REPORT

The 2025 Study on Cyber Insecurity in Healthcare

The cost and impact on patient safety and care

Table of contents

Part 1. Executive Summary

The 2025 Study on Cyber Insecurity in Healthcare

This year's study finds that healthcare organizations' ability to protect confidential patient data and ensure the highest quality of medical care is increasingly at risk, underscoring the need for a more human-centric security approach.

This fourth 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 677 IT and IT security practitioners in U.S. healthcare organizations who are responsible for participating in such cybersecurity strategies as setting IT cybersecurity priorities, managing budgets and selecting vendors and contractors.

Healthcare organizations remain frequent targets, with cyberattacks continuing to disrupt patient care. According to the research, 93 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 43, a 3-point increase from 40 in 2024.

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 72 percent report disruption to patient care, a 3-point jump from 69 percent in 2024.

While the cost of cyberattacks has declined, they remain a significant financial burden. 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 $3.9 million, down from $4.7 million in 2024 but still substantial. This includes all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunities.

93%

of organizations experienced an average of 43 cyberattacks in the past 12 months

72%

reported disruption to patient care

$3.9M

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

Operational disruptions stemming from system availability problems remain the most expensive consequence. 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 $1,210,172, a decrease from $1,469,524 in 2024.
- **Users' idle time and lost productivity** dropped to $858,832 from $995,484 in 2024. These costs were due to downtime or system performance delays.
- **The cost of the time required to ensure the impact on patient care is corrected** decreased to $702,680 from an average of $853,272 in 2024.
- **The damage or theft of IT assets and infrastructure** averaged $624,605, down slightly from $711,060 in 2024.
- **Remediation and technical support activities**, including forensic investigations, incident response activities, help desk and delivery of services to patients saw the largest drop (28.6%) from $711,060 in 2024 to $507,491 in 2025.

For the first time, this year's study examined plans to secure clinical operations in the cloud. Thirty percent of respondents say their organizations have moved clinical applications to the cloud. Forty-five percent say their organizations will move clinical applications to the cloud in the next six months (9 percent), within the next year (8 percent), in the next one to two years (15 percent) or eventually (13 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.

75%

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

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:

Cloud/account compromise. 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.

For the fourth consecutive year, frequent attacks against the cloud make it the top cybersecurity threat. Nearly two-thirds of respondents (64 percent) say their organizations are vulnerable or highly vulnerable to a cloud/account compromise. Seventy-two percent say their organizations have experienced cloud/account compromises, an increase from 69 percent in 2024. These organizations had an average of 21 such compromises in the past two years.

72%

of organizations experienced 21 cloud/account compromises, on average

Supply chain attacks. 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.

Fewer organizations are experiencing supply chain attacks. Forty-four percent of respondents say their organizations experienced an attack against its supply chains, a significant decline from 68 percent in 2024. Of these organizations, on average they experienced four supply chain attacks in the past two years. Fifty-seven percent say their organizations are very or highly vulnerable to supply chain attacks.

Supply chain attacks decreased significantly, 44% (2025) vs. 68% (2024)

Ransomware. 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.

Fewer organizations are paying a ransom, but the amount paid has increased.
The costliest ransom paid (extrapolated value) was $1.2 million. This up from $1.1 million in 2024 and a staggering 60 percent increase from $771,905 in 2022, when we first began tracking this data. This continuous rise underscores how threat actors are demanding and receiving larger payouts, even as payment rates declined (33 percent in 2025 vs. 36 percent in 2024). Fifty-five percent of respondents believe their organizations are vulnerable or highly vulnerable to a ransomware attack. In the past two years, organizations that had ransomware attacks (61 percent) experienced an average of five such attacks. The combination of threat exposure and escalating ransom demands creates operational and financial risk for healthcare organizations.

$1.2M

Average total cost for the highest ransom payment

Business email compromise (BEC)/spoofing/impersonation.
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 are designed to gather data for other criminal activities, attorney impersonations and CEO fraud.

Concerns about these attacks have decreased significantly since 2022, when 64 percent of respondents said their organizations were very or highly vulnerable.
In the 2025 research, 53 percent say their organizations are vulnerable or highly vulnerable to a BEC/spoofing/impersonation incident, a very slight increase from 52 percent in 2024. And 62 percent say their organizations experienced an average of four attacks in the past two years. In 2024, 57 percent said they had an average of four attacks in the past two years.

**Concerns about BEC/ spoofing/impersonation attacks decreased from the study's first year,
53% (2025) vs. 64% (2022)**

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

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 72 percent report disruption to patient care, a 3-point jump from 69 percent in 2024.

As shown in Table 1, an average of 54 percent report poor patient outcomes due to increases in medical procedure complications. An average of 53 percent saw an increase in a longer length of stay and an average of 29 percent say patient mortality rates increased.

Table 1

Percentage of poor outcomes for four types of cyberattacks	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	50%	67%	56%	50%	27%
BEC	55%	51%	65%	46%	21%
Supply Chain	49%	40%	51%	32%	32%
Cloud/Account Compromise	61%	52%	35%	40%	36%
2025 Average Percentage	**54%**	**53%**	**52%**	**42%**	**29%**

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. While fewer organizations in this year's research had a supply chain attack (44 percent in 2025 vs. 68 percent in 2024), 87 percent of those respondents say it disrupted patient care, an increase from 82 percent in 2024. Patients were primarily impacted by delays in procedures and tests that resulted in poor outcomes (51 percent) and an increase in complications from medical procedures (49 percent). Mortality rates increased significantly from 26 percent in 2024 to 32 percent in 2025.

BEC/spoofing/impersonation attacks cause delays in procedures and tests. Sixty-two percent of respondents say their organizations experienced a BEC/spoofing/ impersonation incident and had an average of four attacks. Of these respondents, 70 percent say a BEC/spoofing/impersonation attack against their organizations disrupted patient care. Sixty-five percent say the attacks caused delays in procedures and tests that have resulted in poor outcomes, and 55 percent say it increased complications from medical procedures.

Ransomware attacks cause delays in patient care. Sixty-one percent of respondents say their organizations experienced an average of five successful ransomware attacks. Sixty-seven percent say ransomware attacks had a negative impact on patient care. Of these respondents, 67 percent say it resulted in longer lengths of stay, which affects organizations' ability to care for patients. Fifty-six percent say that it resulted in delays in procedures and tests, which caused a disruption to patient care.

Cloud-based user accounts/collaboration tools that enable productivity are most often attacked. Seventy-two percent of respondents say their organizations experienced an average of 21 cloud/account compromises, a slight increase from 20 in 2024. In this year's study, 61 percent say the cloud/account compromises resulted in disruption in patient care, an increase from 57 percent in 2024. Sixty-one percent say cloud/account compromises increased complications from medical procedures and 52 percent say it resulted in longer length of stay. The tools most often attacked are text messaging (59 percent), Zoom/Skype/video conferencing (54 percent) and email (45 percent).

Data loss or exfiltration disrupts patient care and can increase mortality rates. Ninety-six 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. On average, organizations experienced 18 such incidents in the past two years and 55 percent of respondents say they impacted patient care. Of these respondents, 54 percent say it increased the mortality rate and 36 percent say it caused delays in procedures and tests that resulted in poor outcomes.

Employee negligence because of not following policies (35 percent of respondents), privilege access abuse (25 percent) and employee sends PII or PHI to an unintended recipient via email (25 percent) are the primary root causes of the incident.

For the fourth year in a row, the data reinforces a sobering reality: cyberthreats aren't just IT security issues, they're clinical risks. When care is delayed, disrupted or compromised due to a cyberattack, patient outcomes are impacted, and lives are potentially put at risk.

Other key trends in cyber insecurity

Human error drove most data loss and exfiltration incidents

35%

say employees not following policies were the cause of data loss or exfiltration. There was a tie for second place:

25%

say data loss was caused by privilege access abuse

25%

say it was from an employee sending PII or PHI to the wrong recipient via email

Security awareness training programs continue to be essential

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

76%

in 2025

71%

in 2024

Of this group:

63%

conduct regular training and awareness programs

51%

monitor the actions of employees

47%

use simulations of phishing attacks

Top 3 targeted cloud-based productivity tools

59%

say text messaging was the most attacked collaboration tool

54%

say Zoom/Skype/video conferencing was the second-highest attacked

45%

say email was the third-highest attacked

Insecure mobile apps remain a top concern for the second consecutive year

55%

are worried about the security risks created by insecure mobile apps (eHealth)

49%

are less worried about BYOD

38%

identified generative AI or AI tools as a cybersecurity concern, a new category in this year's study

Security spending is up because cyber safety is patient safety

Concerns about budgets decreased from

40% to 37%

$65M

The annual IT budget

21%

of IT budget dedicated to information security, a 2-point jump YoY

Top 3 cybersecurity tools to protect against email-based attacks

54%

multifactor authentication, a 5-point increase from 2024

52%

secure email gateway, a 7-point increase from 2024

51%

patch and vulnerability management

Top 3 tools to prevent identity risk and lateral movement

59%

privileged access management (PAM)

53%

identity and access management (IAM)

50%

alerts from security information and event management (SIEM) to gain visibility

Top 2 barriers to an effective cybersecurity posture

Expertise:

43%

say they lack in-house expertise

Leadership:

40%

say they lack clear leadership

Trends in AI and machine learning in healthcare

Trends in AI in healthcare

57%

say they have embedded AI in cybersecurity (30%) and in both cybersecurity and patient care (27%)

55%

say AI is very effective in improving organizations' cybersecurity posture

Using AI to protect against email-based attacks

40%

use AI and machine learning to understand human behavior

Of this group:

55%

say understanding human behavior to protect emails is very important

Using AI-based DLP to prevent data loss caused by employees

23%
say their organization has adopted AI-based DLP

29%
plan to adopt this technology in six to 12 months

56%
say AI-based DLP is very or highly effective in preventing employee-caused data loss incidents

50%
say it's very or highly effective in preventing malicious insider data loss incidents

Using AI for time, cost, and productivity

55%
say AI-based security tools will increase productivity for IT security personnel

56%
say AI simplifies patient care and administrators' work by performing tasks in less time and at a lower cost

Challenges to adopting AI

60%

say safeguarding confidential data used in organizations' AI is difficult or very difficult

34%

say interoperability issues among AI technologies deter widespread acceptance

33%

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

28%

believe there's a shortage of mature and/or stable AI tools

Part 2. Key Findings

In this section, we provide an **analysis of the fourth annual findings**. The **complete audited results are presented in the appendix of this report**. Whenever possible, we compare the 2022, 2023 and 2024 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 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

Healthcare organizations believe they are very or highly vulnerable to cyberattacks.

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

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.

As shown in Figure 1, 64 percent of respondents say their organizations are vulnerable or highly vulnerable to a cloud/account compromise and 57 percent say they are vulnerable or highly vulnerable to supply chain attacks. Slightly more than half (55 percent) of respondents say their organizations are vulnerable or highly vulnerable to ransomware attacks and 53 percent say their organizations are very or highly vulnerable to BEC/spoofing/impersonation attacks. As indicated, since 2024 vulnerabilities to all four types of cyberattacks have remained unchanged. Respondents have consistently identified cloud/account compromise as their organizations' greatest areas of vulnerability, dating back to the survey's inception in 2022.

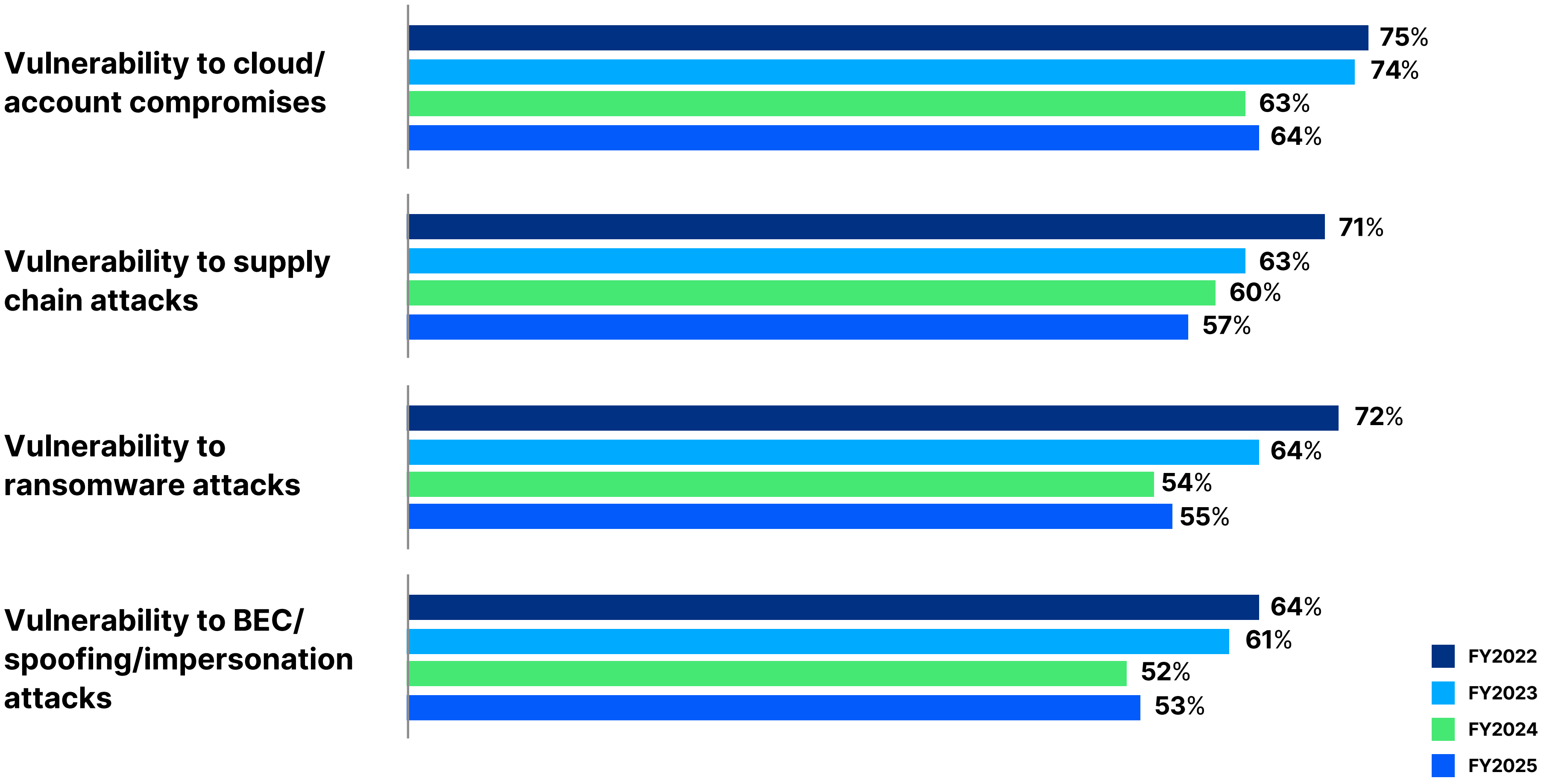


Figure 2

Insecure mobile apps (eHealth), cloud/account compromises and BYOD are considered the greatest cyber threats to healthcare organizations.

Respondents were asked to select the threats of greatest concern. The findings are presented in Figure 2. For the second year, insecure mobile apps (eHealth) are considered the top cybersecurity threat in healthcare. Organizations are less worried about BEC/spoofing/impersonation, which decreased from 46 percent in 2024 to 40 percent of respondents in 2025. Cloud/account compromise concerns decreased from 55 percent in 2024 to 49 percent of respondents in 2025.

Six responses permitted

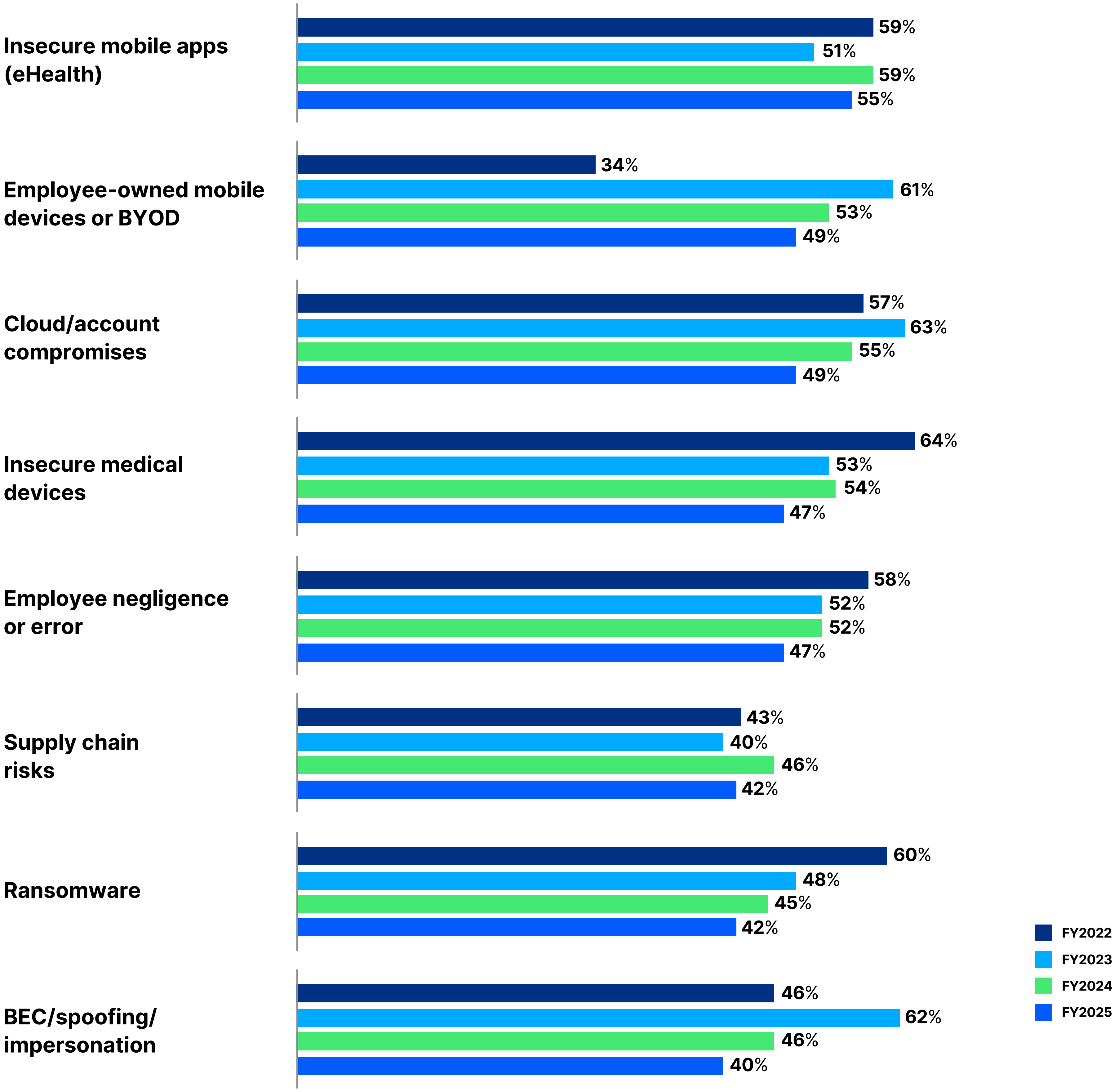


Figure 3

Healthcare organizations are more prone to successful cloud/account compromises and BEC/spoofing/impersonation attacks.

