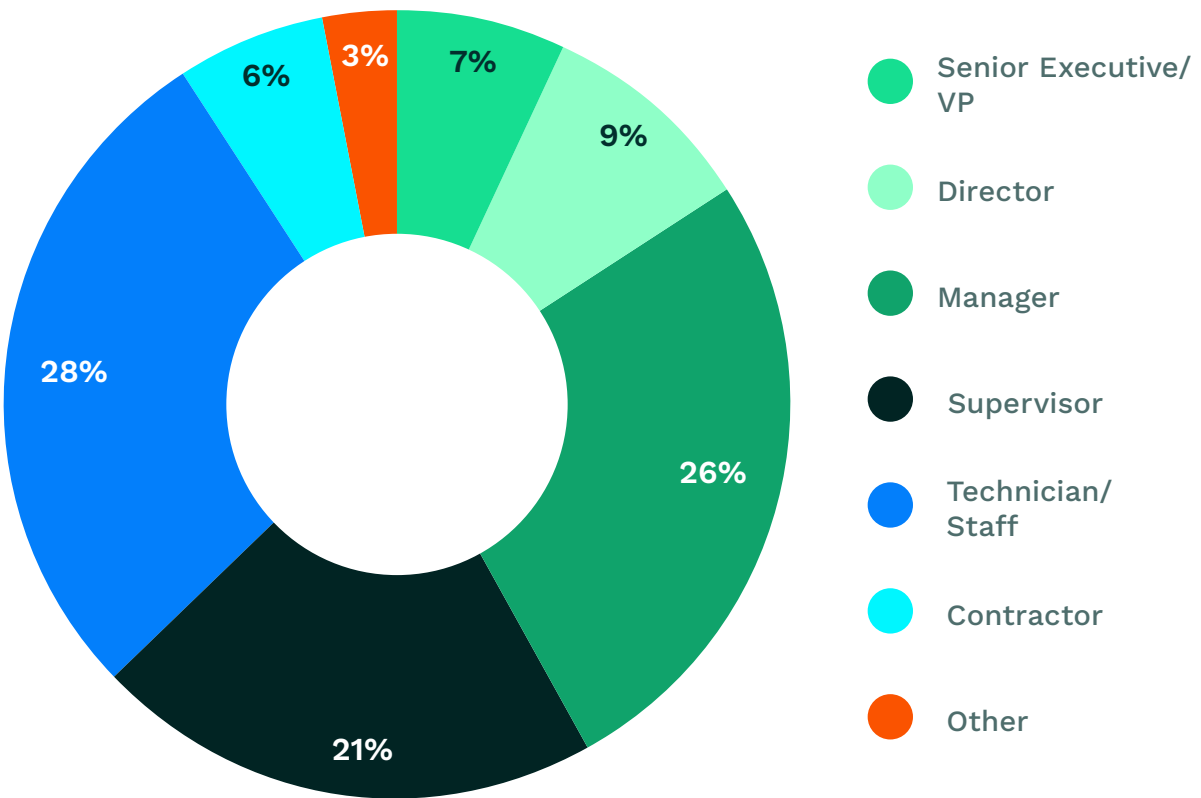


Figure 27. Direct reporting channel.

As shown in Figure 27, 23 percent of respondents report to the chief information security officer, 18 percent report to the chief information officer, 11 percent report to cloud administration, 10 percent report to the chief risk officer and 9 percent report to the chief technology officer.