Figure 3 presents the percentage of organizations that experienced four different types of cyberattacks. For the second year, more organizations say they have experienced a cloud/account compromise (72 percent in 2025 vs. 69 percent in 2024). BEC/spoofing/impersonation attacks increased significantly from 57 percent in 2024 to 62 percent in 2025. Sixty-one percent of organizations had a ransomware attack. Far fewer organizations experienced a supply chain attack (a significant decrease from 68 percent in 2024 to 44 percent in 2025).

Yes responses presented

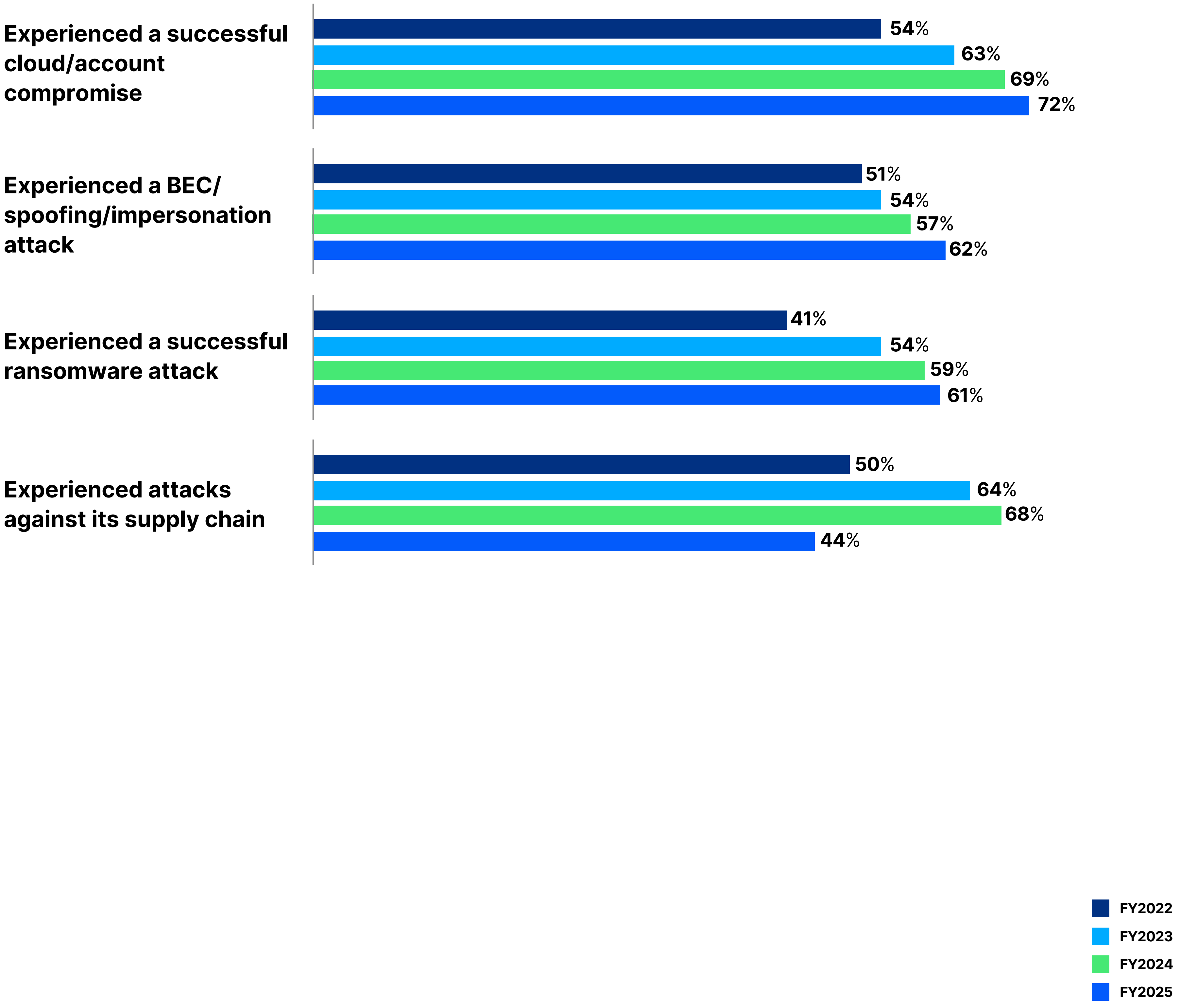


Figure 4

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

Responding organizations that experienced one of the four types of cyberattack were asked about the frequency of those attacks over the past two years. Figure 4 shows the average number of the four cyberattacks. Organizations experienced an average of 21 attacks against the cloud in 2025, which explains the previous finding that most organizations believe they are vulnerable or very vulnerable to such attacks. 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

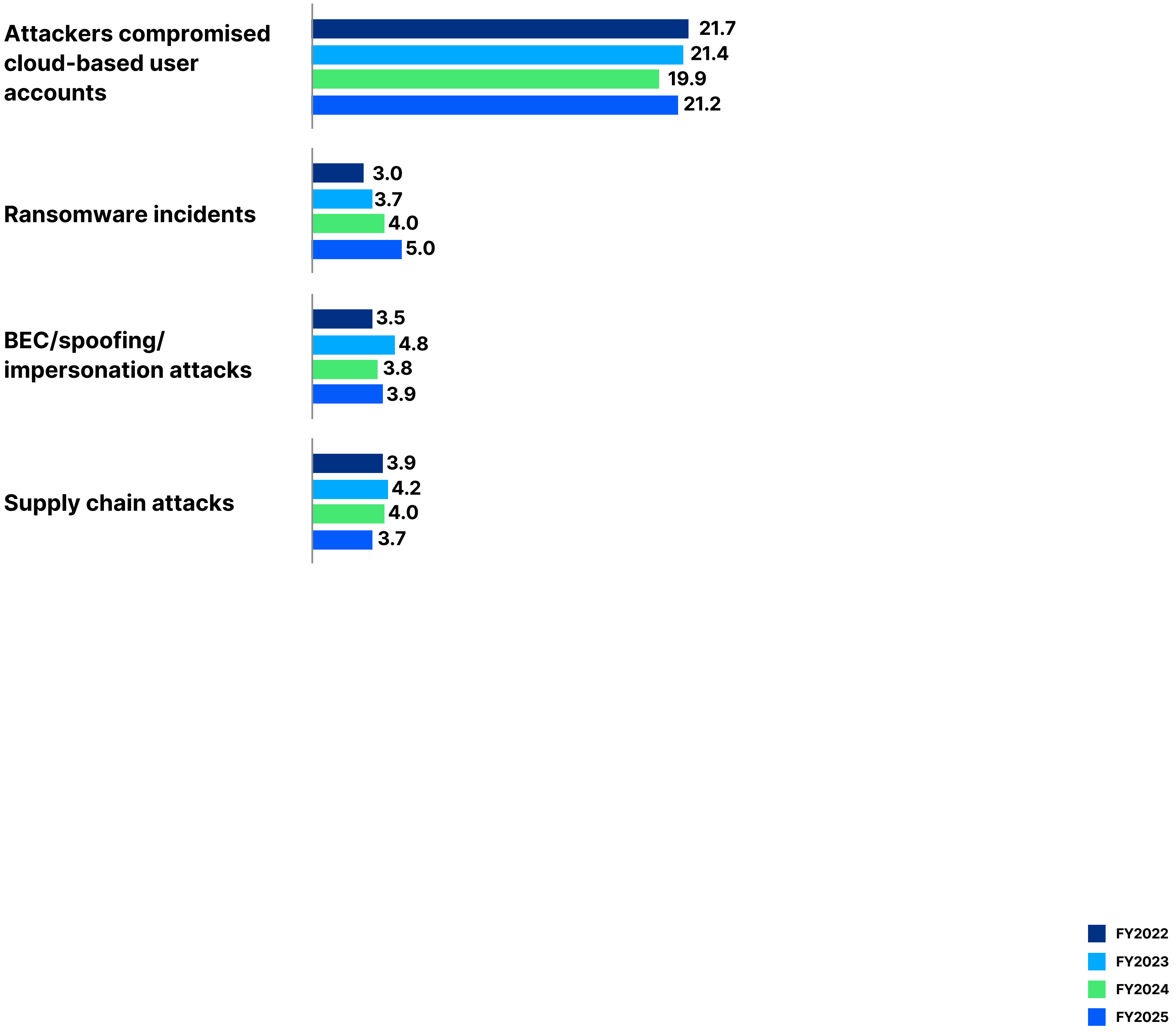


Figure 5

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

Seventy-two 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, cloud-based user accounts/collaboration tools that enable productivity were most often attacked. The tool most often attacked continues to be text messaging (59 percent). Fifty-four percent of respondents say Zoom/Skype/video conferencing is the second greatest target. A reason is the increase in remote working and the use of these tools. While attacks on email accounts decreased significantly from 59 percent in 2024 to 45 percent in 2025, email remains one of the top three most targeted collaboration tools.

More than one response permitted

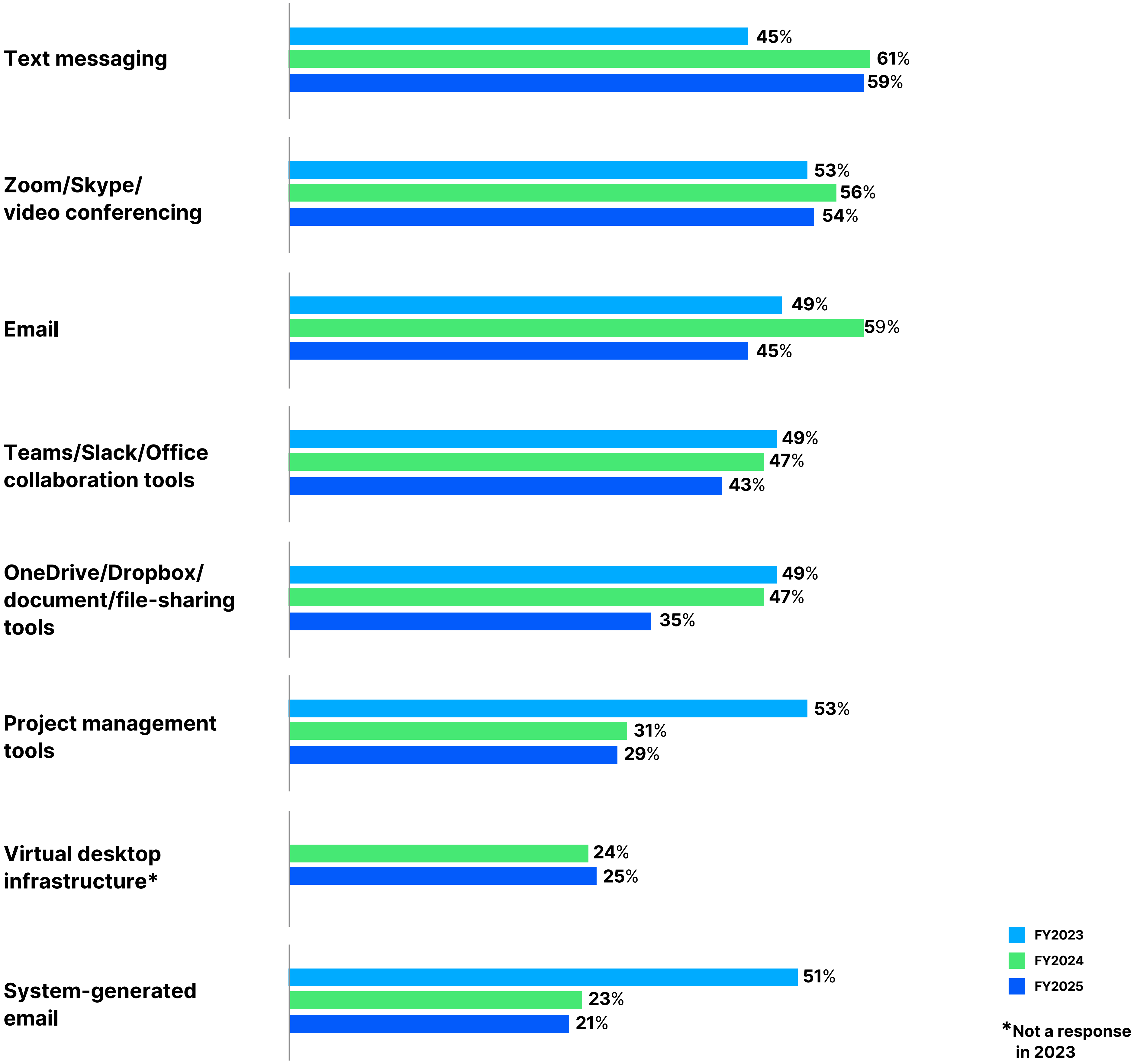


Figure 6

For the first time, this year's study examined plans to secure clinical operations in the cloud.

As shown in Figure 6, 30 percent of respondents say their organizations have moved clinical applications to the cloud. Of this group, 54 percent rate their ability to secure clinical applications in the cloud as very effective.

Forty-five percent say their organizations will move clinical applications to the cloud in the next six months (9 percent) within the next year (8 percent), in the next one to two years (15 percent) or eventually (13 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.

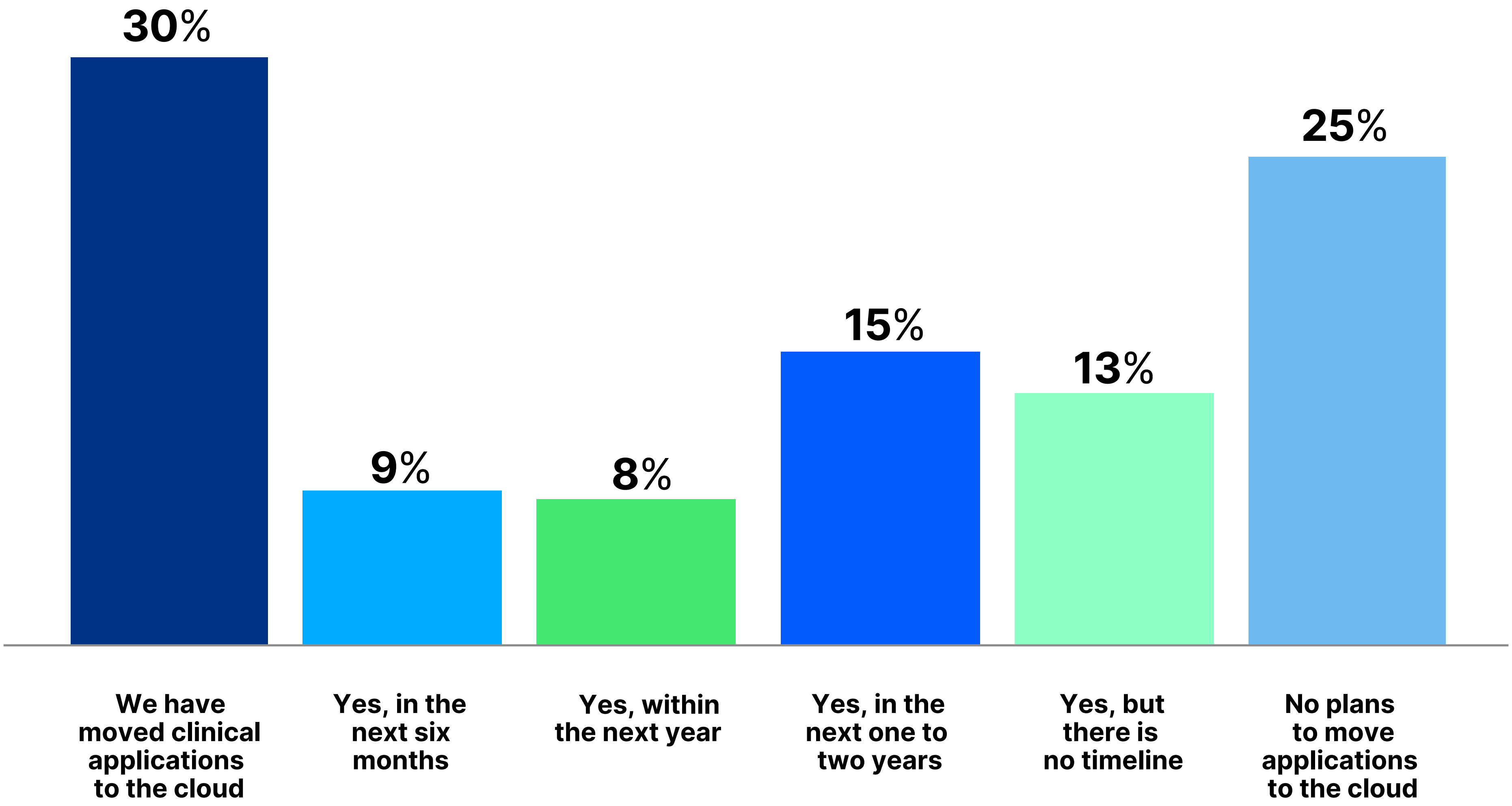
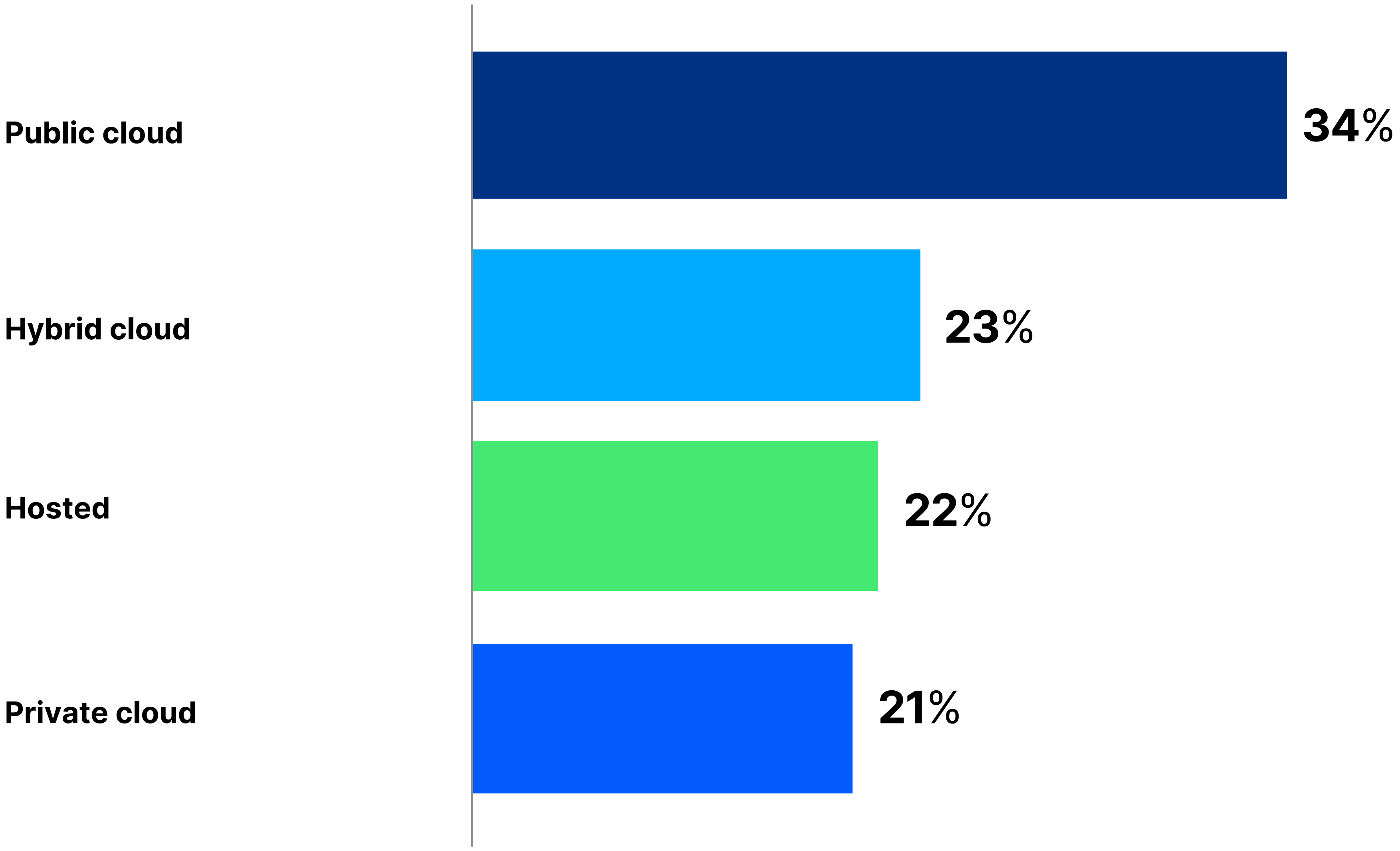


Figure 7

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

As shown in Figure 7, 34 percent of organizations say clinical applications will be moved to the public cloud. This includes 30 percent that have already migrated and 45 percent that are planning to do so.