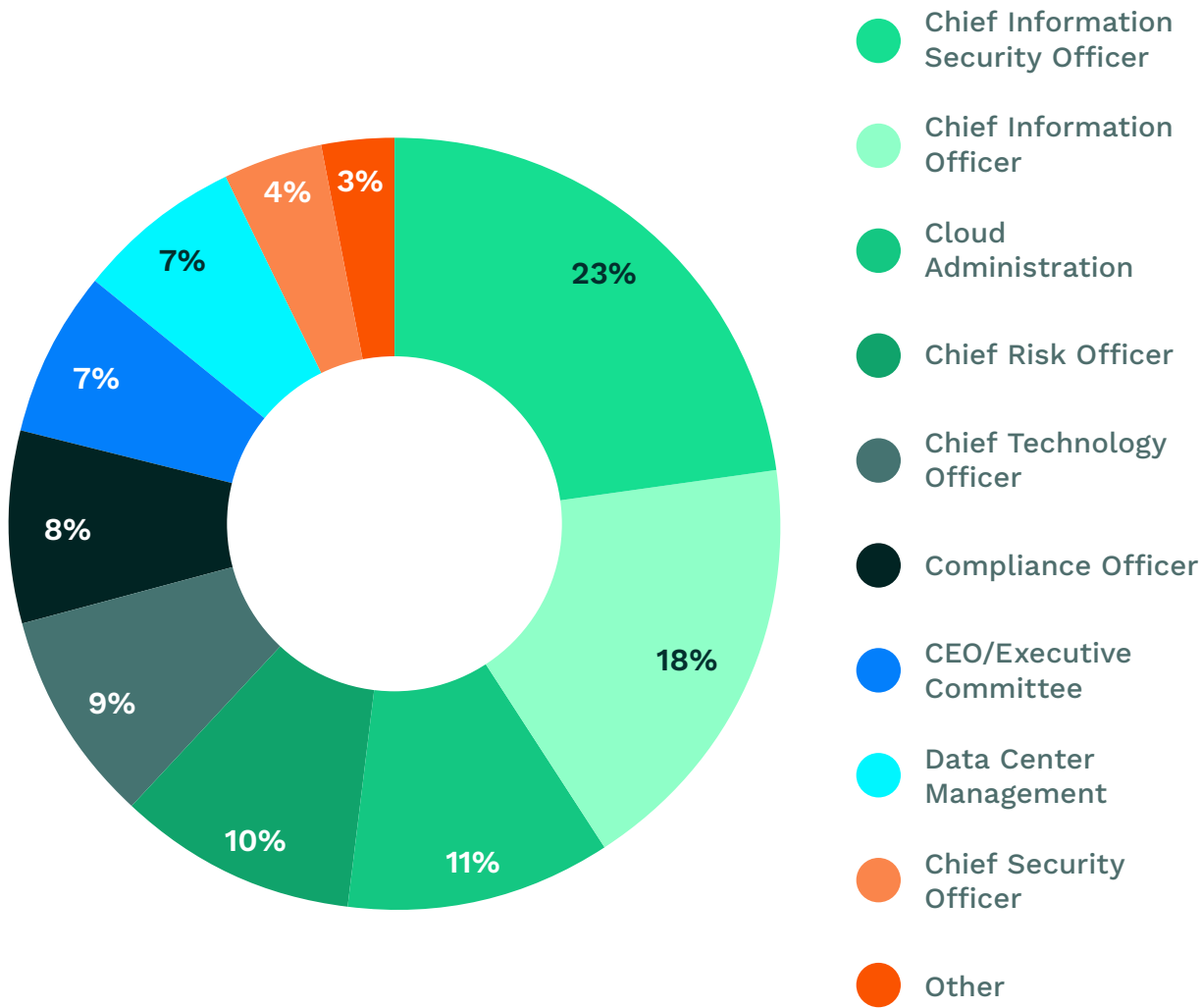
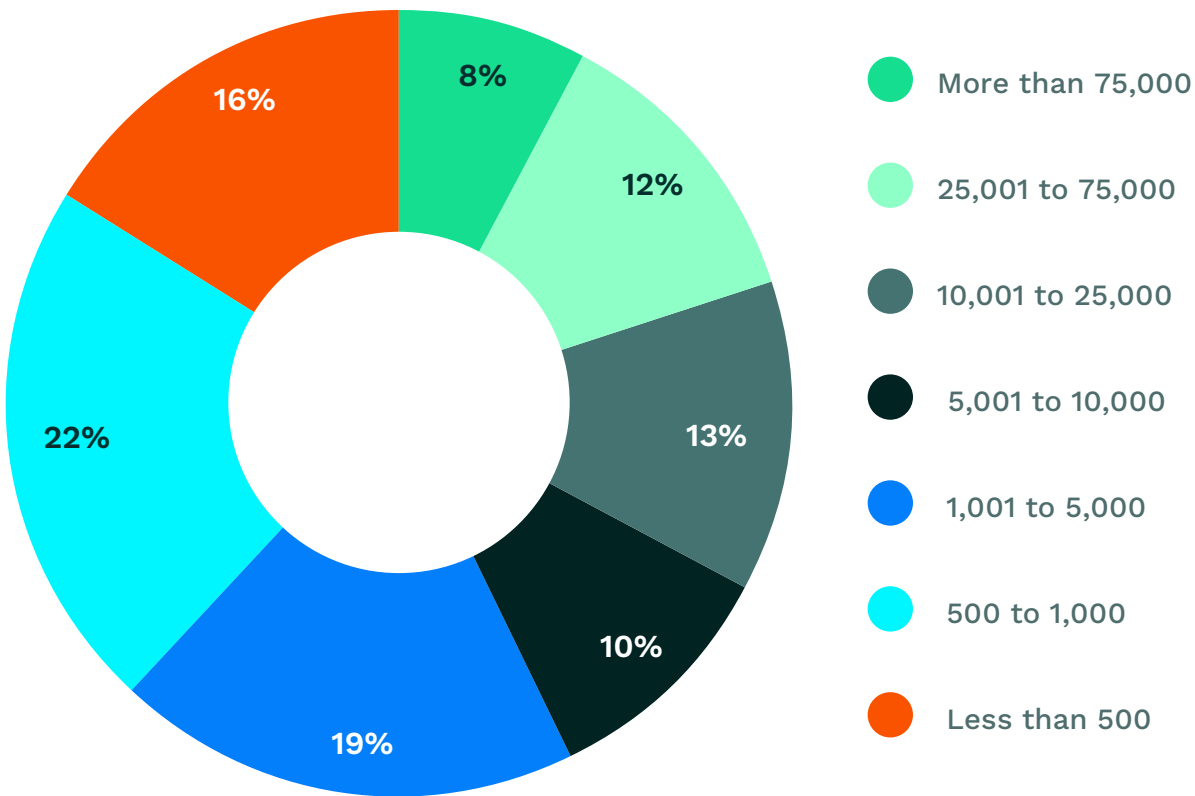


Figure 28. Global full-time headcount.

As shown in Figure 28, 62 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

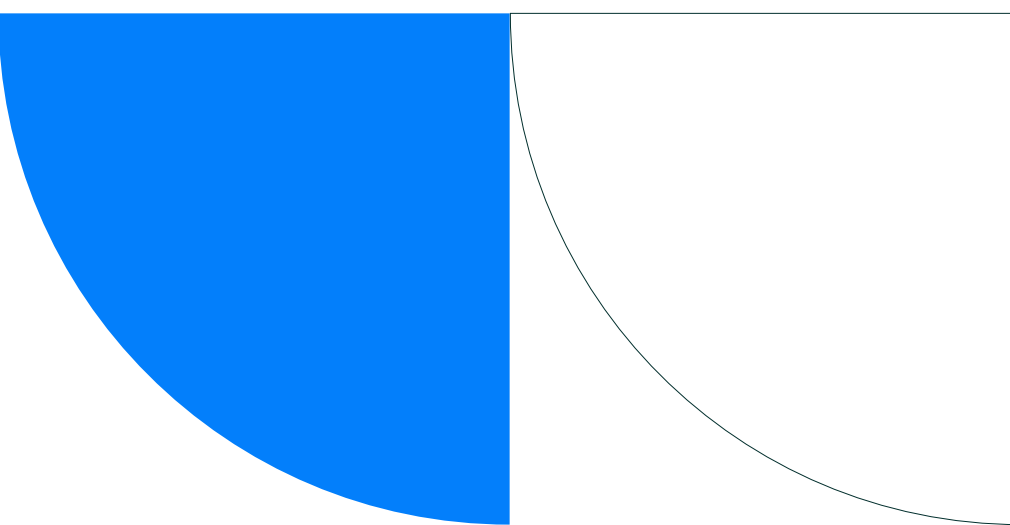


PART 4

Caveats to this report

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.



PART 5

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 May 2026.

Survey response	FY2026	FY2025	FY2024	FY2023	FY2022
Total sampling frame	19,005	17,220	18,015	17,085	16,451
Total returns	788	756	732	715	698
Rejected returns	83	79	84	62	57
Total sample	705	677	648	653	641
Response rate	3.7%	3.9%	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.	FY2026	FY2025	FY2024	FY2023	FY2022
Setting IT cybersecurity priorities	60%	55%	49%	51%	46%
Managing IT security budgets	46%	41%	43%	45%	42%
Selecting vendors and contractors	51%	50%	47%	49%	47%
Participating in IT cybersecurity strategies	57%	53%	52%	51%	51%
Evaluating and measuring effectiveness of cybersecurity strategies	48%	46%	36%	36%	34%
Managing cybersecurity risk	43%	37%	40%	34%	36%
Overseeing governance and compliance	30%	26%	28%	27%	29%
None of the above [Stop]	0%	0%	0%	0%	0%

Part 1. Cybersecurity threats to healthcare organizations

Q1. What cybersecurity threats is your organization most concerned about? Please select the top six (6).	FY2026	FY2025	FY2024	FY2023	FY2022
BEC/spoofing/impersonation	48%	40%	46%	62%	46%
Cloud/account takeovers or compromises	54%	49%	55%	63%	57%
Employee negligence or error	41%	47%	52%	52%	58%
Employee-owned mobile devices or BYOD	46%	49%	53%	61%	34%
Generative AI or AI tools	46%	38%			
Insecure medical devices	50%	47%	54%	53%	64%
Insecure mobile apps (eHealth)	53%	55%	59%	51%	59%
Malicious insiders	36%	37%	42%	45%	37%
Malware	21%	23%			
Nation state attacks	23%	26%	21%	19%	17%
Process failures	25%	23%	31%	31%	36%
Ransomware	40%	42%	45%	48%	60%
Supply chain risks	37%	42%	46%	40%	43%
System failures	33%	34%	44%	35%	36%
Third-party misuse of patient data	28%	29%	31%	26%	33%
Use of public cloud services	16%	15%	17%	11%	18%
Other (please specify)	3%	4%	4%	3%	2%
Total	600%	600%	600%	600%	600%

Q2. What challenges keep your organization's cybersecurity posture from being fully effective? Please select the top three (3) challenges	FY2026	FY2025	FY2024	FY2023	FY2022
Insufficient budget (money)	42%	37%	40%	47%	41%
Insufficient staffing	29%	34%	42%	50%	46%
Lack of in-house expertise	46%	43%	55%	58%	53%
Lack of technologies to prevent cybersecurity attacks	40%	39%			
Lack of clear leadership	38%	40%	49%	14%	19%
Management does not see cyberattacks as a significant risk	26%	25%	21%	17%	16%
Lack of collaboration with other functions	32%	31%	32%	43%	50%
No understanding how to protect against cyberattacks	27%	29%	32%	38%	35%
Not considered a priority	20%	22%	29%	33%	40%
Total	300%	300%	300%	300%	300%

Q3. Did your organization ever experience a successful ransomware attack?	FY2026	FY2025	FY2024	FY2023	FY2022
Yes	63%	61%	59%	54%	41%
No (please skip to Q8a)	32%	35%	33%	44%	52%
Unsure (please skip to Q8a)	5%	4%	8%	2%	7%
Total	100%	100%	100%	100%	100%