The impact of cyberattacks on patient care

Figure 8

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 72 percent reported disruption to patient care. Specifically, attacks against the supply chain continue to have the most impact on patient care. Figure 8 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.

Forty-four percent of respondents say their organizations had a supply chain attack. Of these respondents, 87 percent say it resulted in a disruption in patient care, an increase from 82 percent in 2024 and 77 percent in 2023.

Sixty-one percent say their organizations had a ransomware attack and 67 percent of these respondents say it disrupted patient care. Seventy-two percent of organizations had cloud/account compromises and are becoming more impactful on patient care, an increase from 57 percent in 2024 to 61 percent in 2025. Sixty-two percent of organizations had a BEC/spoofing/impersonation attack and there was an increase from 65 percent to 70 percent in having an impact on patient care.

Yes responses presented

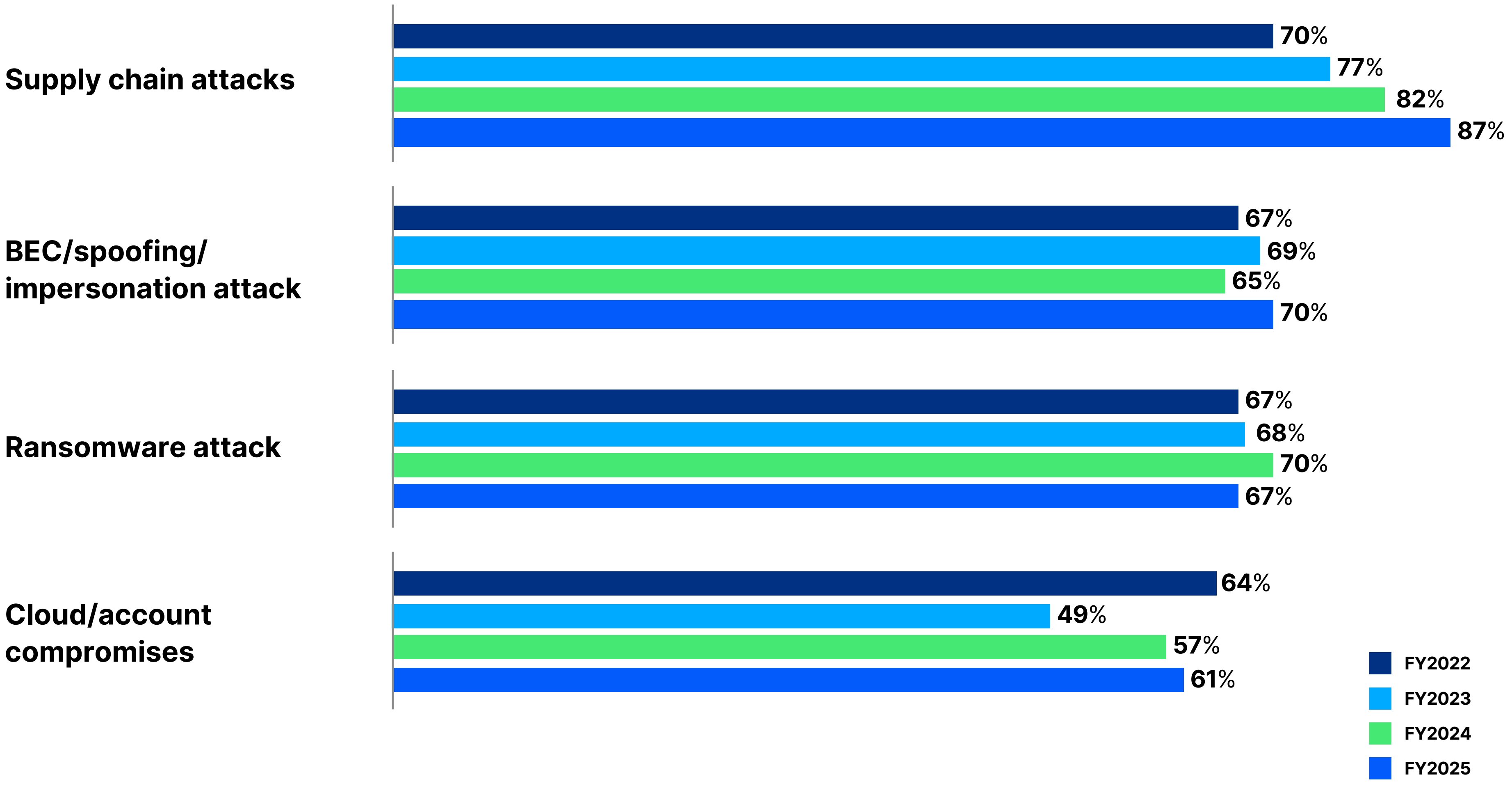
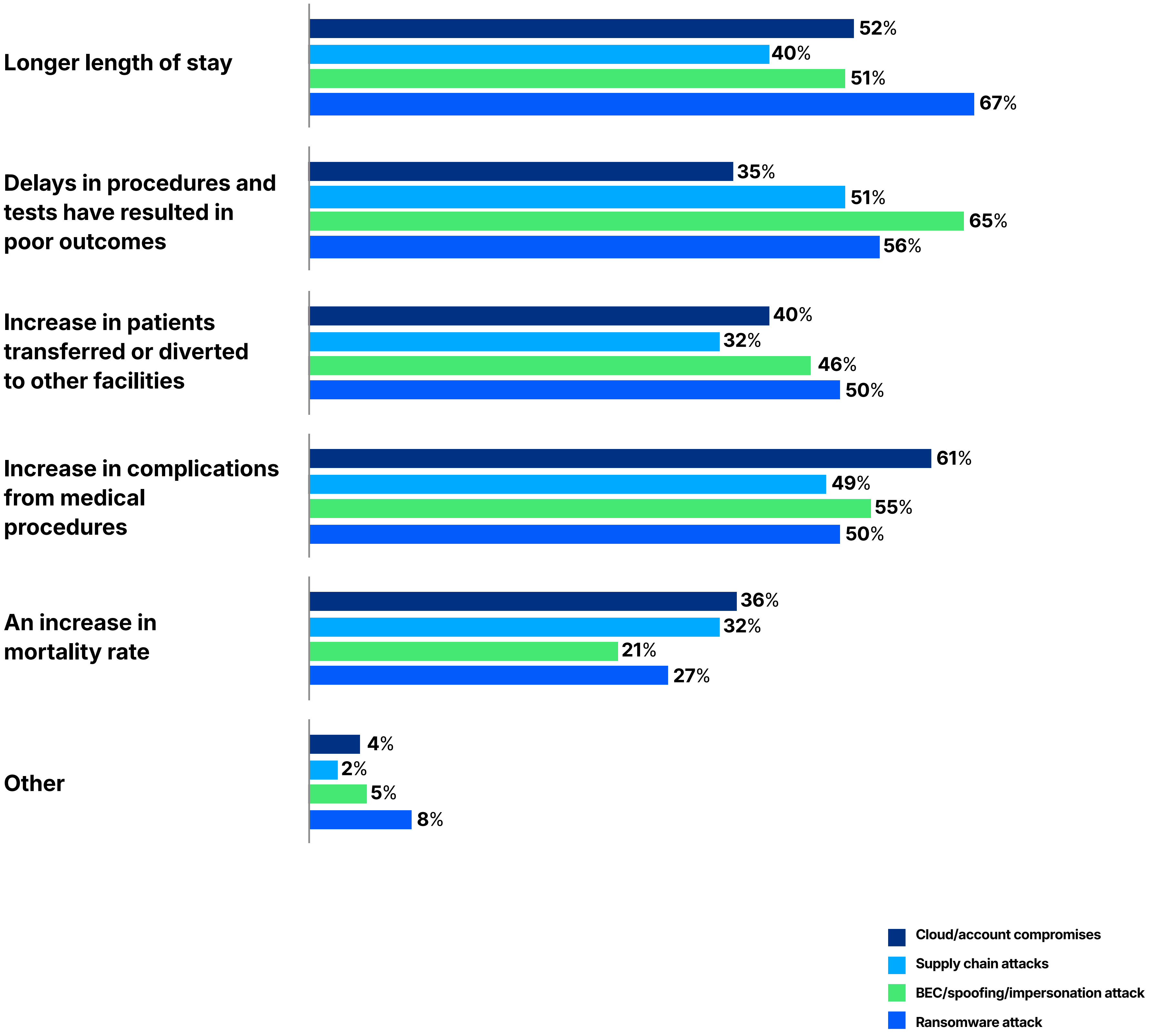


Figure 9

Ransomware attacks are most likely to result in prolonged patient length of stay, due to widespread disruption to clinical systems and care delivery.

Respondents were asked if their organization experienced the four cyberattacks what was the impact on patient care. According to Figure 9, 67 percent of respondents say ransomware attacks have resulted in longer lengths of stay. This is followed by 65 percent that say BEC/spoofing/impersonation attacks have caused delays in procedures and tests and have resulted in poor outcomes. Cloud/account compromises are most likely to result in an increase in mortality rate (36 percent) followed by supply chain attacks (32 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. For the first time, healthcare is spending less on remediation and technical support activities, as shown in Table 2.

Table 2 shows the five average costs of a healthcare cybersecurity compromise. According to the research, 93 percent of respondents say their organizations experienced at least one cyberattack in the past 12 months. The average number of attacks was 43. The average total cost for the **single most expensive cyberattack was $3,903,780**, a decrease from $4,740,400 in 2024, and reflects the lowest average cost of a healthcare cybersecurity compromise to date. This includes all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunities.

All average costs of a healthcare cybersecurity compromise decreased since 2024. Respondents estimate that the average highest cost ($1,210,172) was caused by disruption to normal healthcare operations because of system availability problems, a decrease from $1,469,524 in 2024. The cost due to users' idle time and lost productivity because of downtime or system performance delays decreased from an average of $995,484 in 2024 to $858,832 in 2025. The time required to ensure the impact on patient care is corrected decreased from $853,272 in 2024 to $702,680 in 2025.

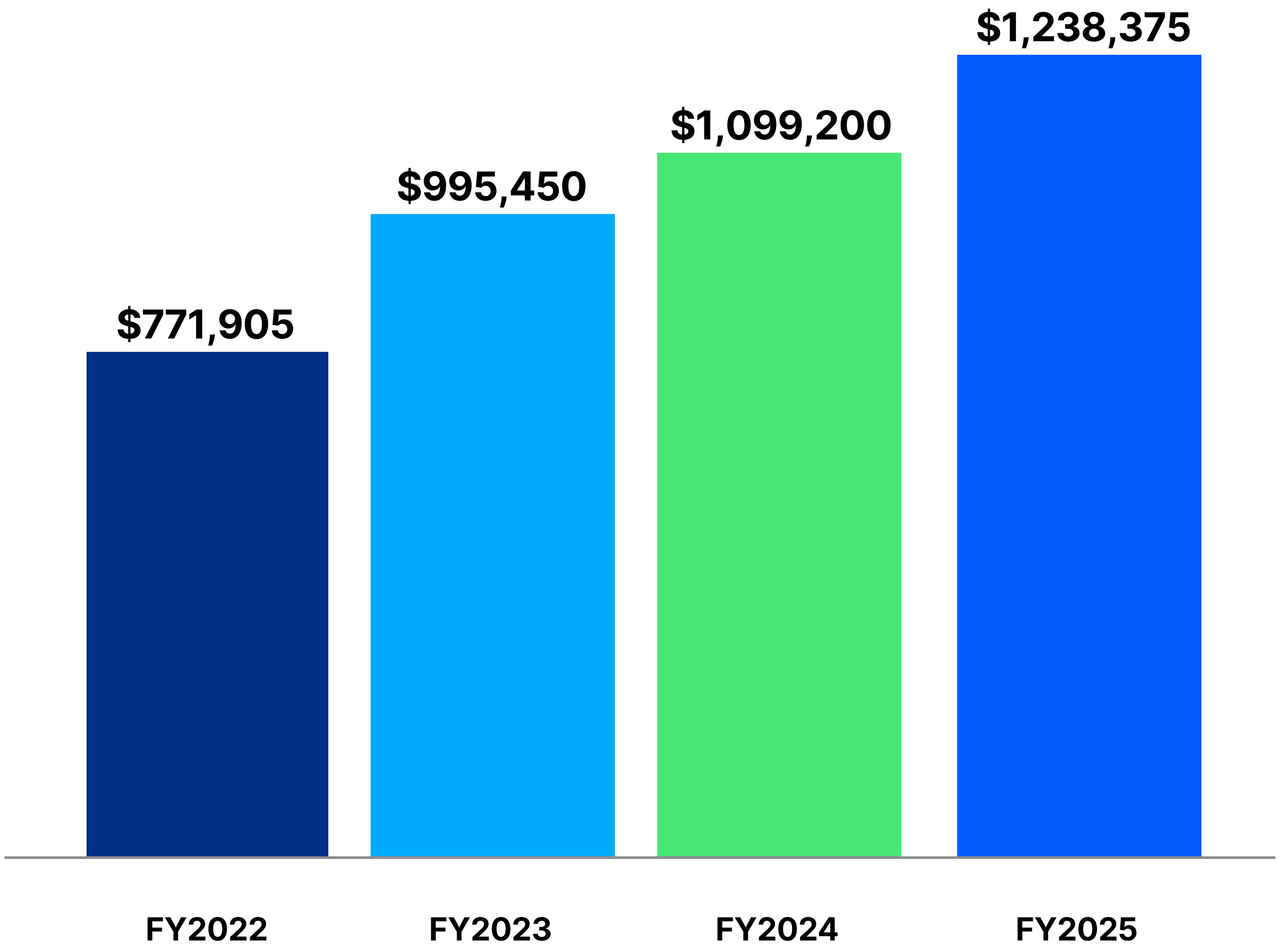
Remediation and technical support activities saw the largest drop in cost among all categories falling by $203,569, a 28.6% decrease from 2024, highlighting a significant reduction in post-attack response expenses.

Five average costs of a healthcare cybersecurity compromise	2025 Average cost	2024 Average cost	2023 Average cost	2022 Average cost
Disruption to normal healthcare operations because of system availability problems	$1,210,172	$1,469,524	$1,297,790	$1,018,670
Users' idle time and lost productivity because of downtime or system performance delays	$858,832	$995,484	$1,148,045	$1,107,250
Time required to ensure impact on patient care is corrected	$702,680	$853,272	$1,048,215	$664,350
Damage or theft of IT assets and infrastructure	$624,605	$711,060	$748,725	$930,090
Remediation & technical support activities, including forensic investigations, incident response activities, help desk and delivery of services to patients	$507,491	$711,060	$748,725	$708,640
Total	**$3,903,780**	**$4,740,400**	**$4,991,500**	**$4,429,000**

Figure 10

The average total cost for the highest ransomware payment is on the rise. Ransomware remains a persistent and serious threat to healthcare organizations.

The average total cost of ransomware continues to increase. Sixty-one percent of respondents say their organizations had a ransomware attack. Of these respondents, 33 percent say their organizations paid the ransomware, a slight decrease from 36 percent in 2024. Although fewer respondents say their organizations are paying the ransom, the average total cost increased, up 12.7% from $1,099,200 in 2024 to $1,238,375 in 2025, which is more than 60% higher than average ransom paid reported in the 2022 inaugural report, as shown in Figure 10.



The insider risk to sensitive data and patient safety

Figure 11

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

Organizations had an average of 18 data loss and exfiltration incidents in the past two years, a slight decrease from 20. Respondents were asked to identify the root causes of the data loss and exfiltration. Their responses are shown in Figure 11. Ninety-six 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 (35 percent). Twenty-five percent of respondents say it was due to employees sending PII or PHI to an unintended recipient via email and privilege access abuse.

More than one response permitted

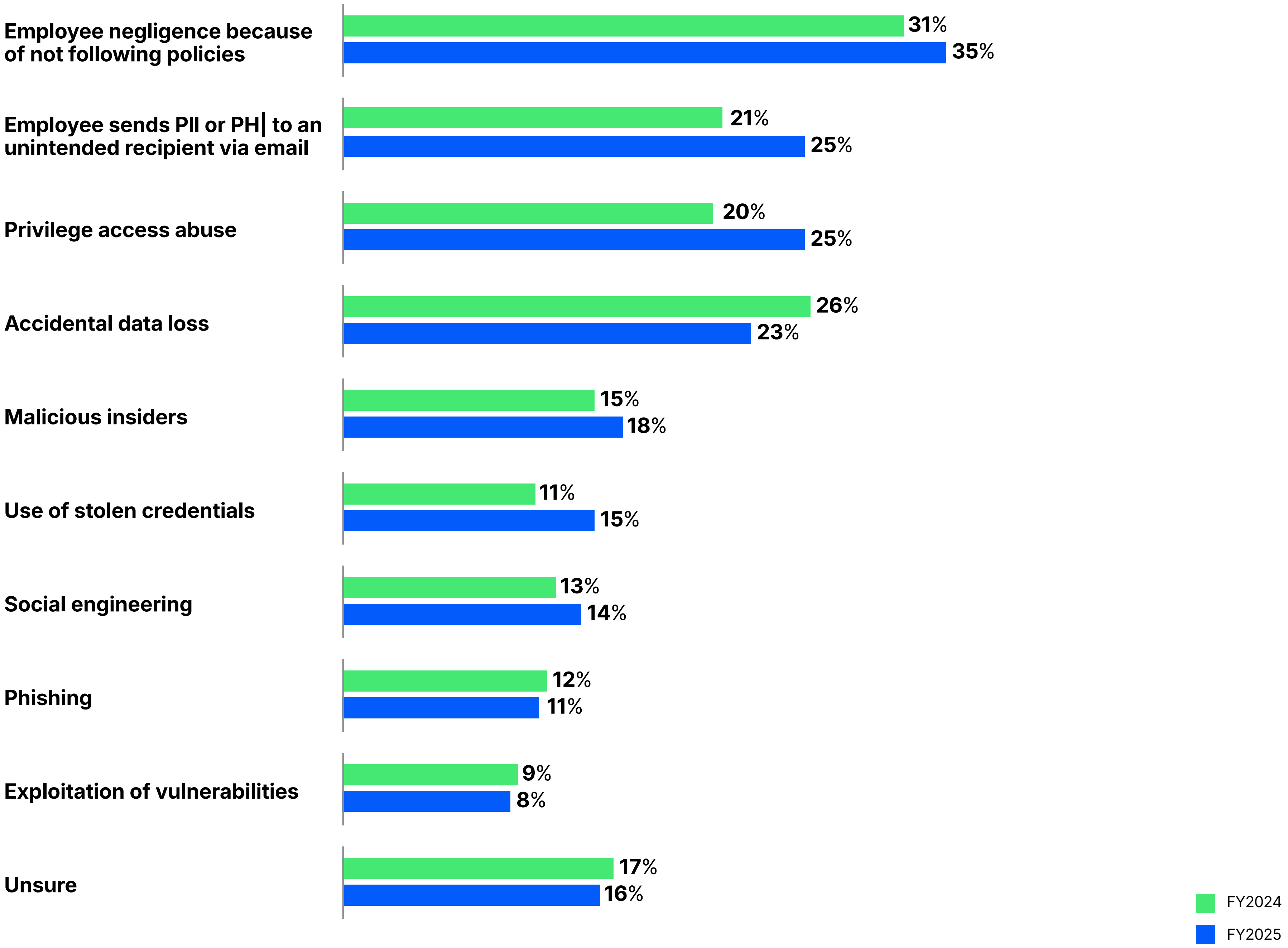


Figure 12

Data loss or exfiltration can increase patient mortality.

Respondents were asked what impact the data loss protection or infiltration incident had on patient care. Fifty-five 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 12, 54 percent say it increased the mortality rate and 36 percent say it caused delays in procedures and tests that resulted in poor outcomes.

More than one response permitted

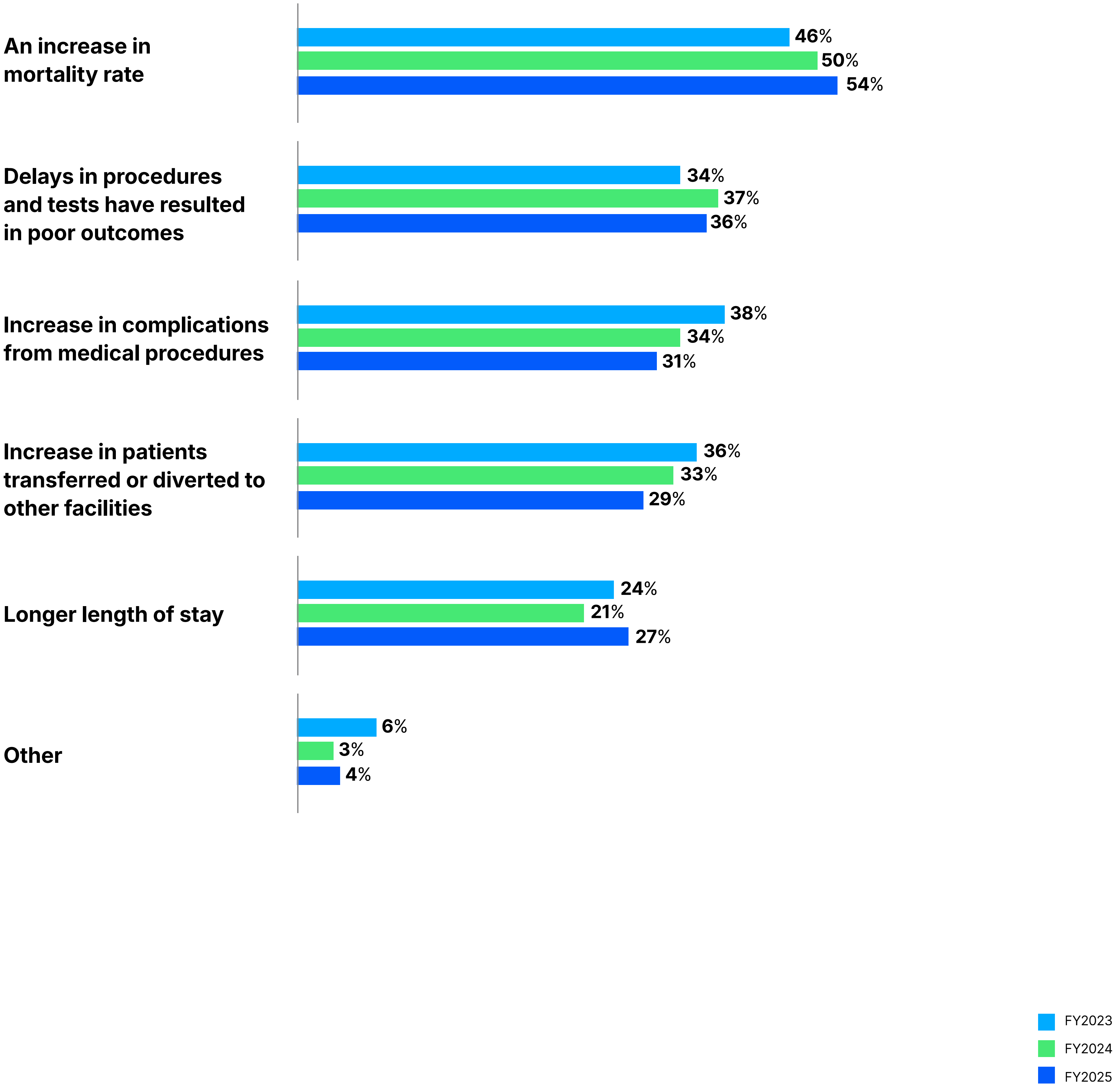


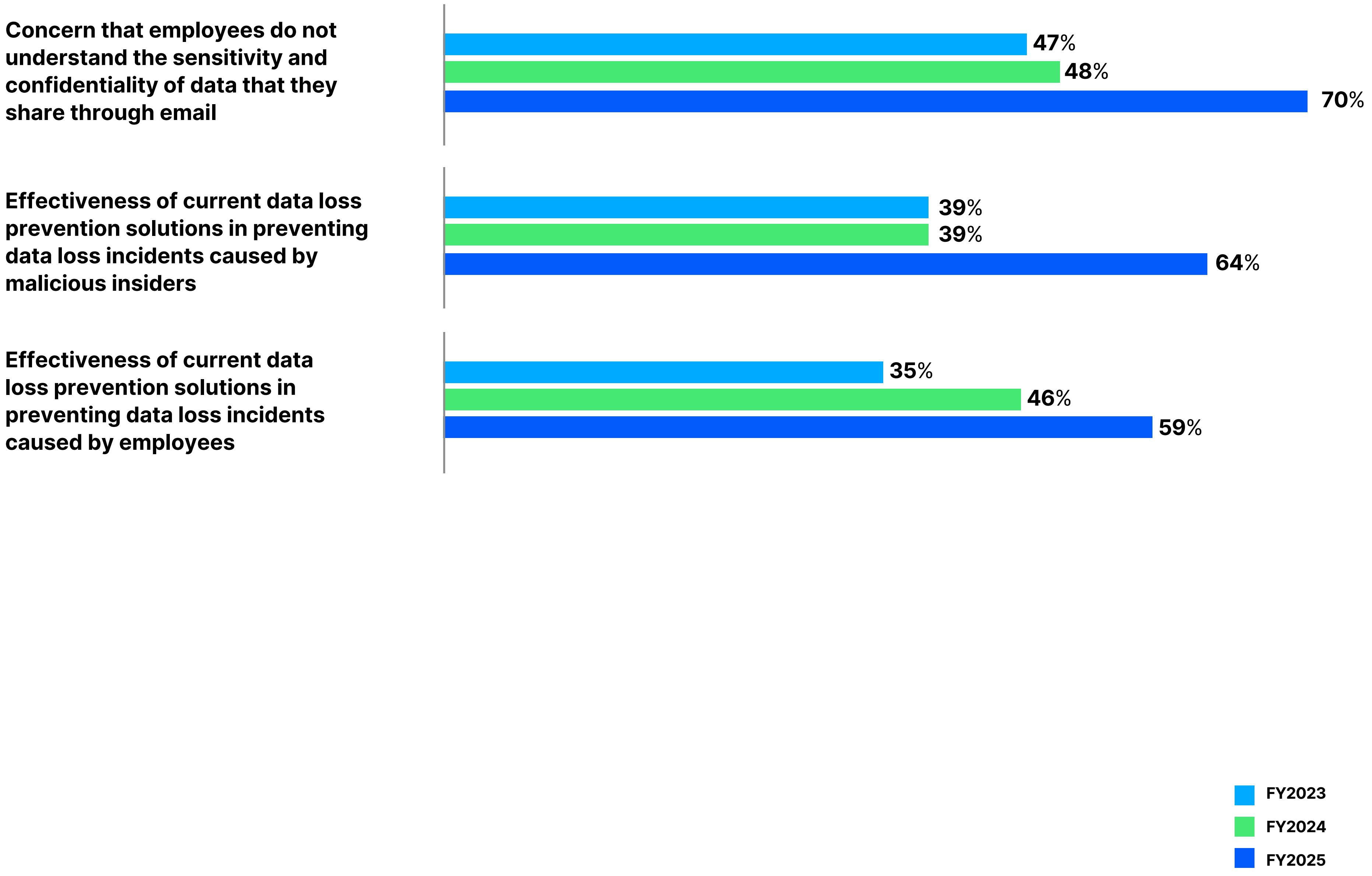
Figure 13

Solutions to prevent data loss incidents reduces insider risks but concerns that employees do not understand the sensitivity and confidentiality of data shared by email increased dramatically.

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 13 presents the very effective responses (7+ on the 10-point scale). As shown, organizations are more positive about the solutions to prevent data loss incidents caused by malicious insiders (an increase from 39 percent to 64 percent) and data loss prevention solutions to prevent data loss incidents caused by employees (an increase from 46 percent to 59 percent). However, concerns that employees do not understand the sensitivity and confidentiality of data shared through email increased significantly from 48 percent to 70 percent.

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



AI and machine learning in healthcare

Figure 14

AI is becoming a critical component of healthcare's cybersecurity strategies.

For the second 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 14, 57 percent of respondents say their organizations have embedded AI in cybersecurity (30 percent) or embedded in both cybersecurity and patient care (27 percent).

Only one choice permitted

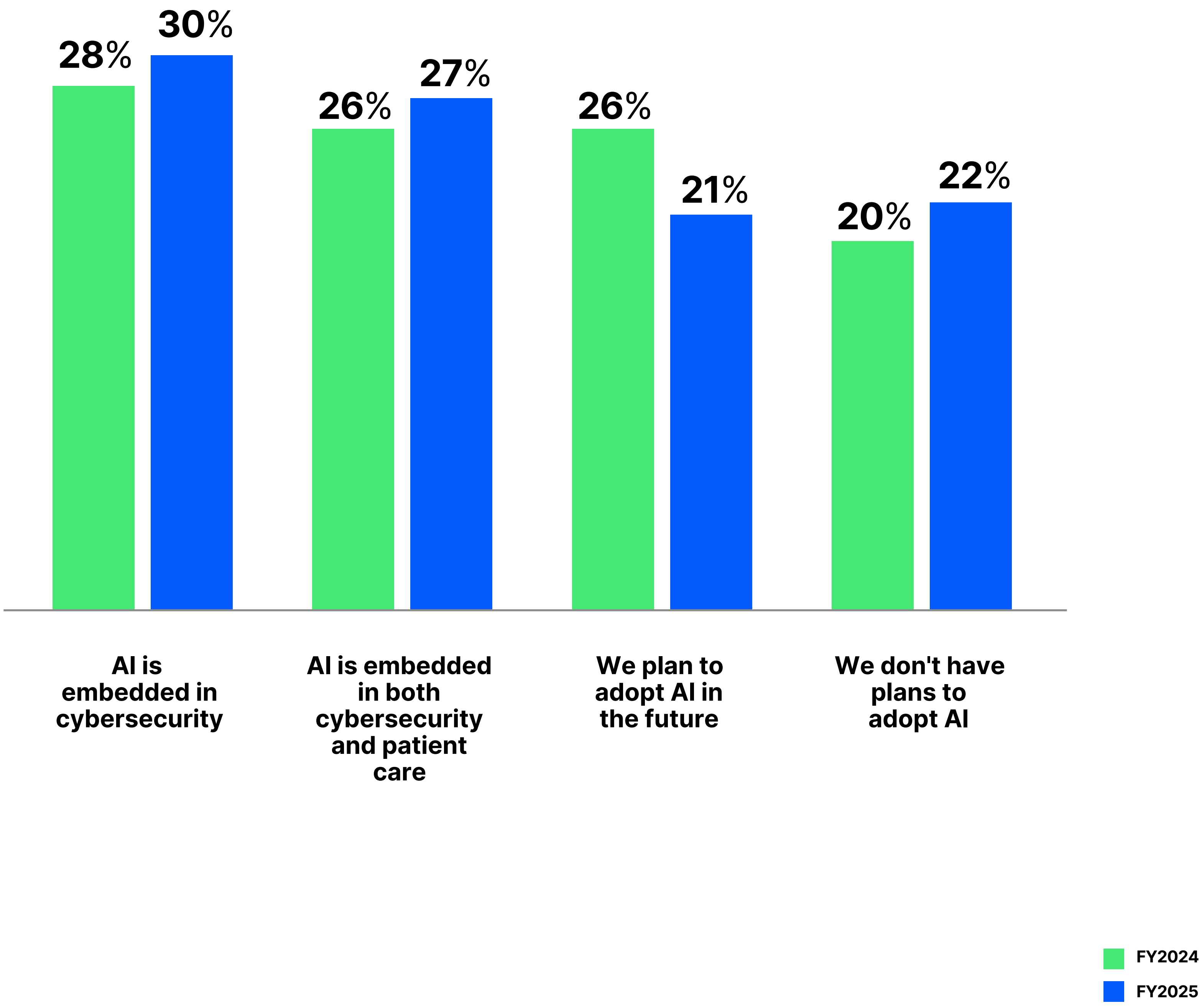


Figure 15

AI can improve patient care and the productivity of IT security personnel.

AI can increase efficiency and cost savings in patient care. As shown in Figure 15, 55 percent of respondents agree or strongly agree that AI-based security technologies will increase the productivity of their organizations' IT security personnel. Fifty-six percent 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, a significant increase from 48 percent in 2024.

Strongly agree and Agree responses combined

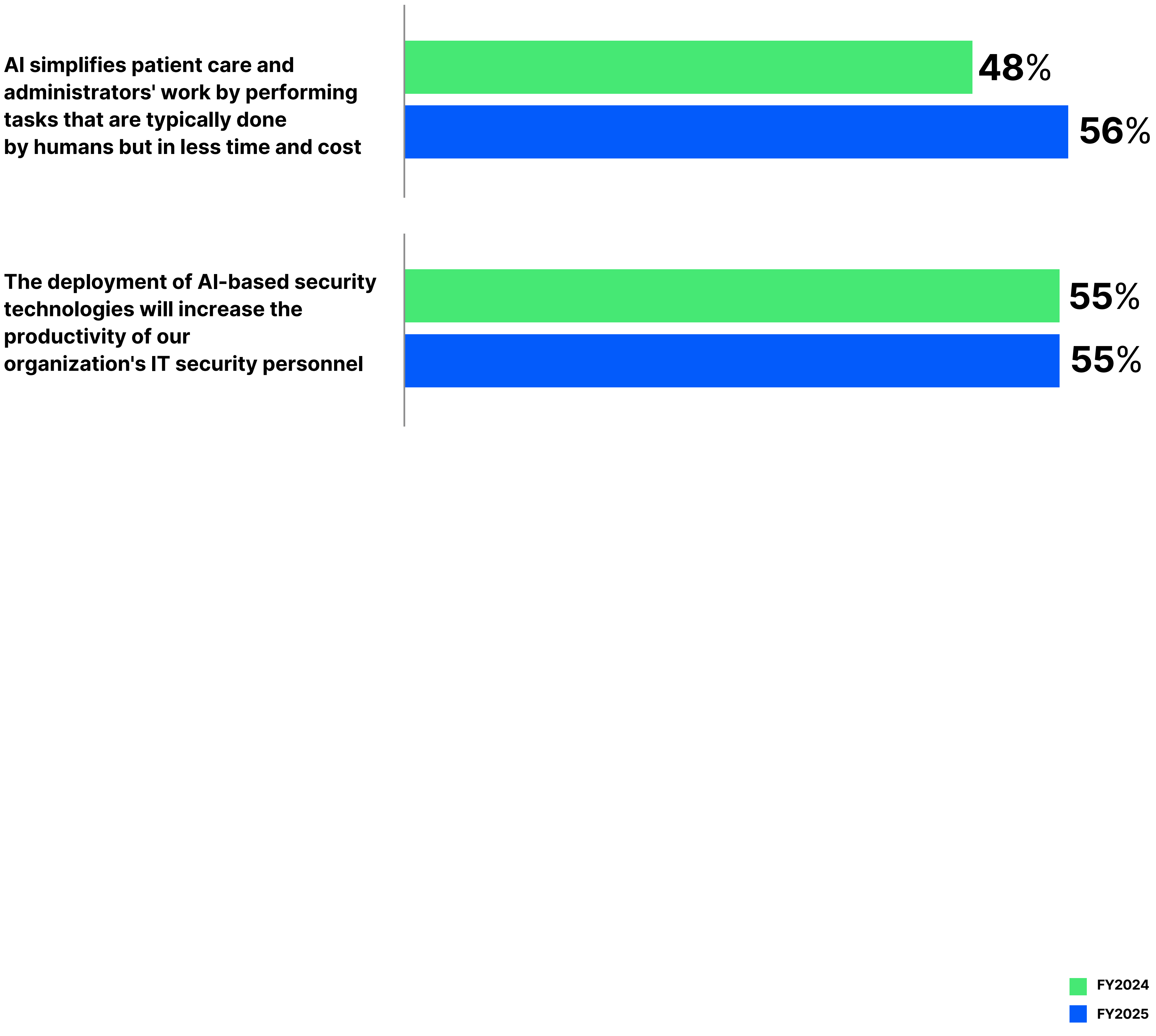


Figure 16

AI can reduce risks caused by employees' email practices and improve the cybersecurity posture.

Forty percent of respondents use AI and machine learning to understand human behavior. Of these respondents, 55 percent say understanding human behavior to protect against email attacks is very important.

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, 55 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). However, organizations are still struggling to safeguard confidential and sensitive patient data used in the organization's AI. Sixty percent say it is difficult or very difficult to protect this data.