Q4. How many successful ransomware attacks did your organization experience over the past two years?	FY2026	FY2025	FY2024	FY2023	FY2022
One	33%	32%	37%	43%	53%
Two to five	34%	35%	36%	34%	33%
Six to 10	23%	24%	21%	16%	9%
More than 10	10%	9%	6%	7%	5%
Total	100%	100%	100%	100%	100%
Extrapolated value	4.6	5.0	4.0	3.7	3.0

Q5. Did your organization pay the ransom?	FY2026	FY2025	FY2024	FY2023	FY2022
Yes	31%	33%	36%	40%	51%
No (please skip to Q7a)	69%	67%	64%	60%	49%
Total	100%	100%	100%	100%	100%

Q6. If yes, how much was the ransom? If your organization has had more than one ransomware attack, please select the costliest ransom paid.	FY2026	FY2025	FY2024	FY2023	FY2022
Less than \$10,000	0%	0%	0%	0%	2%
\$10,000 to \$25,000	7%	6%	9%	13%	9%
\$25,001 to \$50,000	10%	11%	10%	9%	7%
\$50,001 to \$75,000	14%	13%	12%	14%	10%
\$75,001 to \$100,000	18%	9%	19%	18%	17%
\$100,001 to \$250,000	15%	14%	12%	11%	19%
\$250,001 to \$500,000	12%	11%	13%	12%	18%
\$500,001 to \$1,00,000	8%	9%	8%	9%	8%
\$1,00,001 to \$5,000,000	9%	8%	9%	7%	5%
\$5,00,001 to \$10,000,000	3%	4%	6%	4%	3%
More than \$10,000,000	4%	5%	2%	3%	2%
Total	100%	100%	100%	100%	100%
Extrapolated value	\$1,089,225	\$1,238,375	\$1,099,200	\$995,450	\$771,905

Q7a. Did the ransomware attack result in a disruption in patient care?	FY2026	FY2025	FY2024	FY2023	FY2022
Yes	72%	67%	70%	68%	67%
No	24%	28%	25%	26%	30%
Unsure	4%	5%	5%	6%	3%
Total	100%	100%	100%	100%	100%

Q7b. If yes, what impact did the ransomware attack have on patient care? Please select all that apply.	FY2026	FY2025	FY2024	FY2023	FY2022
An increase in mortality rate	25%	27%	29%	28%	24%
Delays in procedures and tests have resulted in poor outcomes	53%	56%	61%	59%	64%
Increase in complications from medical procedures	49%	50%	47%	44%	48%
Increase in patients transferred or diverted to other facilities	51%	50%	52%	46%	50%
Longer length of stay	70%	67%	58%	48%	59%
Other (please specify)	7%	8%	5%	3%	3%
Total	255%	258%	252%	228%	248%

Q8a. Did your organization ever experience a BEC/spoofing /impersonation attack?	FY2026	FY2025	FY2024	FY2023	FY2022
Yes	65%	62%	57%	54%	51%
No (please skip to Q10a)	31%	32%	38%	41%	40%
Unsure (please skip to Q10a)	4%	6%	5%	5%	9%
Total	100%	100%	100%	100%	100%

Q8b. If yes, how many BEC/spoofing/impersonation attacks did your organization experience over the past two years?	FY2026	FY2025	FY2024	FY2023	FY2022
One	50%	53%	53%	40%	49%
Two to five	21%	19%	21%	24%	31%
Six to 10	15%	16%	15%	19%	12%
More than 10	14%	12%	11%	17%	8%
Total	100%	100%	100%	100%	100%
Extrapolated value	4.1	3.9	3.8	4.8	3.5

Q9a. Did the BEC/spoofing/impersonation attack result in a disruption in patient care operations?	FY2026	FY2025	FY2024	FY2023	FY2022
Yes	69%	70%	65%	69%	67%
No	25%	26%	31%	26%	30%
Unsure	6%	4%	4%	5%	3%
Total	100%	100%	100%	100%	100%

Q9b. If yes, what impact did the BEC/spoofing/impersonation attack have on patient care? Please select all that apply.	FY2026	FY2025	FY2024	FY2023	FY2022
An increase in mortality rate	26%	21%	24%	12%	21%
Delays in procedures and tests have resulted in poor outcomes	68%	65%	69%	71%	60%
Increase in complications from medical procedures	52%	55%	57%	56%	51%
Increase in patients transferred or diverted to other facilities	44%	46%	50%	46%	45%
Longer length of stay	50%	51%	52%	55%	48%
Other (please specify)	5%	5%	4%	4%	2%
Total	245%	243%	256%	244%	227%

Q10a. Did your organization ever experience attacks against its supply chain?	FY2026	FY2025	FY2024	FY2023	FY2022
Yes	50%	44%	68%	64%	50%
No (please skip to Q12a)	47%	54%	28%	30%	44%
Unsure (please skip to Q12a)	3%	2%	4%	6%	6%
Total	100%	100%	100%	100%	100%

Q10b. If yes, how many successful supply chain attacks did your organization experience over the past two years?	FY2026	FY2025	FY2024	FY2023	FY2022
One	50%	53%	46%	36%	44%
Two to five	21%	22%	26%	33%	29%
Six to 10	15%	16%	19%	21%	19%
More than 10	14%	9%	9%	10%	8%
Total	100%	100%	100%	100%	100%
Extrapolated value	4.1	3.7	4.0	4.2	3.9

Q11a. Did the supply chain attacks result in a disruption in patient care operations?	FY2026	FY2025	FY2024	FY2023	FY2022
Yes	90%	87%	82%	77%	70%
No	9%	11%	18%	18%	24%
Unsure	1%	2%	0%	5%	6%
Total	100%	100%	100%	100%	100%

Q11b. If yes, what impact did the supply chain attacks have on patient care? Please select all that apply.	FY2026	FY2025	FY2024	FY2023	FY2022
An increase in mortality rate	35%	32%	26%	21%	23%
Delays in procedures and tests have resulted in poor outcomes	47%	51%	48%	50%	54%
Increase in complications from medical procedures	53%	49%	51%	45%	48%
Increase in patients transferred or diverted to other facilities	30%	32%	38%	39%	40%
Longer length of stay	39%	40%	45%	48%	51%
Other (please specify)	0%	2%	3%	4%	3%
Total	204%	206%	211%	207%	219%

Part 2. Protecting the cloud

Q12a. Will your organization move its clinical applications to the cloud?	FY2026	FY2025
Yes, we have moved clinical applications to the cloud	35%	30%
Yes, we plan to move clinical applications to the cloud in the next six months	12%	9%
Yes, we plan to move clinical applications to the cloud within the next year	9%	8%
Yes, we plan to move clinical applications to the cloud in the next one to two years	14%	15%
Yes, we plan to move clinical applications to the cloud but there is no timeline	9%	13%
No, we have no plans to move applications to the cloud (please skip to Q15)	21%	25%
Total	100%	100%

Q12b. If yes, what type of cloud environment have you or will you move clinical applications to?	FY2026	FY2025
Public cloud	32%	34%
Private cloud	23%	21%
Hybrid cloud	24%	23%
Hosted	21%	22%
Total	100%	100%

Q12c. If yes, using the following 10-point scale, please rate how effective your organization is in securing clinical applications in the cloud from 1 = not effective to 10 = highly effective.	FY2026	FY2025
1 or 2	8%	16%
3 or 4	12%	13%
5 or 6	19%	17%
7 or 8	25%	23%
9 or 10	36%	31%
Total	100%	100%
Extrapolated value	6.88	6.30

Q13a. Did your organization ever experience a successful cloud/account compromise?	FY2026	FY2025	FY2024	FY2023	FY2022
Yes	76%	72%	69%	63%	54%
No (please skip to Q15)	23%	28%	29%	33%	41%
Unsure (please skip to Q15)	1%	0%	2%	4%	5%
Total	100%	100%	100%	100%	100%

Q13b. How many times have attackers compromised cloud-based user accounts within your organization over the past two years?	FY2026	FY2025	FY2024	FY2023	FY2022
Once	3%	2%	0%	0%	5%
2 to 5	9%	10%	13%	12%	9%
6 to 10	13%	11%	12%	14%	6%
11 to 15	15%	16%	16%	10%	9%
16 to 20	22%	23%	21%	21%	22%
21 to 25	18%	15%	19%	19%	22%
26 to 50	12%	14%	13%	16%	18%
More than 50	8%	9%	6%	8%	9%
Total	100%	100%	100%	100%	100%
Extrapolated value	20.4	21.2	19.9	21.4	21.7

Q13c. Which cloud-based user accounts/collaboration tools were most attacked in your organization? Please select all that apply.	FY2026	FY2025	FY2024	FY2023
Email	50%	45%	59%	49%
Text messaging	64%	59%	61%	45%
Zoom/Skype/Videoconferencing	56%	54%	56%	53%
Teams/Slack/Office collaboration tools	58%	43%	47%	49%
Project management tools	34%	29%	31%	53%
OneDrive/DropBox/Document/file-sharing tools	39%	35%	47%	49%
System-generated email	18%	21%	23%	51%
Virtual desktop infrastructure (VDI)	28%	25%	24%	
Total	347%	348%	348%	349%

Q14a. Did the cloud/account compromises result in a disruption in patient care operations?	FY2026	FY2025	FY2024	FY2023	FY2022
Yes	65%	61%	57%	49%	64%
No	29%	31%	34%	40%	32%
Unsure	6%	8%	9%	11%	4%
Total	100%	100%	100%	100%	100%

Q14b. If yes, what impact did the cloud/account compromises have on patient care? Please select all that apply.	FY2026	FY2025	FY2024	FY2023	FY2022
An increase in mortality rate	35%	36%	32%	29%	18%
Delays in procedures and tests have resulted in poor outcomes	40%	35%	44%	47%	49%
Increase in complications from medical procedures	59%	61%	56%	53%	51%
Increase in patients transferred or diverted to other facilities	44%	40%	36%	37%	37%
Longer length of stay	50%	52%	52%	48%	50%
Other (please specify)	5%	4%	1%	3%	2%
Total	233%	228%	221%	217%	207%



Part 3. Data loss protection/exfiltration

Q15. How many data loss and exfiltration incidents involving sensitive and confidential healthcare data occurred within your organization over the past two years?	FY2026	FY2025	FY2024	FY2023
Once	3%	4%	0%	8%
2 to 5	8%	9%	8%	5%
6 to 10	12%	13%	14%	12%
11 to 15	16%	19%	25%	24%
16 to 20	19%	21%	12%	10%
21 to 25	18%	20%	25%	23%
26 to 50	15%	9%	10%	13%
More than 50	8%	5%	6%	5%
Total	100%	100%	100%	100%
Extrapolated value	21.0	18.4	20.0	19.4