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

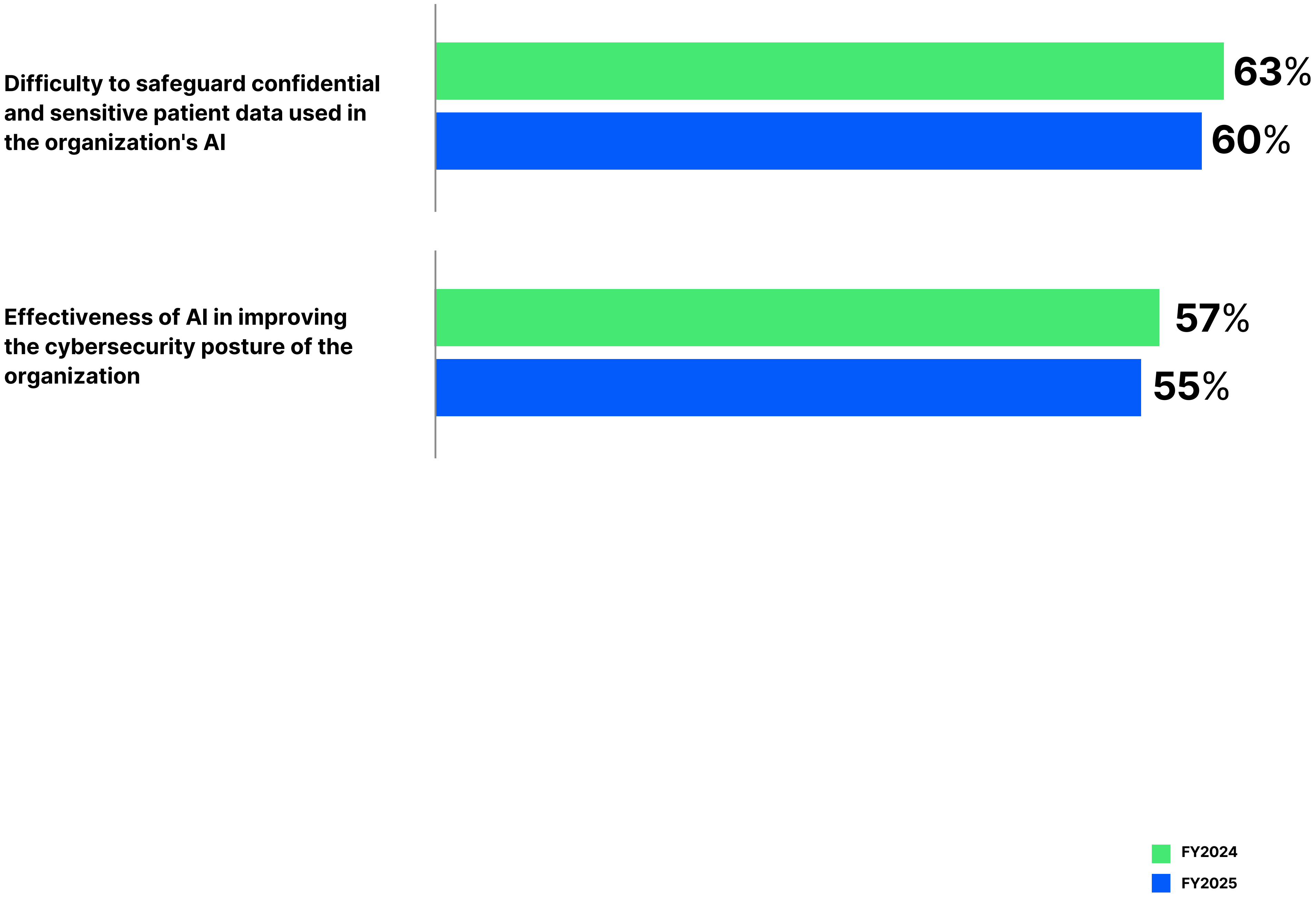


Figure 17

AI technologies are maturing and stabilizing.

Respondents were asked to identify the challenges to adopting AI-based security technologies. Figure 17 presents the issues that may delay adoption. The top challenges are interoperability issues among AI technologies (34 percent of respondents) and errors and inaccuracies in data inputs ingested by AI technology (33 percent). Only 28 percent say there is a lack of mature and/or stable AI technologies.

Two responses permitted

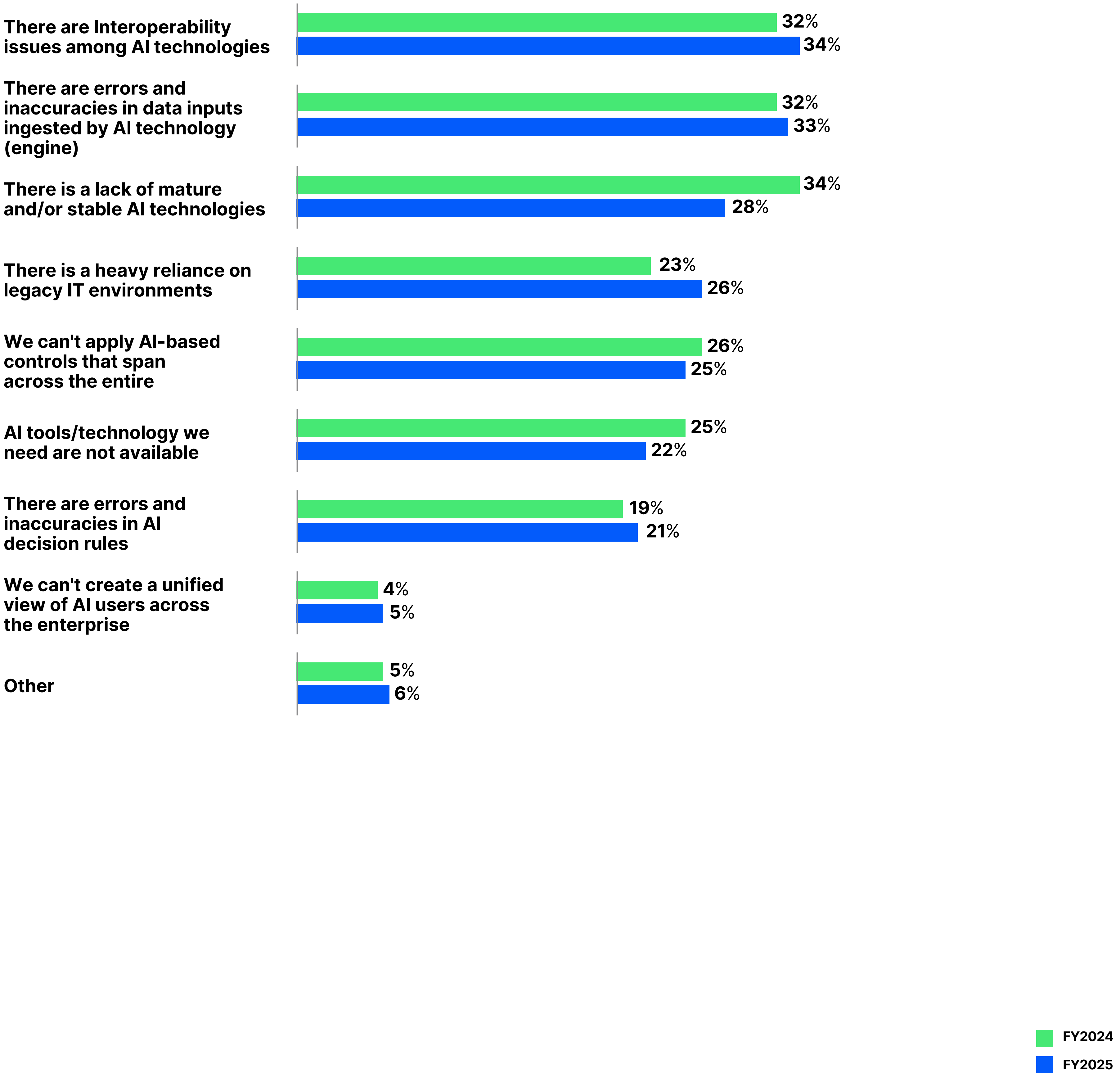


Figure 18

Data loss prevention (DLP) can make it less difficult to safeguard confidential and sensitive patient data.

AI systems, especially those dealing with large language models (LLMs), often process sensitive information. DLP solutions help manage this data by controlling its access and usage, and by preventing it from leaving the organization's control.

As shown in Figure 18, 87 percent of organizations plan to adopt AI-based DLP at some point. Currently, 23 percent of respondents say their organizations use AI-based DLP and 29 percent say they plan to adopt in six months, (14 percent) or within one year (15 percent).

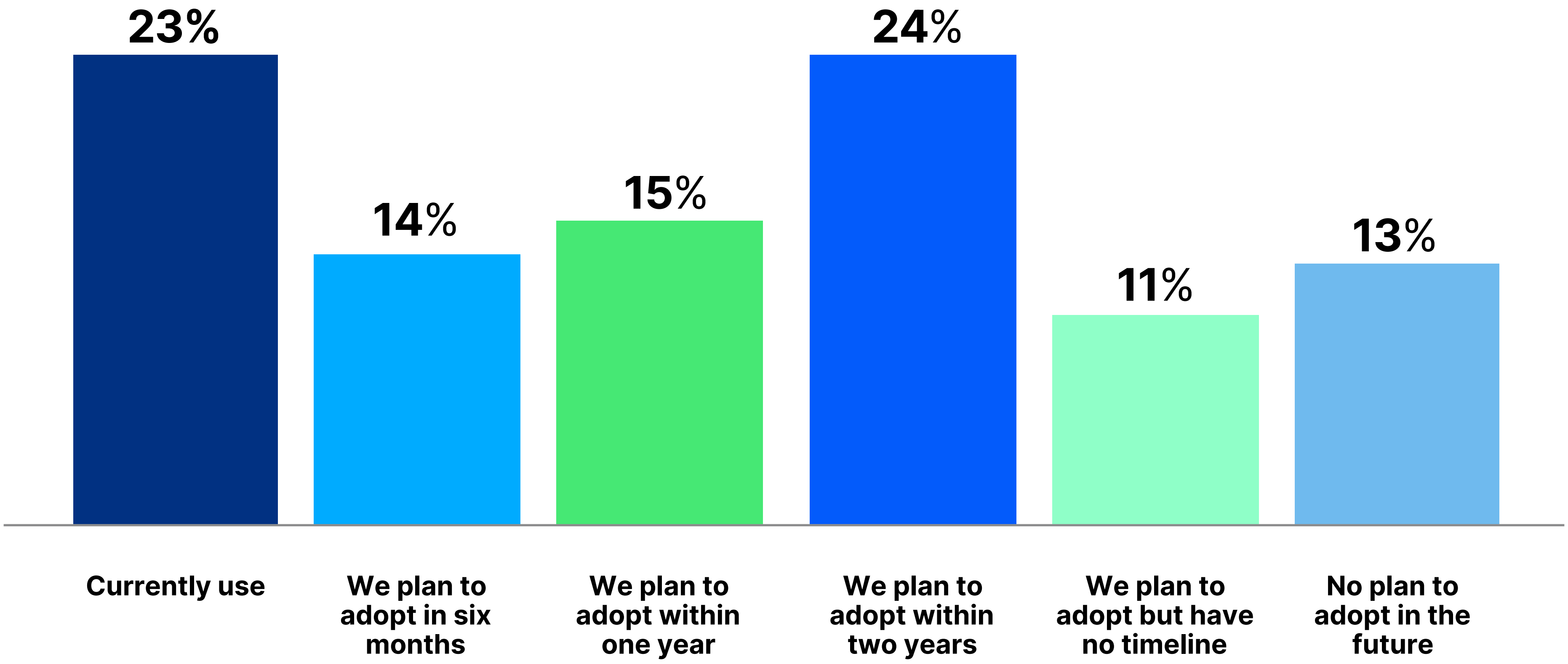
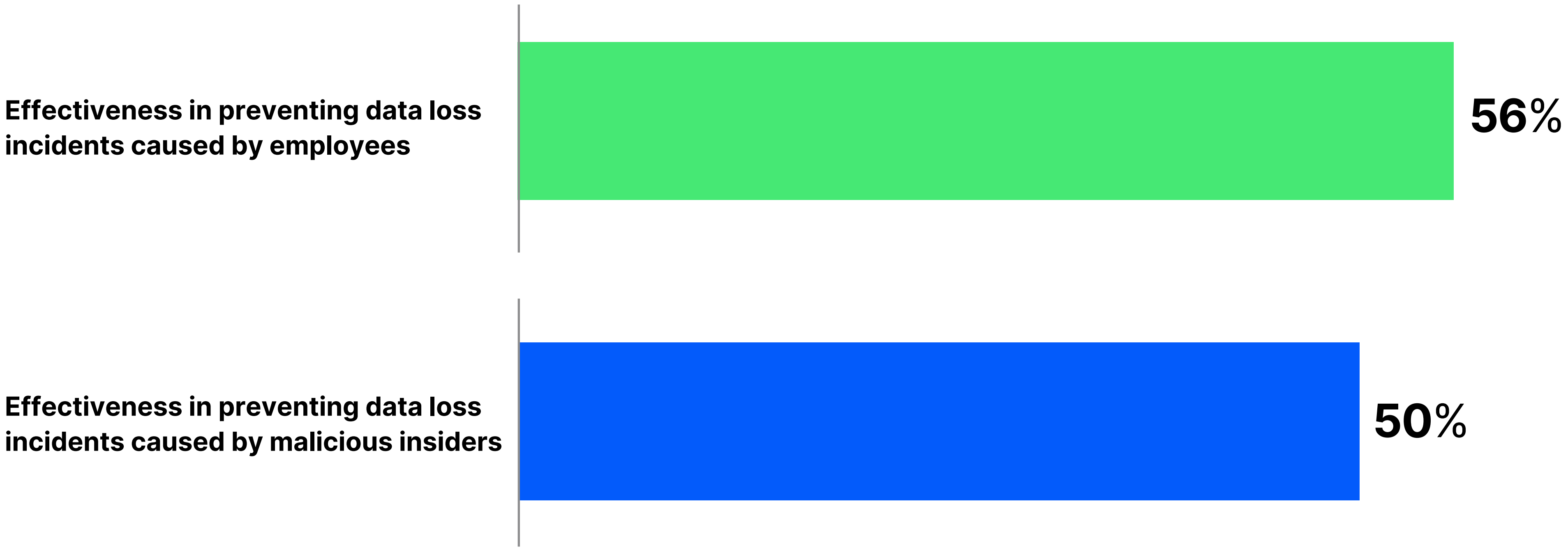


Figure 19

Healthcare organizations can use AI-based DLP to prevent data loss caused by employees and malicious insiders.

Respondents were asked to rate the effectiveness of AI-based DLP in preventing data loss incidents caused by employees and malicious insiders on a scale of 1 = not effective to 10 = highly effective. According to Figure 19, of the 87 percent of organizations that currently use or plan to use AI-based DLP, 56 percent say it is effective or very effective in preventing employee incidents and 50 percent say it is effective or very effective in preventing malicious insider incidents.

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



Solutions and responses to cyber insecurity

Figure 20

Organizations prioritize prevention and response to ransomware and cloud account compromises.

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 20, a significant number of organizations are concentrating on measures to prevent and respond to ransomware risks and cloud compromises (63 percent and 59 percent of respondents, respectively). In contrast, efforts to address supply chain attacks and malicious insiders are 38 percent and 36 percent of respondents, respectively.

More than one response permitted

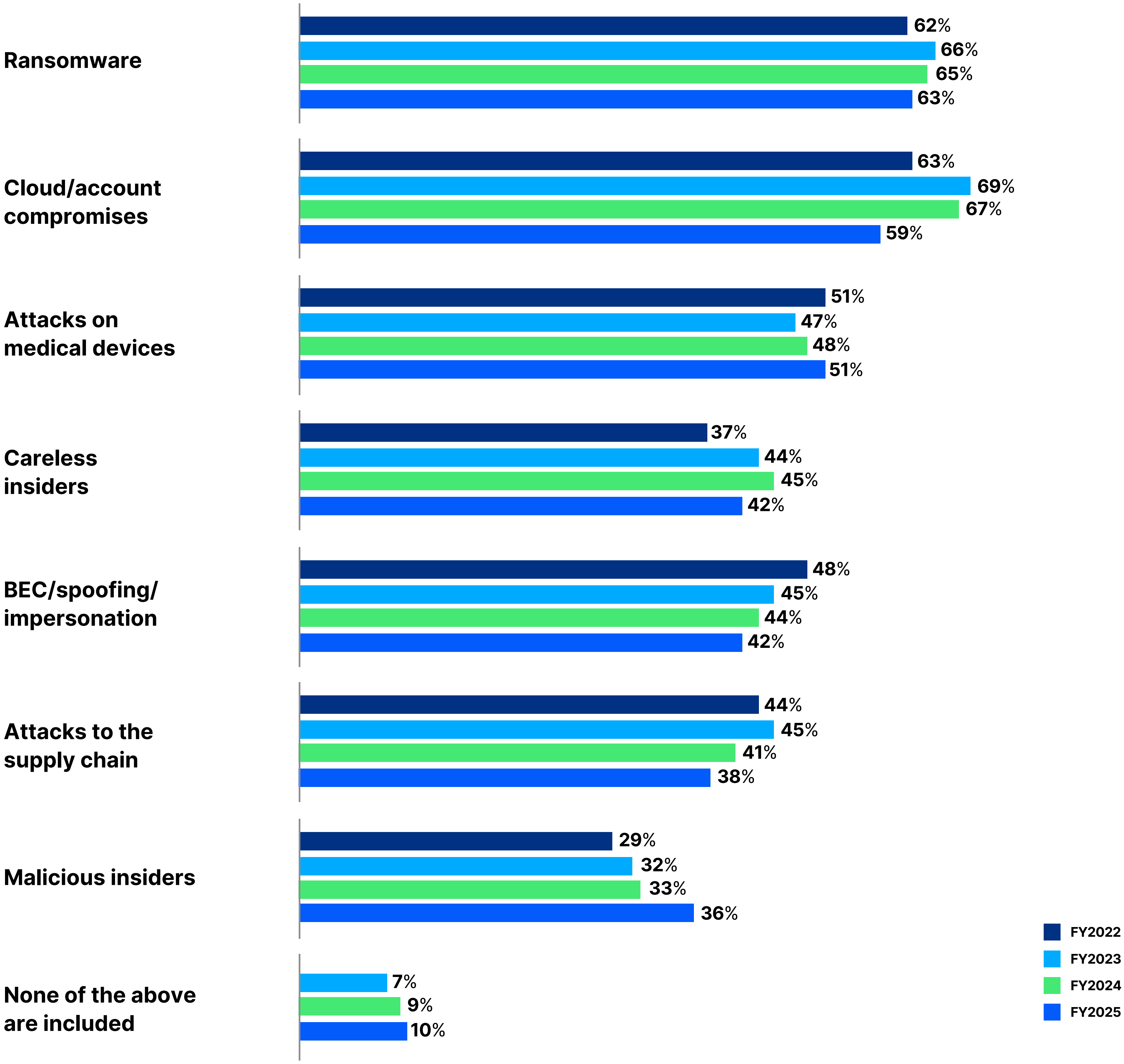


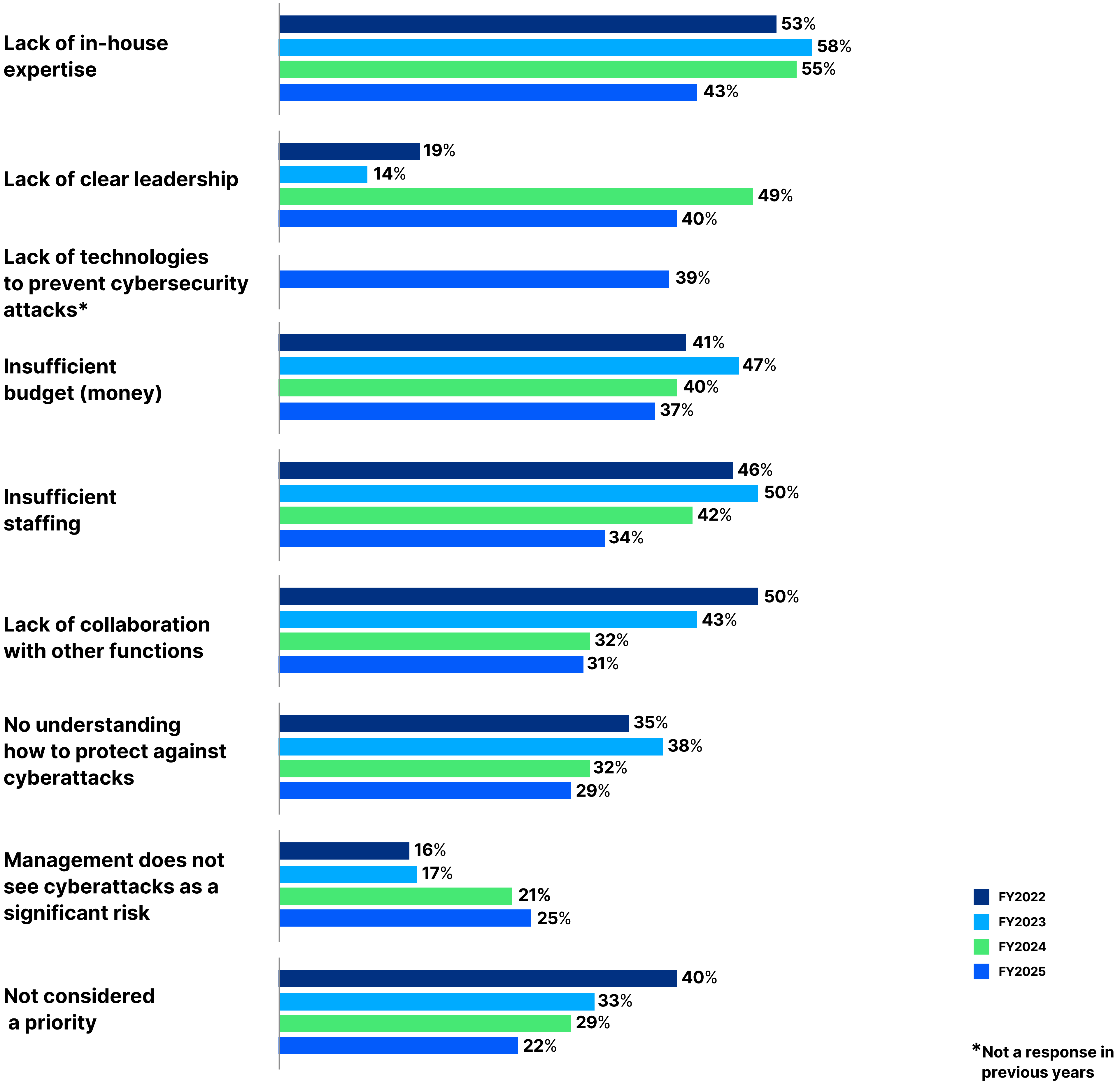
Figure 21

The lack of in-house expertise and clear leadership continues to be a problem and a threat to healthcare organizations' cybersecurity posture.

Respondents were asked what challenges keep their organization's cybersecurity posture from being fully effective. While 43 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 is a challenge according to 40 percent, as shown in Figure 21.

Not having enough budget decreased from 40 percent to 37 percent of respondents in 2025. The annual IT budget in 2025 is $65 million with 21 percent of that budget dedicated to information security.

More than one response permitted



*Not a response in previous years

Figure 22

Organizations continue to rely on security training and awareness programs to reduce risks caused by employees. But are they effective?

Respondents were asked what steps are taken to address the risk of employees' lack of awareness about cybersecurity threats. Seventy-six 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, 63 percent of respondents say their organizations conduct regular training and awareness programs. Fifty-one 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 response permitted

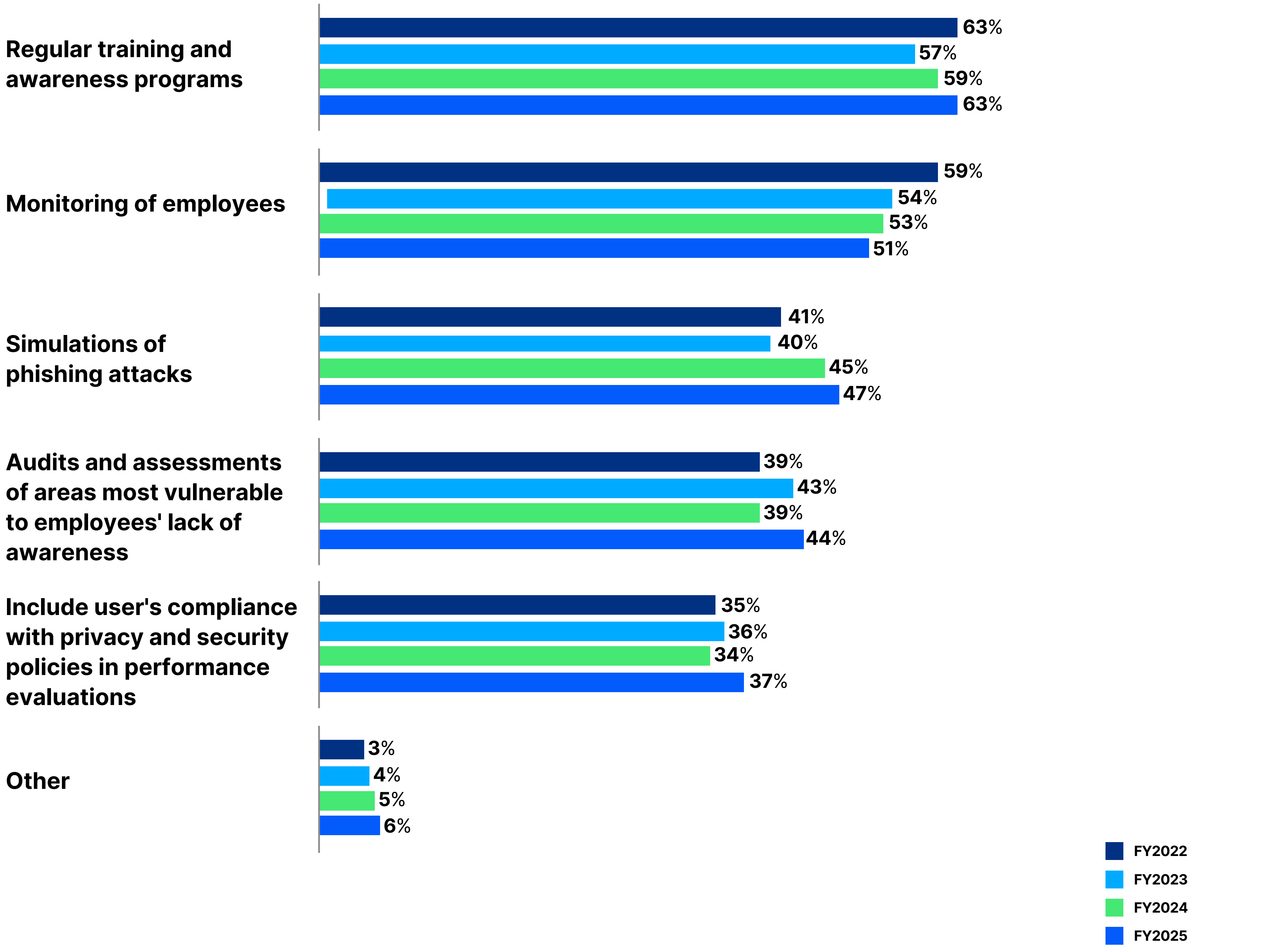


Figure 23

Just in the past year, the use of multi-factor authentication and secure email gateways to reduce phishing and other email-based attacks has increased significantly.

Respondents were asked what security methods and technologies their organizations use to reduce phishing and other email-based attacks. As shown in Figure 23, 54 percent of respondents say they use multi-factor authentication (an increase from 49 percent in 2024) and 52 percent say they use a secure email gateway (an increase from 45 percent). Technologies such as DMARC, AI/ML and threat intelligence did not rank in the top five.

More than one response permitted

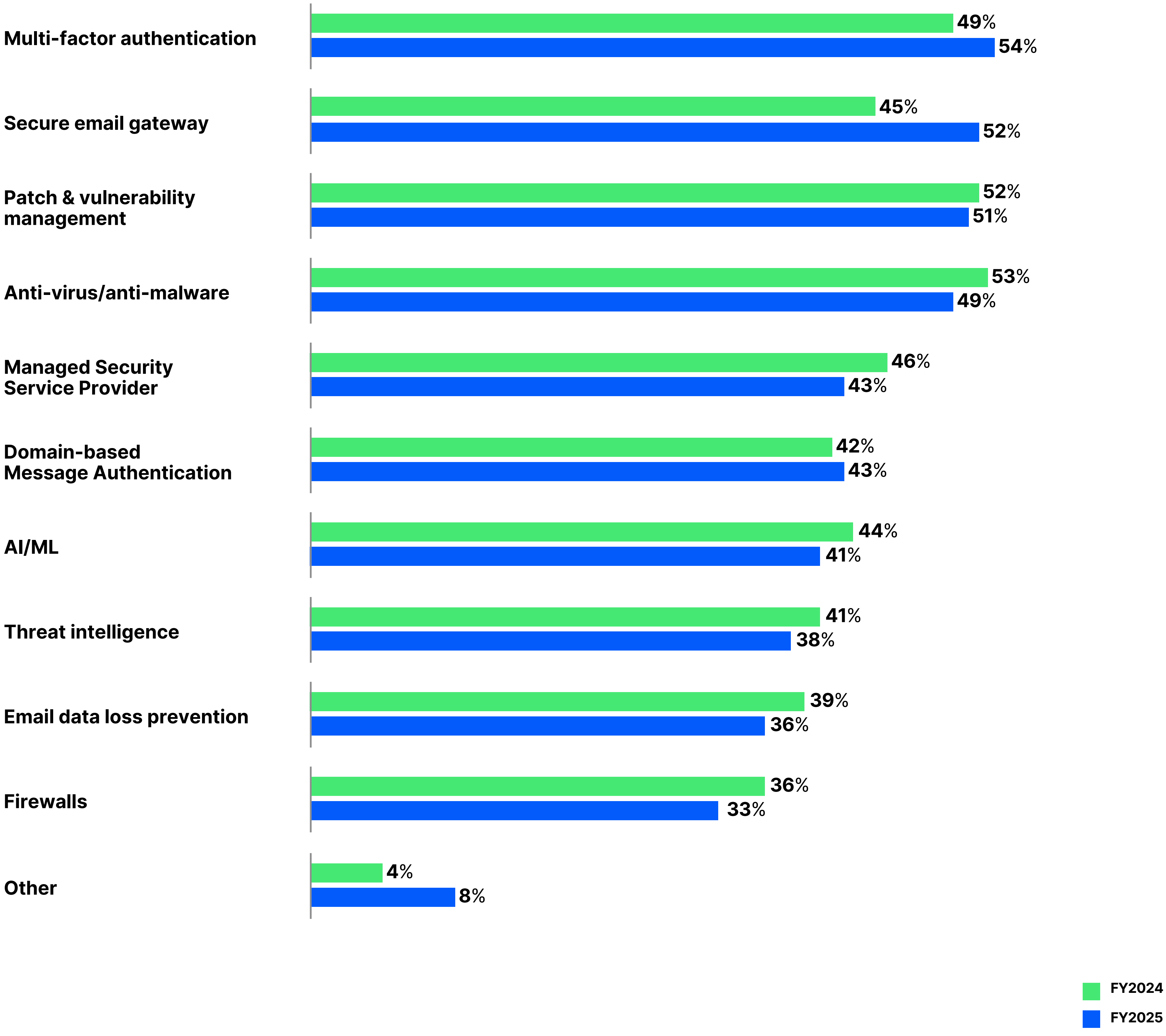


Figure 24

Endpoint and network 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. In this year's study, seven security methods and technologies were added to the list.

According to Figure 24, 45 percent of respondents say endpoint data loss prevention and 44 percent say network data loss prevention tools are used to prevent data loss or an exfiltration incident. Forty-three percent say encryption for data in transit and insider threat management tools are used.

More than one response permitted

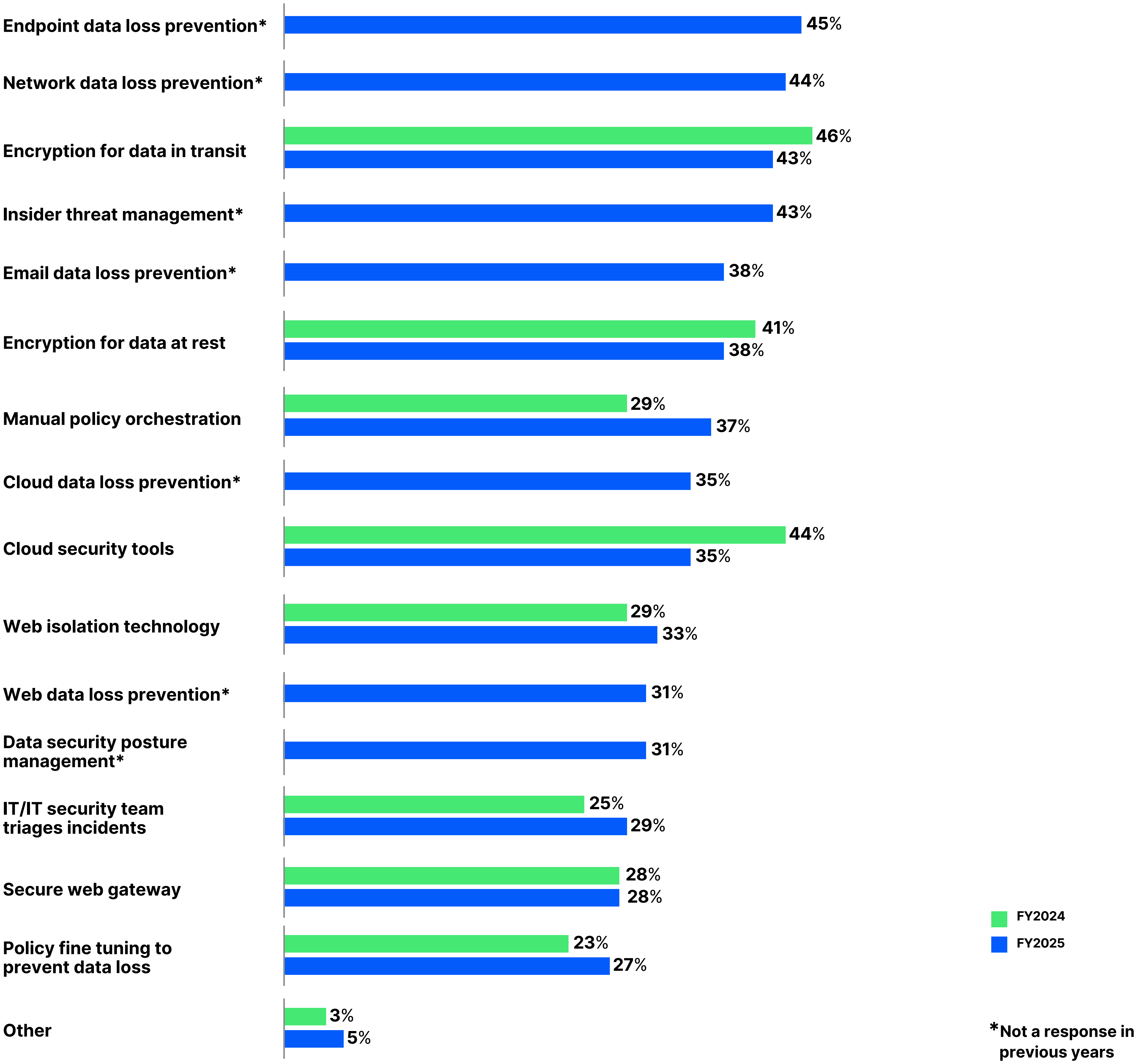


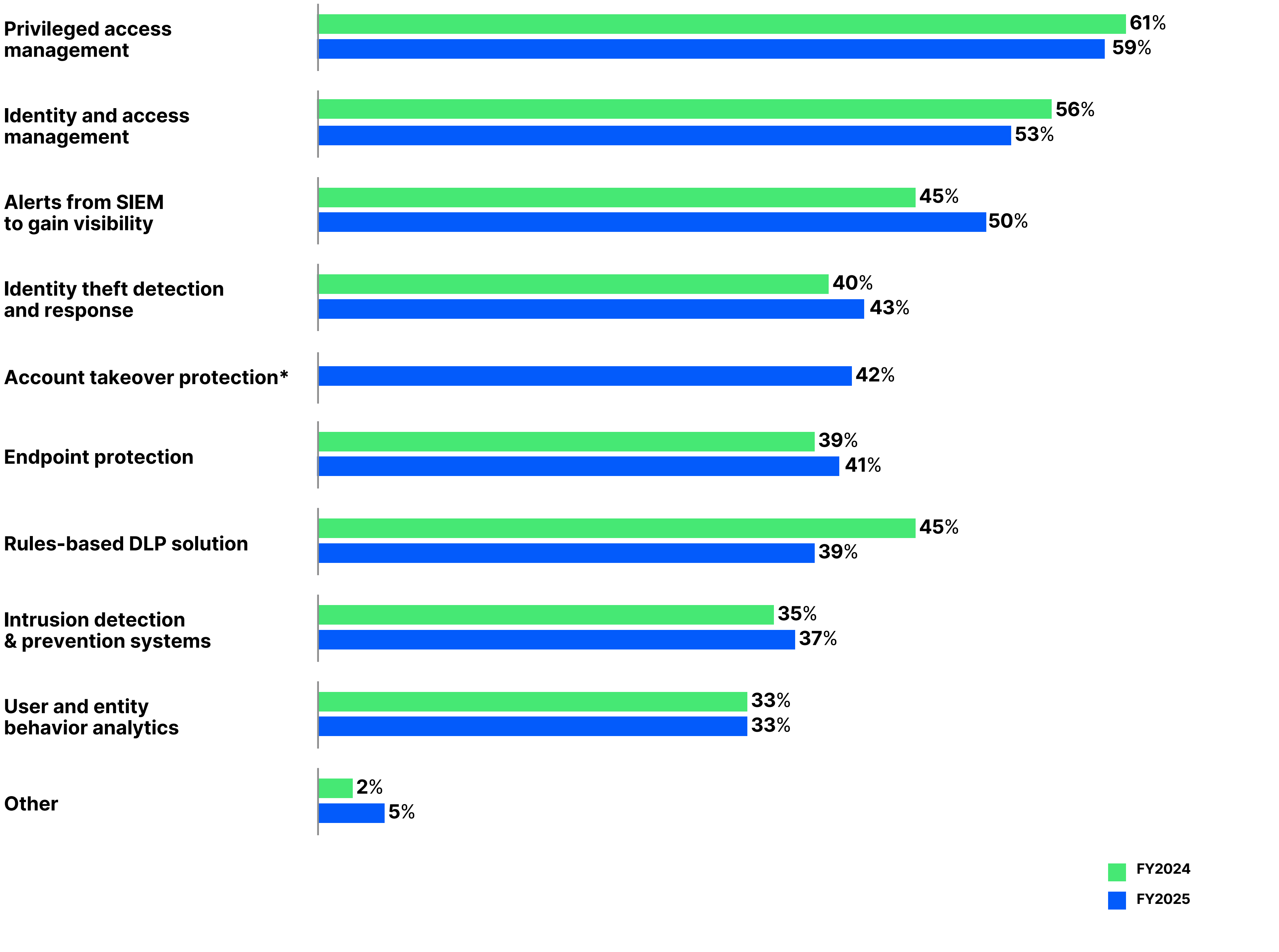
Figure 25

Privileged access management and identity and access management continue to be the technologies most often used to reduce identity risk and lateral movement in their networks.

Lateral movement in cybersecurity refers to the ability of attackers to move within a network after gaining initial access, often to spread to other systems and data. It's a key tactic in cyberattacks, allowing threat actors to extend their control and reach valuable assets after an initial breach.

Respondents were asked what other technologies are implemented to prevent identity risk and lateral movement in their networks. Figure 25 presents the technologies healthcare organizations are implementing to prevent identity risk and lateral movement in their networks. Most frequently implemented are privileged access management (59 percent of respondents), identity and access management (53 percent) and alerts from SIEM to gain visibility (50 percent).

More than one response permitted



*Not a response in previous years

Part 3. Methodology

Our final sample consisted of 677 surveys or a 3.9 percent response rate.

A sampling frame of 17,220 IT and IT security practitioners in U.S. 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 756 total returns. Screening and reliability checks required the removal of 79 surveys. Our final sample consisted of 677 surveys or a 3.9 percent response rate.