Q16. What were the root cause(s) of the data loss and exfiltration incident? Please select all that apply.	FY2026	FY2025	FY2024
Accidental data loss	26%	23%	26%
Employee negligence because of not following policies	32%	35%	31%
Privilege access abuse	27%	25%	20%
Malicious insiders	21%	18%	15%
Employee sends PII or PHI to an unintended recipient via email	23%	25%	21%
Use of stolen credentials	21%	15%	11%
Social engineering	15%	14%	13%
Exploitation of vulnerabilities	12%	8%	9%
Phishing	10%	11%	12%
AI agents without guardrails	24%		
Unsure	14%	16%	17%
Total	225%	190%	175%

Q17a. Did the data loss or exfiltration result in a disruption in patient care operations?	FY2026	FY2025	FY2024	FY2023
Yes	54%	55%	51%	43%
No, Please skip to Q18	43%	40%	45%	51%
Unsure, Please skip to Q18	3%	5%	4%	6%
Total	100%	100%	100%	100%

Q17b. If yes, what impact did the data loss or exfiltration incident have on patient care? Please select all that apply.	FY2026	FY2025	FY2024	FY2023
An increase in mortality rate	56%	54%	50%	46%
Delays in procedures and tests have resulted in poor outcomes	34%	36%	37%	34%
Increase in complications from medical procedures	35%	31%	34%	38%
Increase in patients transferred or diverted to other facilities	28%	29%	33%	36%
Longer length of stay	28%	27%	21%	24%
Other (please specify)	2%	4%	3%	6%
Total	183%	181%	178%	184%

Q18. What security methods and technologies does your organization use to reduce phishing and other email-based attacks? Please select all that apply.	FY2026	FY2025	FY2024
Secure email gateway (SEG)	53%	52%	45%
API-based email security	51%		
Mix of SEG and API-based email security	48%		
Domain-based Message Authentication (DMARC)	40%	43%	42%
Email data loss prevention	41%	36%	39%
Anti-virus/anti-malware	54%	49%	53%
Multi-factor authentication	51%	54%	49%
Patch & vulnerability management	49%	51%	52%
Managed Security Service Provider (MSSP)	39%	43%	46%
Firewalls	31%	33%	36%
AI/ML	47%	41%	44%
Threat intelligence	38%	38%	41%
Other (please specify)	7%	8%	4%
Total	549%	448%	451%

Q19. Using the following 10-point scale, please rate how important is understanding human behavior to protecting email on a scale from 1 = not important to 10 = very important.	FY2026
1 or 2	9%
3 or 4	12%
5 or 6	15%
7 or 8	28%
9 or 10	36%
Total	100%
Extrapolated value	6.90

Q20. What security methods and technologies has your organization implemented to prevent data loss or an exfiltration incident? Please select all that apply.	FY2026	FY2025	FY2024
Policy fine tuning to prevent data loss	31%	27%	23%
Secure web gateway (SWG)	26%	28%	28%
Cloud security tools	34%	35%	44%
Data security posture management (DSPM)	29%	31%	
Insider threat management (ITM)	42%	43%	
Web isolation technology	30%	33%	29%
Encryption for data at rest	37%	38%	41%
Encryption for data in transit	50%	43%	46%
Endpoint data loss prevention	49%	45%	
Network data loss prevention	46%	44%	
Email data loss prevention	34%	38%	
Cloud data loss prevention	33%	35%	
Web data loss prevention	28%	31%	
IT/IT security team triages incidents	31%	29%	25%
Manual policy orchestration	36%	37%	29%
Other (please specify)	4%	5%	3%
Total	540%	542%	304%

Q21a. Does your organization take steps to address the risk of employees' lack of awareness about cybersecurity threats?	FY2026	FY2025	FY2024	FY2023	FY2022
Yes	75%	76%	71%	65%	59%
No	23%	20%	29%	30%	35%
Unsure	2%	4%	0%	5%	6%
Total	100%	100%	100%	100%	100%

Q21b. If yes, what steps does it take? Please select all that apply.	FY2026	FY2025	FY2024	FY2023	FY2022
Regular training and awareness programs	65%	63%	59%	57%	63%
Simulations of phishing attacks	56%	47%	45%	40%	41%
AI-related threats such as deep fakes, AI phishing	36%				
Monitoring of employees	50%	51%	53%	54%	59%
Audits and assessments of areas most vulnerable to employees' lack of awareness	47%	44%	39%	43%	39%
Include user's compliance with privacy and security policies in performance evaluations	40%	37%	34%	36%	35%
Other (please specify)	5%	6%	5%	4%	3%
Total	299%	248%	235%	234%	240%

Q22. 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?	FY2026	FY2025	FY2024	FY2023
1 or 2	12%	11%	11%	18%
3 or 4	18%	19%	23%	33%
5 or 6	15%	11%	20%	14%
7 or 8	25%	28%	26%	16%
9 or 10	30%	31%	20%	19%
Total	100%	100%	100%	100%
Extrapolated value	6.36	6.48	5.92	5.20