Table 3

Sample response	Freq	Pct%
Sampling frame	17,220	100%
Total returns	756	4.4%
Rejected or screened surveys	79	0.5%
Final sample	**677**	**3.9%**

Figure 26

Type of organization

Figure 26 reports the respondent's type of organizations. Twenty-one percent of respondents are from organizations that are private healthcare providers. This is followed by healthcare insurer (20 percent), public healthcare provider (18 percent), healthcare insurance (11 percent) and payer (10 percent).

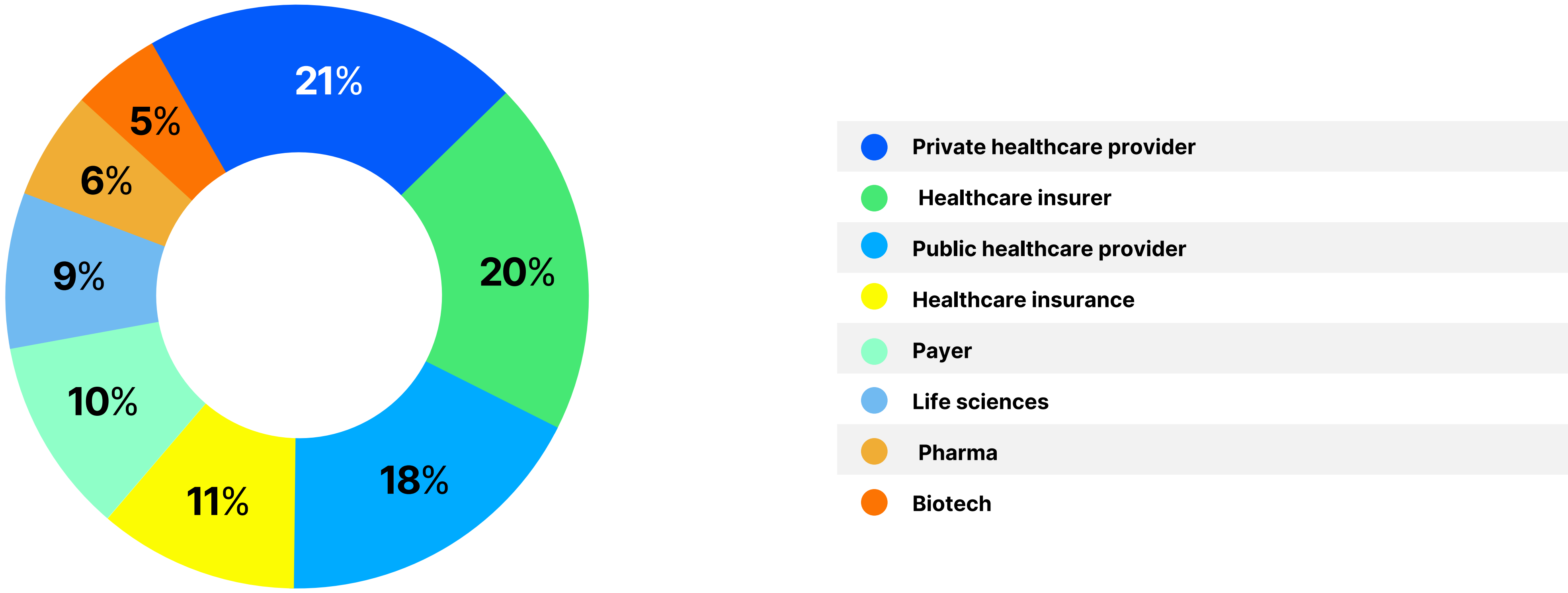


Figure 27

Current position within the organization

Figure 27 reports the respondent's organizational level within participating organizations. By design, more than half (64 percent) are at or above the supervisory levels. The largest category is technician/staff (27 percent).

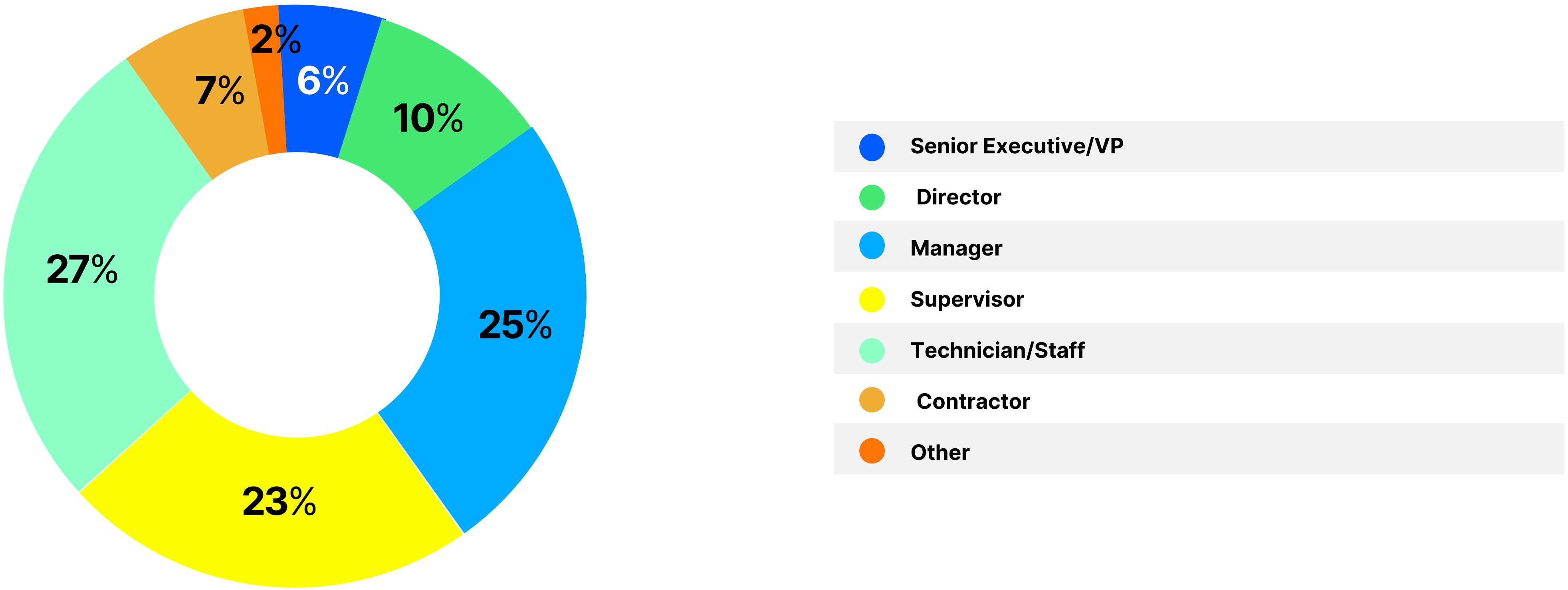


Figure 28

Direct reporting channel

As shown in Figure 28, 22 percent of respondents report to the chief information security officer, 16 percent report to the chief information officer, 12 percent report to cloud administration, 10 percent report to the compliance officer and 9 percent report to the chief risk officer.

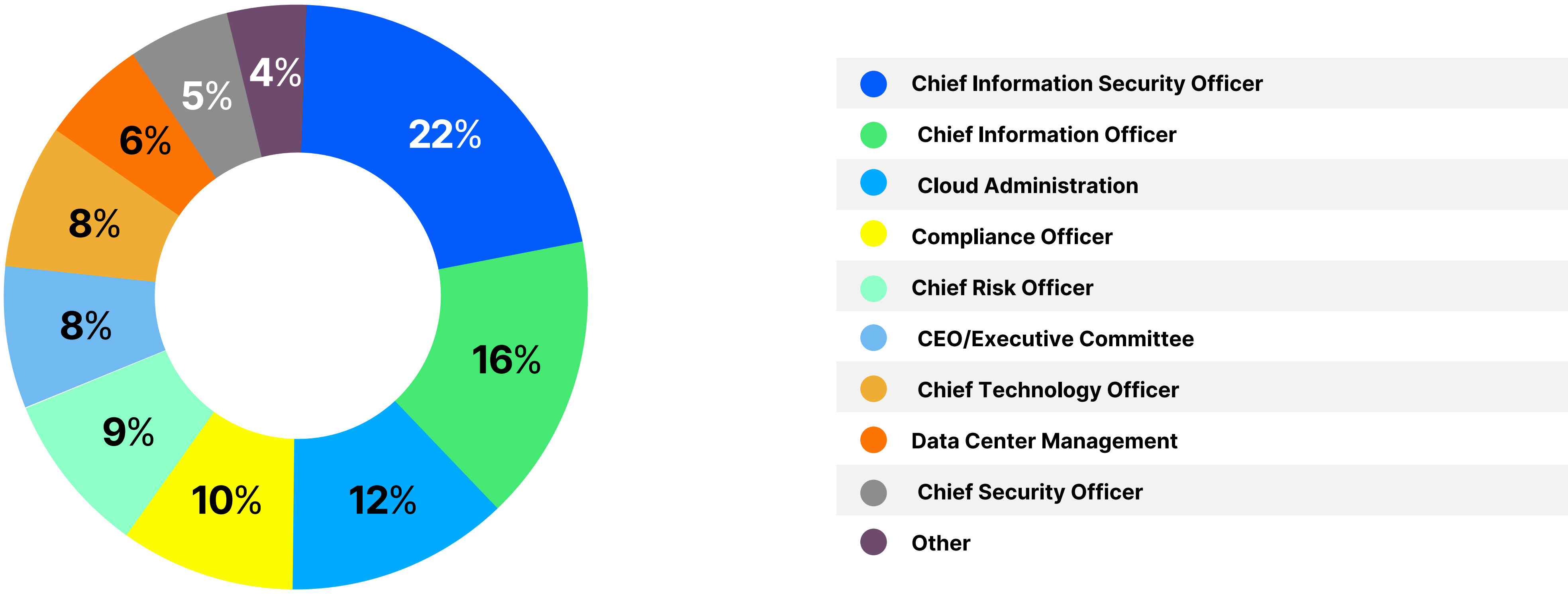
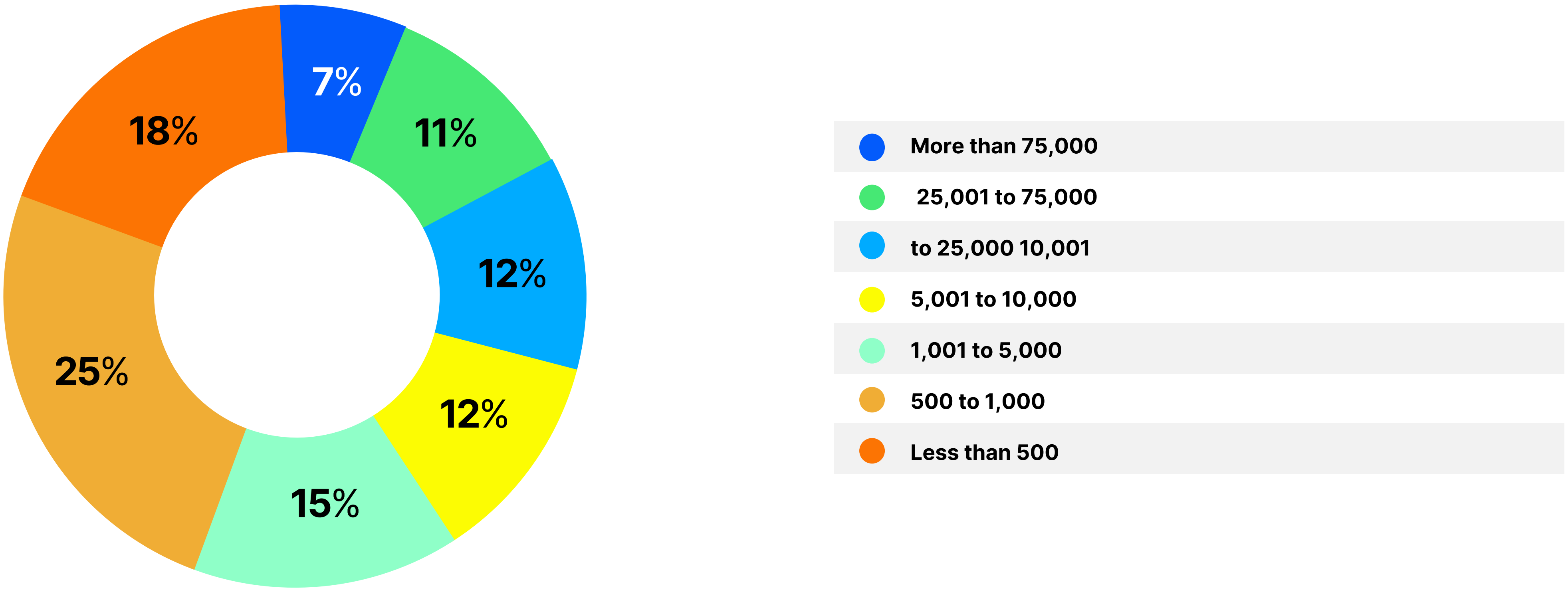


Figure 29

Full-time headcount

As shown in Figure 29, 57 percent of respondents are from organizations with a 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 April 2025.

Survey response	FY2025	FY2024	FY2023	FY2022
Total sampling frame	17220	18015	17085	16,451
Total returns	756	732	715	698
Evaluating and measuring effectiveness of cybersecurity strategies	79	84	62	57
Total sample	677	648	653	641
Response rate	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.	FY2025	FY2024	FY2023	FY2022
Setting IT cybersecurity priorities	55%	49%	51%	46%
Managing IT security budgets	41%	43%	45%	42%
Selecting vendors and contractors	50%	47%	49%	47%
Participating in IT cybersecurity strategies	53%	52%	51%	51%
Evaluating and measuring effectiveness of cybersecurity strategies	46%	36%	36%	34%
Managing cybersecurity risk	37%	40%	34%	36%
Overseeing governance and compliance	26%	28%	27%	29%
None of the above [Stop]	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).	FY2025	FY2024	FY2023	FY2022
BEC/spoofing/impersonation	40%	46%	62%	46%
Cloud/account compromises	49%	55%	63%	57%
Employee negligence or error	47%	52%	52%	58%
Employee-owned mobile devices or BYOD	49%	53%	61%	34%
Generative AI or AI tools	38%			
Insecure medical devices	47%	54%	53%	64%
Insecure mobile apps (eHealth)	55%	59%	51%	59%
Malicious insiders	37%	42%	45%	37%
Malware	23%			
Nation state attacks	26%	21%	19%	17%
Process failures	23%	31%	31%	36%
Ransomware	42%	45%	48%	60%
Supply chain risks	42%	46%	40%	43%
System failures	34%	44%	35%	36%
Third-party misuse of patient data	29%	31%	26%	33%
Use of public cloud services	15%	17%	11%	18%
Other (please specify)	4%	4%	3%	2%
Total	600%	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.	FY2025	FY2024	FY2023	FY2022
Attacks on medical devices	51%	48%	47%	51%
Attacks to the supply chain	38%	41%	45%	44%
BEC/spoofing/impersonation	42%	44%	45%	48%
Cloud/account compromises	59%	67%	69%	63%
Malicious insiders	36%	33%	32%	29%
Careless insiders	42%	45%	44%	37%
Ransomware	63%	65%	66%	62%
None of the above are included	10%	9%	7%	
Total	352%	352%	355%	334%

Q3. What challenges keep your organization's cybersecurity posture from being fully effective? Please select the top three (3) challenges	FY2025	FY2024	FY2023	FY2022
Insufficient budget (money)	37%	40%	47%	41%
Insufficient staffing	34%	42%	50%	46%
Lack of in-house expertise	43%	55%	58%	53%
Lack of technologies to prevent cybersecurity attacks	39%			
Lack of clear leadership	40%	49%	14%	19%
Management does not see cyberattacks as a significant risk	25%	21%	17%	16%
Lack of collaboration with other functions	31%	32%	43%	50%
No understanding how to protect against cyberattacks	29%	32%	38%	35%
Not considered a priority	22%	29%	33%	40%
Total	300%	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.	FY2025	FY2024	FY2023	FY2022
1 or 2	12%	13%	8%	11%
3 or 4	18%	16%	16%	13%
5 or 6	17%	19%	15%	12%
7 or 8	20%	21%	25%	24%
9 or 10	33%	31%	36%	40%
Total	100%	100%	100%	100%
Extrapolated value	6.38	6.32	6.80	6.88

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.	FY2025	FY2024	FY2023	FY2022
1 or 2	5%	2%	2%	5%
3 or 4	15%	18%	11%	8%
5 or 6	23%	20%	24%	16%
7 or 8	22%	24%	23%	23%
9 or 10	35%	36%	40%	48%
Total	100%	100%	100%	100%
Extrapolated value	6.94	6.98	7.26	7.52

Q6. Using the following 10-point scale, please rate your organization’s vulnerability to ransomware attacks from 1 = not vulnerable to 10 = highly vulnerable.	FY2025	FY2024	FY2023	FY2022
1 or 2	12%	14%	5%	6%
3 or 4	17%	15%	10%	9%
5 or 6	16%	17%	21%	13%
7 or 8	30%	30%	26%	25%
9 or 10	25%	24%	38%	47%
Total	100%	100%	100%	100%
Extrapolated value	6.28	6.20	7.14	7.46

Q7. Using the following 10-point scale, please rate your organization’s vulnerability to cloud/account compromises from 1 = not vulnerable to 10 = highly vulnerable.	FY2025	FY2024	FY2023	FY2022
1 or 2	7%	8%	5%	0%
3 or 4	8%	9%	6%	9%
5 or 6	21%	20%	15%	16%
7 or 8	37%	34%	40%	30%
9 or 10	27%	29%	34%	45%
Total	100%	100%	100%	100%
Extrapolated value	6.88	6.84	7.34	7.72

Q8. Did your organization ever experience a successful ransomware attack?	FY2025	FY2024	FY2023	FY2022
Yes	61%	59%	54%	41%
No (please skip to Q12a)	35%	33%	44%	52%
Unsure (please skip to Q12a)	4%	8%	2%	7%
Total	100%	100%	100%	100%

Q9. How many successful ransomware attacks did your organization experience over the past two years?	FY2025	FY2024	FY2023	FY2022
One	32%	37%	43%	53%
Two to five	35%	36%	34%	33%
Six to 10	24%	21%	16%	9%
More than 10	9%	6%	7%	5%
Total	100%	100%	100%	100%
Extrapolated value	5.0	4.0	3.7	3.0

Q10a. Did your organization pay the ransom?	FY2025	FY2024	FY2023	FY2022
Yes	33%	36%	40%	51%
No	67%	64%	60%	49%
Total	100%	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.	FY2025	FY2024	FY2023	FY2022
Less than $10,000	0%	0%	0%	2%
$10,000 to $25,000	6%	9%	13%	9%
$25,001 to $50,000	11%	10%	9%	7%
$50,001 to $75,000	13%	12%	14%	10%
$75,001 to $100,000	9%	19%	18%	17%
$100,001 to $250,000	14%	12%	11%	19%
$250,001 to $500,000	11%	13%	12%	18%
$500,001 to $1,000,000	9%	8%	9%	8%
$1,000,000 to $5,000,000	8%	9%	7%	5%
$5,000,000 to $10,000,000	4%	6%	4%	3%
More than $10,000,000	5%	2%	3%	2%
Total	100%	100%	100%	100%
Extrapolated value	$1,238,375	$1,099,200	$ 995,450	$771,905

Q11a. Did the ransomware attack result in a disruption in patient care?	FY2025	FY2024	FY2023	FY2022
Yes	67%	70%	68%	67%
No	28%	25%	26%	30%
Unsure	5%	5%	6%	3%
Total	100%	100%	100%	100%