Q23. 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?	FY2026	FY2025	FY2024	FY2023
1 or 2	13%	9%	15%	15%
3 or 4	16%	11%	23%	20%
5 or 6	15%	16%	23%	26%
7 or 8	29%	32%	24%	25%
9 or 10	27%	32%	15%	14%
Total	100%	100%	100%	100%
Extrapolated value	6.32	6.84	5.52	5.56

Q24. 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?	FY2026	FY2025	FY2024	FY2023
1 or 2	10%	8%	11%	15%
3 or 4	12%	10%	18%	17%
5 or 6	16%	12%	23%	21%
7 or 8	28%	30%	23%	25%
9 or 10	34%	40%	25%	22%
Total	100%	100%	100%	100%
Extrapolated value	6.78	7.18	6.16	5.94

Part 4. AI and machine learning in healthcare

Q25. Has your organization adopted AI? Please select one choice only.	FY2026	FY2025	FY2024
Yes, AI is embedded in cybersecurity	24%	30%	28%
Yes, AI is embedded in both cybersecurity and patient care	21%	27%	26%
No, but we plan to adopt AI in the future (please skip to Part 5)	30%	21%	26%
We don't have plans to adopt AI (please skip to Part 5)	25%	22%	20%
Total	100%	100%	100%

Q26. What AI tasks and applications does your organization use? Please select all that apply.	FY2026
Medical imaging and diagnostics	62%
Administrative automation	63%
Medical scribes	44%
Clinical decision support	19%
Virtual nursing/patient monitoring	48%
Robotic surgery	12%
Other (please specify)	0%
Total	248%

Q27a. Does your organization have controls in place to govern sensitive data used in AI systems?	FY2026
Yes	40%
No	60%
Total	100%

Q27b. If yes, what controls are in place to govern sensitive data used in AI systems? Please select all that apply.	FY2026
Data minimization practices	39%
De-identification/anonymization	42%
Access controls	46%
Encryption at rest/in use	43%
Data lineage tracking	29%
DSPM for AI data	36%
Strong encryption and data access controls for AI training data	52%
All AI outputs are monitored by professionals to prevent mistakes	46%
Regularly test AI models for "drift", bias and vulnerabilities	23%
Total	356%

Q28. To what extent do employees use generative AI tools approved or unapproved?		FY2026
Widely used with governance		23%
Widely used without governance		23%
Limited use		31%
Not used		20%
Unsure		3%
Total		100%
Q29. Does your organization have visibility into employee use of unsanctioned AI tools?		FY2026
Full visibility		32%
Partial visibility		42%
No visibility		24%
Unsure		2%
Total		100%
Q30. Which AI-specific risks are you most concerned about? Please select the top three concerns		FY2026
Data leakage via prompts		36%
Model inversion/training data extraction		27%
Prompt injection attacks		30%
Malicious or biased outputs affecting care decisions		32%
Unauthorized AI model access		29%
Supply chain risk from AI vendors		40%
AI-generated phishing/social engineering		34%
Vulnerabilities in connected devices		28%
Inadequate privacy protections		14%
Non-compliant tools		11%
Adversarial attacks		19%
Total		300%
Q31a. Does your organization use security measures to protect AI systems, agents and generative AI usage?		FY2026
Yes		42%
No (please skip to Q32)		48%
Unsure (please skip to Q32)		10%
Total		100%

Q31b. If yes, what security measures does your organization apply specifically to protect AI systems, agents and generative AI usage? Please select all that apply.	FY2026
AI usage discovery and visibility controls	33%
Runtime policy enforcement for AI interactions and workflows	24%
AI data protection and data loss prevention (DLP)	45%
AI data governance and access controls	50%
Protection against prompt injection and AI-targeted attacks	31%
AI agent governance and behavior control	19%
Monitoring and auditing of AI activity	23%
Secure AI integration and workflow protection	17%
Intent-based threat detection for AI systems	30%
Collaboration and communication security for AI-assisted workflows	25%
Automated security response using AI agents	20%
Other (please specify)	4%
Total	321%

Q32. 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.	FY2026	FY2025	FY2024
AI tools/technology we need are not available	21%	22%	25%
We can't apply AI-based controls that span across the entire enterprise	29%	25%	26%
We can't create a unified view of AI users across the enterprise	3%	5%	4%
There are errors and inaccuracies in AI decision rules	30%	21%	19%
There are errors and inaccuracies in data inputs ingested by AI technology (engine)	26%	33%	32%
There is a heavy reliance on legacy IT environments	25%	26%	23%
There are Interoperability issues among AI technologies	32%	34%	32%
There is a lack of mature and/or stable AI technologies	29%	28%	34%
Other (please specify)	5%	6%	5%
Total	200%	200%	200%

Part 5. Cyberattack experience

Q33. How many cyberattacks has your organization experienced over the past 12 months?	FY2026	FY2025	FY2024	FY2023	FY2022
None (please skip to Part 6)	3%	7%	8%	12%	11%
1 to 5	10%	10%	15%	13%	12%
6 to 10	21%	22%	23%	21%	15%
11 to 25	15%	16%	12%	11%	13%
26 to 50	11%	13%	11%	9%	11%
51 to 100	14%	11%	12%	18%	23%
More than 100	26%	21%	19%	16%	15%
Total	100%	100%	100%	100%	100%
Extrapolated value	50.5	43.3	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.

Q34. Approximately, how much was the total cost from the one most significant cybersecurity attack in the past 12 months?	FY2026	FY2025	FY2024	FY2023	FY2022
None	0%	0%	0%	0%	0%
Less than \$10,000	0%	2%	0%	0%	0%
\$10,001 to \$100,000	7%	7%	9%	7%	6%
\$100,001 to \$250,000	9%	12%	10%	13%	12%
\$250,001 to \$500,000	18%	15%	14%	18%	18%
\$500,001 to \$1,000,000	21%	19%	18%	14%	16%
\$1,000,001 to \$5,000,000	22%	21%	21%	19%	21%
\$5,000,001 to \$10,000,000	11%	14%	15%	11%	13%
\$10,000,001 to \$25,000,000	9%	8%	9%	15%	12%
More than \$25,000,000	3%	2%	4%	3%	2%
Cannot estimate	0%	0%	0%	0%	0%
Total	100%	100%	100%	100%	100%
Extrapolated value	\$4,204,600	\$3,903,780	\$4,740,400	\$4,991,500	\$4,429,000

Part 6. Security spending & investment

Q36.What is your organization’s approximate annual budget for IT?	FY2026	FY2025	FY2024	FY2023	FY2022
Less than \$1,000,000	0%	2%	0%	2%	0%
1,000,000 to \$5,000,000	3%	5%	4%	3%	2%
5,000,001 to \$10,000,000	5%	7%	9%	8%	6%
10,000,001 to \$25,000,000	14%	12%	11%	11%	10%
25,000,001 to \$50,000,000	20%	18%	20%	25%	17%
\$50,000,001 to \$100,000,000	25%	26%	25%	23%	28%
\$100,000,000+	33%	30%	31%	25%	37%
Cannot estimate	0%	0%	0%	3%	0%
Total	100%	100%	100%	100%	100%
Extrapolated value	\$68,765,000	\$65,043,000	\$66,170,000	\$59,258,000	\$75,200,000

Q37. What percentage of your organization’s IT budget is dedicated to information security?	FY2026	FY2025	FY2024	FY2023	FY2022
Less than 5%	0%	5%	4%	5%	3%
5 to 10%	9%	10%	4%	8%	7%
11 to 15%	13%	16%	19%	21%	23%
16 to 20%	25%	22%	33%	37%	35%
21 to 30%	31%	27%	25%	19%	21%
More than 30%	22%	20%	10%	10%	11%
Total	100%	100%	100%	100%	100%
Extrapolated value	22%	21%	19%	18%	19%

Part 7. Your role and organizational characteristics

D1. What best describes your organization?	FY2026	FY2025	FY2024	FY2023	FY2022
Public healthcare provider	22%	18%	21%	19%	19%
Private healthcare provider	18%	21%	22%	20%	22%
Healthcare insurer	18%	20%	19%	18%	13%
Payer	11%	10%	8%	14%	15%
Healthcare insurance	10%	11%	12%	11%	9%
Life sciences	8%	9%	6%	5%	8%
Biotech	6%	5%	4%	4%	5%
Pharma	7%	6%	8%	9%	9%
Total	100%	100%	100%	100%	100%

D2. What organizational level best describes your current position?	FY2026	FY2025	FY2024	FY2023	FY2022
Senior Executive/VP	7%	6%	7%	8%	9%
Director	9%	10%	10%	17%	16%
Manager	26%	25%	27%	29%	23%
Supervisor	21%	23%	25%	23%	14%
Technician/Staff	28%	27%	26%	19%	33%
Contractor	6%	7%	5%	4%	5%
Other (please specify)	3%	2%	0%	0%	0%
Total	100%	100%	100%	100%	100%

D3. Check the primary person you or your IT security leader reports to within the organization.	FY2026	FY2025	FY2024	FY2023	FY2022
CEO/Executive Committee	7%	8%	7%	9%	8%
Chief Information Officer	18%	16%	18%	19%	21%
Chief Information Security Officer	23%	22%	21%	20%	19%
Chief Risk Officer	10%	9%	8%	7%	6%
Chief Security Officer	4%	5%	6%	5%	4%
Chief Technology Officer	9%	8%	7%	8%	7%
Compliance Officer	8%	10%	9%	8%	9%
Data Center Management	7%	6%	8%	9%	10%
Cloud Administration	11%	12%	13%	11%	12%
Other (please specify)	3%	4%	3%	4%	4%
Total	100%	100%	100%	100%	100%

D4. What is the headcount of your organization?	FY2026	FY2025	FY2024	FY2023	FY2022
Less than 500	16%	18%	19%	18%	16%
500 to 1,000	22%	25%	23%	21%	25%
1,001 to 5,000	19%	15%	17%	18%	19%
5,001 to 10,000	10%	12%	12%	10%	9%
10,001 to 25,000	13%	12%	10%	12%	13%
25,001 to 75,000	12%	11%	13%	14%	12%
More than 75,000	8%	7%	6%	7%	6%
Total	100%	100%	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.

proofpoint®

About Proofpoint, Inc.

Proofpoint, Inc. is a global leader in human and agent cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 14,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration, data and AI security platform helps organizations of all sizes protect their people and adopt AI securely and confidently. Learn more at www.proofpoint.com.

Connect with Proofpoint on **LinkedIn**.

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.



**DISCOVER THE
PROOFPOINT PLATFORM**