Q11b. If yes, what impact did the ransomware attack have on patient care? Please select all that apply.	FY2025	FY2024	FY2023	FY2022
An increase in mortality rate	27%	29%	28%	24%
Delays in procedures and tests have resulted in poor outcomes	56%	61%	59%	64%
Increase in complications from medical procedures	50%	47%	44%	48%
Increase in patients transferred or diverted to other facilities	50%	52%	46%	50%
Longer length of stay	67%	58%	48%	59%
Other (please specify)	8%	5%	3%	3%
Total	258%	252%	228%	248%

Q12a. Did your organization ever experience a BEC/spoofing / impersonation attack?	FY2025	FY2024	FY2023	FY2022
Yes	62%	57%	54%	51%
No (please skip to Q14a)	32%	38%	41%	40%
Unsure (please skip to Q14a)	6%	5%	5%	9%
Total	100%	100%	100%	100%

Q12b. If yes, how many BEC/spoofing/impersonation attacks did your organization experience over the past two years?	FY2025	FY2024	FY2023	FY2022
One	53%	53%	40%	49%
Two to five	19%	21%	24%	31%
Six to 10	16%	15%	19%	12%
More than 10	12%	11%	17%	8%
Total	100%	100%	100%	100%
Extrapolated value	3.9	3.8	4.8	3.5

Q13a. Did the BEC/spoofing/impersonation attack result in a disruption in patient care operations?	FY2025	FY2024	FY2023	FY2022
Yes	70%	65%	69%	67%
No	26%	31%	26%	30%
Unsure	4%	4%	5%	3%
Total	100%	100%	100%	100%

Q13b. If yes, what impact did the BEC/spoofing/impersonation attack have on patient care? Please select all that apply.	FY2025	FY2024	FY2023	FY2022
An increase in mortality rate	21%	24%	12%	21%
Delays in procedures and tests have resulted in poor outcomes	65%	69%	71%	60%
Increase in complications from medical procedures	55%	57%	56%	51%
Increase in patients transferred or diverted to other facilities	46%	50%	46%	45%
Longer length of stay	51%	52%	55%	48%
Other (please specify)	5%	4%	4%	2%
Total	243%	256%	244%	227%

Q14a. Did your organization ever experience attacks against its supply chain?	FY2025	FY2024	FY2023	FY2022
Yes	44%	68%	64%	50%
No (please skip to Q16a)	54%	28%	30%	44%
Unsure (please skip to Q16a)	2%	4%	6%	6%
Total	100%	100%	100%	100%

Q14b. If yes, how many supply chain attacks did your organization experience over the past two years?	FY2025	FY2024	FY2023	FY2022
One	53%	46%	36%	44%
Two to five	22%	26%	33%	29%
Six to 10	16%	19%	21%	19%
More than 10	9%	9%	10%	8%
Total	100%	100%	100%	100%
Extrapolated value	3.7	4.0	4.2	3.9

Q15a. Did the supply chain attacks result in a disruption in patient care operations?	FY2025	FY2024	FY2023	FY2022
Yes	87%	82%	77%	70%
No	11%	18%	18%	24%
Unsure	2%	0%	5%	6%
Total	100%	100%	100%	100%

Q15b. If yes, what impact did the supply chain attacks have on patient care? Please select all that apply.	FY2025	FY2024	FY2023	FY2022
An increase in mortality rate	32%	26%	21%	23%
Delays in procedures and tests have resulted in poor outcomes	51%	48%	50%	54%
Increase in complications from medical procedures	49%	51%	45%	48%
Increase in patients transferred or diverted to other facilities	32%	38%	39%	40%
Longer length of stay	40%	45%	48%	51%
Other (please specify)	2%	3%	4%	3%
Total	206%	211%	207%	219%

Part 2. Protecting the cloud

Q16a. Will your organization move its clinical applications to the cloud?	FY2025
Yes, we have moved clinical applications to the cloud	30%
Yes, we plan to move clinical applications to the cloud in the next six months	9%
Yes, we plan to move clinical applications to the cloud within the next year (please skip to Q16c)	8%
Yes, we plan to move clinical applications to the cloud in the next one to two years (please skip to Q16c)	15%
Yes, we plan to move clinical applications to the cloud but there is no timeline (please skip to Q16c)	13%
No, we have no plans to move applications to the cloud (please skip to Q17a)	25%
Total	100%

Q16b. 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.	FY2025
1 or 2	16%
3 or 4	13%
5 or 6	17%
7 or 8	23%
9 or 10	31%
Total	100%
Extrapolated value	6.30

Q16c. If yes, what type of cloud environment have you or will you move clinical applications to?	FY2025
Public cloud	34%
Private cloud	21%
Hybrid cloud	23%
Hosted	22%
Total	100%

Q17a. Did your organization ever experience a successful cloud/account compromise?	FY2025	FY2024	FY2023	FY2022
Yes	72%	69%	63%	54%
No (please skip to Q18)	28%	29%	33%	41%
Unsure (please skip to Q18)	0%	2%	4%	5%
Total	100%	100%	100%	100%

Q17b. How many times have attackers compromised cloud-based user accounts within your organization over the past two years?	FY2025	FY2024	FY2023	FY2022
Once	2%	0%	0%	5%
2 to 5	10%	13%	12%	9%
6 to 10	11%	12%	14%	6%
11 to 15	16%	16%	10%	9%
16 to 20	23%	21%	21%	22%
21 to 25	15%	19%	19%	22%
26 to 50	14%	13%	16%	18%
More than 50	9%	6%	8%	9%
Total	100%	100%	100%	100%
Extrapolated value	21.2	19.9	21.4	21.7

Q17c. Which cloud-based user accounts/collaboration tools were most attacked in your organization? Please select all that apply.	FY2025	FY2024	FY2023
Email	45%	59%	49%
Text messaging	59%	61%	45%
Zoom/Skype/video conferencing	54%	56%	53%
Teams/Slack/Office collaboration tools	43%	47%	49%
Project management tools	29%	31%	53%
OneDrive/Dropbox/document/file-sharing tools	35%	47%	49%
System-generated email	21%	23%	51%
Virtual desktop infrastructure (VDI)	25%	24%	
Total	348%	348%	349%

Q18a. Did the cloud/account compromises result in a disruption in patient care operations?	FY2025	FY2024	FY2023	FY2022
Yes	61%	57%	49%	64%
No	31%	34%	40%	32%
Unsure	8%	9%	11%	4%
Total	100%	100%	100%	100%

Q18b. If yes, what impact did the cloud/account compromises have on patient care? Please select all that apply.	FY2025	FY2024	FY2023	FY2022
An increase in mortality rate	36%	32%	29%	18%
Delays in procedures and tests have resulted in poor outcomes	35%	44%	47%	49%
Increase in complications from medical procedures	61%	56%	53%	51%
Increase in patients transferred or diverted to other facilities	40%	36%	37%	37%
Longer length of stay	52%	52%	48%	50%
Other (please specify)	4%	1%	3%	2%
Total	228%	221%	217%	207%

Part 3. Data loss protection/exfiltration

Q19. How many data loss and exfiltration incidents involving sensitive and confidential healthcare data occurred within your organization over the past two years?	FY2025	FY2024	FY2023
Once	4%	0%	8%
2 to 5	9%	8%	5%
6 to 10	13%	14%	12%
11 to 15	19%	25%	24%
16 to 20	21%	12%	10%
21 to 25	20%	25%	23%
26 to 50	9%	10%	13%
More than 50	5%	6%	5%
Total	100%	100%	100%
Extrapolated value	18.4	20.0	19.4

Q20. What were the root cause(s) of the data loss and exfiltration incident? Please select all that apply.	FY2025	FY2024
Accidental data loss	23%	26%
Employee negligence because of not following policies	35%	31%
Privilege access abuse	25%	20%
Malicious insiders	18%	15%
Employee sends PII or PHI to an unintended recipient via email	25%	21%
Use of stolen credentials	15%	11%
Social engineering	14%	13%
Exploitation of vulnerabilities	8%	9%
Phishing	11%	12%
Unsure	16%	17%
Total	190%	175%

Q21a. Did the data loss or exfiltration result in a disruption in patient care operations?	FY2025	FY2024	FY2023
Yes	55%	51%	43%
No, Please skip to Q22	40%	45%	51%
Unsure, Please skip to Q22	5%	4%	6%
Total	100%	100%	100%

Q21b. If yes, what impact did the data loss or exfiltration incident have on patient care? Please select all that apply.	FY2025	FY2024	FY2023
An increase in mortality rate	54%	50%	46%
Delays in procedures and tests have resulted in poor outcomes	36%	37%	34%
Increase in complications from medical procedures	31%	34%	38%
Increase in patients transferred or diverted to other facilities	29%	33%	36%
Longer length of stay	27%	21%	24%
Other (please specify)	4%	3%	6%
Total	181%	178%	184%

Q22. What security methods and technologies does your organization use to reduce phishing and other email-based attacks? Please select all that apply.	FY2025	FY2024
Secure email gateway (SEG)	52%	45%
Domain-based Message Authentication (DMARC)	43%	42%
Email data loss prevention	36%	39%
Anti-virus/anti-malware	49%	53%
Multi-factor authentication	54%	49%
Patch & vulnerability management	51%	52%
Managed Security Service Provider (MSSP)	43%	46%
Firewalls	33%	36%
AI/ML	41%	44%
Threat intelligence	38%	41%
Other (please specify)	8%	4%
Total	448%	451%

Q23. What other technologies has your organization implemented to prevent identity risk and lateral movement in its network? Please select all that apply.	FY2025	FY2024
Account takeover protection	42%	
Identity and access management (IAM)	53%	56%
Privileged access management (PAM)	59%	61%
Identity theft detection and response (ITDR)	43%	40%
Intrusion detection & prevention systems (IDPS)	37%	35%
User and entity behavior analytics (UEBA)	33%	33%
Alerts from SIEM to gain visibility	50%	45%
Endpoint protection	41%	39%
Rules-based DLP solution	39%	45%
Other (please specify)	5%	2%
Total	402%	356%

Q24. What security methods and technologies has your organization implemented to prevent data loss or an exfiltration incident? Please select all that apply.	FY2025	FY2024
Policy fine tuning to prevent data loss	27%	23%
Secure web gateway (SWG)	28%	28%
Cloud security tools	35%	44%
Data security posture management (DSPM)	31%	
Insider threat management (ITM)	43%	
Web isolation technology	33%	29%
Encryption for data at rest	38%	41%
Encryption for data in transit	43%	46%
Endpoint data loss prevention	45%	
Network data loss prevention	44%	
Email data loss prevention	38%	
Cloud data loss prevention	35%	
Web data loss prevention	31%	
IT/IT security team triages incidents	29%	25%
Manual policy orchestration	37%	29%
Other (please specify)	5%	3%
Total	542%	304%

Q25a. Does your organization take steps to address the risk of employees' lack of awareness about cybersecurity threats?	FY2025	FY2024	FY2023	FY2022
Yes	76%	71%	65%	59%
No	20%	29%	30%	35%
Unsure	4%	0%	5%	6%
Total	100%	100%	100%	100%

Q25b. If yes, what steps does it take? Please select all that apply.	FY2025	FY2024	FY2023	FY2022
Regular training and awareness programs	63%	59%	57%	63%
Simulations of phishing attacks	47%	45%	40%	41%
Monitoring of employees	51%	53%	54%	59%
Audits and assessments of areas most vulnerable to employees' lack of awareness	44%	39%	43%	39%
Include user's compliance with privacy and security policies in performance evaluations	37%	34%	36%	35%
Other (please specify)	6%	5%	4%	3%
Total	248%	235%	234%	240%

Q26. 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?	FY2025	FY2024	FY2023
1 or 2	11%	11%	8%
3 or 4	19%	23%	33%
5 or 6	11%	20%	14%
7 or 8	28%	26%	16%
9 or 10	31%	20%	19%
Total	100%	100%	100%
Extrapolated value	6.48	5.92	5.20

Q27. 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?	FY2025	FY2024	FY2023
1 or 2	9%	15%	15%
3 or 4	11%	23%	20%
5 or 6	16%	23%	26%
7 or 8	32%	24%	25%
9 or 10	32%	15%	14%
Total	100%	100%	100%
Extrapolated value	6.84	5.52	5.56

Q28. 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?	FY2025	FY2024	FY2023
1 or 2	8%	11%	15%
3 or 4	10%	18%	17%
5 or 6	12%	23%	21%
7 or 8	30%	23%	25%
9 or 10	40%	25%	22%
Total	100%	100%	100%
Extrapolated value	7.18	6.16	5.94

Part 4. AI and machine learning in healthcare

Q29. Has your organization adopted AI? Please select one choice only.	FY2025	FY2024
Yes, AI is embedded in cybersecurity	30%	28%
Yes, AI is embedded in both cybersecurity and patient care	27%	26%
No, but we plan to adopt AI in the future (please skip to Part 5)	21%	26%
We don't have plans to adopt AI (please skip to Part 5)	22%	20%
Total	100%	100%

Q30. The deployment of AI-based security technologies will increase the productivity of our organization's IT security personnel.	FY2025	FY2024
Strongly disagree	20%	21%
Disagree	18%	15%
Unsure	7%	9%
Agree	25%	25%
Strongly Agree	30%	30%
Total	100%	100%

Q31. AI simplifies patient care and administrators' work by performing tasks that are typically done by humans but in less time and cost.	FY2025	FY2024
Strongly disagree	13%	15%
Disagree	11%	16%
Unsure	20%	21%
Agree	30%	23%
Strongly Agree	26%	25%
Total	100%	100%

Q32. To protect email from employees' negligence and error, does your organization use AI and machine learning to understand human behavior?	FY2025	FY2024
Yes	40%	36%
No (please skip to Q35)	60%	64%
Total	100%	100%

Q33. If yes, how important is understanding human behavior to protecting email on a scale from 1 = not important to 10 = very important?	FY2025	FY2024
1 or 2	9%	8%
3 or 4	17%	15%
5 or 6	19%	21%
7 or 8	23%	23%
9 or 10	32%	33%
Total	100%	100%
Extrapolated value	6.54	6.66

Q34. How effective is AI in improving the cybersecurity posture of your organization from 1 = not effective to 10 = very effective?	FY2025	FY2024
1 or 2	11%	11%
3 or 4	13%	13%
5 or 6	21%	19%
7 or 8	23%	25%
9 or 10	32%	32%
Total	100%	100%
Extrapolated value	6.54	6.66

Q35. How difficult is it to safeguard confidential and sensitive patient data used in your organization's AI on a scale from 1 = not difficult to 10 = very difficult?	FY2025	FY2024
1 or 2	9%	5%
3 or 4	12%	9%
5 or 6	19%	23%
7 or 8	25%	30%
9 or 10	35%	33%
Total	100%	100%
Extrapolated value	6.80	7.04

Q36. 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.	FY2025	FY2024
AI tools/technology we need are not available	22%	25%
We can't apply AI-based controls that span across the entire enterprise	25%	26%
We can't create a unified view of AI users across the enterprise	5%	4%
There are errors and inaccuracies in AI decision rules	21%	19%
There are errors and inaccuracies in data inputs ingested by AI technology (engine)	33%	32%
There is a heavy reliance on legacy IT environments	26%	23%
There are Interoperability issues among AI technologies	34%	32%
There is a lack of mature and/or stable AI technologies	28%	34%
Other (please specify)	6%	5%
Total	200%	200%

Q37. Does your organization use AI-based DLP?	FY2025
Yes, currently use	23%
We plan to adopt in six months	14%
We plan to adopt within one year	15%
We plan to adopt in one to two years	24%
We plan to adopt but have no timeline	11%
No, plan to adopt in the future (please skip to Part 5)	13%
Total	100%

Q38. How effective is AI-based DLP in preventing data loss incidents caused by employees from 1 =not effective to 10 = very effective?	FY2025
1 or 2	8%
3 or 4	17%
5 or 6	19%
7 or 8	31%
9 or 10	25%
Total	100%
Extrapolated balue	6.46

Q39. How effective is AI-based DLP in preventing data loss incidents caused by malicious insiders from 1 =not effective to 10 = very effective?	FY2025
1 or 2	12%
3 or 4	16%
5 or 6	22%
7 or 8	27%
9 or 10	23%
Total	100%
Extrapolated value	6.16

Part 5. Cyberattack experience

Q40. How many cyberattacks has your organization experienced over the past 12 months?	FY2025	FY2024	FY2023	FY2022
None (please skip to Part 6)	7%	8%	12%	11%
1 to 5	10%	15%	13%	12%
6 to 10	22%	23%	21%	15%
11 to 25	16%	12%	11%	13%
26 to 50	13%	11%	9%	11%
51 to 100	11%	12%	18%	23%
More than 100	21%	19%	16%	15%
Total	100%	100%	100%	100%
Extrapolated value	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.

Q41. Approximately, how much was the total cost from the one most significant cybersecurity attack in the past 12 months?	FY2025	FY2024	FY2023	FY2022
None	0%	0%	0%	0%
Less than $10,000	2%	0%	0%	0%
$10,001 to $100,000	7%	9%	7%	6%
$100,001 to $250,000	12%	10%	13%	12%
$250,001 to $500,000	15%	14%	18%	18%
$500,001 to $1,000,000	19%	18%	14%	16%
$1,000,001 to $5,000,000	21%	21%	19%	21%
$5,000,001 to $10,000,000	14%	15%	11%	13%
$10,000,001 to $25,000,000	8%	9%	15%	12%
More than $25,000,000	2%	4%	3%	2%
Cannot estimate	0%	0%	0%	0%
Total	100%	100%	100%	100%
Extrapolated value	$3,903,780	$4,740,400	$4,991,500	$4,429,000

Q42. To understand the relationship of each of the five categories to the total cost of a cybersecurity compromise, please allocate points to each category for a total of 100 points.	FY2025	FY2024	FY2023	FY2022
Remediation & technical support activities, including forensic investigations, incident response activities, help desk and delivery of services to patients	13	15	15	16
Users' idle time and lost productivity because of downtime or system performance delays	22	21	23	25
Disruption to normal healthcare operations because of system availability problems	31	31	26	23
Damage or theft of IT assets and infrastructure	16	15	15	21
Time required to ensure impact on patient care is corrected	18	18	21	15
Total Points	100	100	100	100

Part 6. Security spending & investment

Q43.What is your organization's approximate annual budget for IT?	FY2025	FY2024	FY2023	FY2022
Less than $1,000,000	2%	0%	2%	0%
1,000,000 to $5,000,000	5%	4%	3%	2%
5,000,001 to $10,000,000	7%	9%	8%	6%
10,000,001 to $25,000,000	12%	11%	11%	10%
25,000,001 to $50,000,000	18%	20%	25%	17%
$50,000,001 to $100,000,000	26%	25%	23%	28%
$100,000,000+	30%	31%	25%	37%
Cannot estimate	0%	0%	3%	0%
Total	100%	100%	100%	100%
Extrapolated value	$65,043,000	$66,170,000	$59,258,000	$75,200,000

Q44. What percentage of your organization's IT budget is dedicated to information security?	FY2025	FY2024	FY2023	FY2022
Less than 5%	5%	4%	5%	3%
5 to 10%	10%	9%	8%	7%
11 to 15%	16%	19%	21%	23%
16 to 20%	22%	33%	37%	35%
21 to 30%	27%	25%	19%	21%
More than 30%	20%	10%	10%	11%
Total	100%	100%	100%	100%
Extrapolated value	21%	19%	18%	19%

Part 7. Your role and organizational characteristics

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

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

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

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

Contact us

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

Ponemon INSTITUTE

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.

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% 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

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM