



2024 HIMSS HEALTHCARE CYBERSECURITY SURVEY

2024 HIMSS Healthcare Cybersecurity Survey

Table of Contents

- Executive Summary 3
- Methodology and Demographics..... 4
 - Methodology 4
 - Demographics 4
 - Levels of Responsibility 5
 - Types of Organizations Represented 5
- Economics of Healthcare Cybersecurity 6
 - Budgets are Improving 6
 - Overall IT Budgets are Modestly Improving 6
 - Allocation of current IT budget to cybersecurity 7
 - Comparing 2023 to 2024: Cybersecurity Budget Allocations 8
 - Trends in Cybersecurity Budget Allocations 9
 - Cybersecurity Budgets Projected to Rise 10
 - Changes to cybersecurity budget in 2025..... 10
 - Effect of Cybersecurity Budget Increases in 2025 11
- Security Awareness 12
 - Security Awareness Programs..... 12
 - Effectiveness of security awareness programs..... 13
- Security Incidents 14
 - Significant Security Incidents 14
 - Initial Points of Compromise..... 14
 - Testing of Incident Response Plans..... 15
 - Stakeholder Participation in Tabletop Exercises..... 16
- What’s Happening with Ransomware 17
 - Present State 17
 - 2024 Ransomware Trends 17
 - Ransomware Trends: 2022-2024 18
 - To Pay or Not to Pay – Ransomware Payments..... 19
 - Proactive vs. Reactive Security Measures..... 20
 - Future State..... 21
- AI Adoption in Healthcare 22
 - Allowing the Use of AI in Healthcare 22



To Govern or Not: Organizational Approaches to AI	22
AI Technology Use Cases.....	23
AI Guardrails.....	24
Approval Process for AI Technology	24
Active Monitoring of AI Technology	25
Acceptable Use Policy for AI Technology.....	25
Future Concerns Regarding AI	26
Managing Third-Party Risks	27
Third-Party Risk Management Programs.....	27
Third-Party Security Incidents.....	28
Impacts of Third-Party Security Incidents.....	29
Insider Threat Programs.....	30
Formal Insider Threat Programs	30
Insider Threat and AI.....	31
Insider Threat Activity Involving Third Parties.....	32
Conclusion	33
About HIMSS	34
How to Cite this Survey.....	34
How to Request Additional Information.....	34

Executive Summary



Cybersecurity Budgets

-  **Investments** - Organizations are dedicating more resources to fortify defenses.
 -  **Strategic Focus** - Budgets are increasingly aligned with critical vulnerabilities.
-



Security Awareness

-  **Phishing Mitigation** - Programs target phishing, the leading attack vector.
 -  **Innovative Training** - Gamification and scenario-based training boost engagement.
-



Security Incidents

-  **Phishing Dominance** - Phishing is the top method of compromise.
 -  **AI-Driven Attacks** - Deepfakes are an emerging threat.
-



Ransomware

-  **Combating Ransomware** - Ransomware defense continues to be a priority.
 -  **Fewer Ransom Payments** - Fewer ransomware victims are reporting paying ransom.
-

Artificial Intelligence

-  **Policy Shortfalls** - A lack of formal AI governance increases risk.
 -  **Limited Oversight** - There is limited monitoring of AI usage.
-

Third-Party Risks

-  **Third-Party Incidents** - Significant incidents involving third-parties are notable.
 -  **Impacts** - Third-party incidents cause disruption and other impacts.
-

Insider Threats

-  **Formal Programs** - Formal programs are needed to manage insider threats.
-

Methodology and Demographics

The **2024 HIMSS Healthcare Cybersecurity Survey** reflects the responses of **273** healthcare cybersecurity professionals. These professionals had at least some responsibility for day-to-day cybersecurity operations or oversight of the healthcare organization's cybersecurity program. Respondents who indicated they did not have any level of responsibility for either day-to-day cybersecurity operations or oversight were not eligible to take the survey.

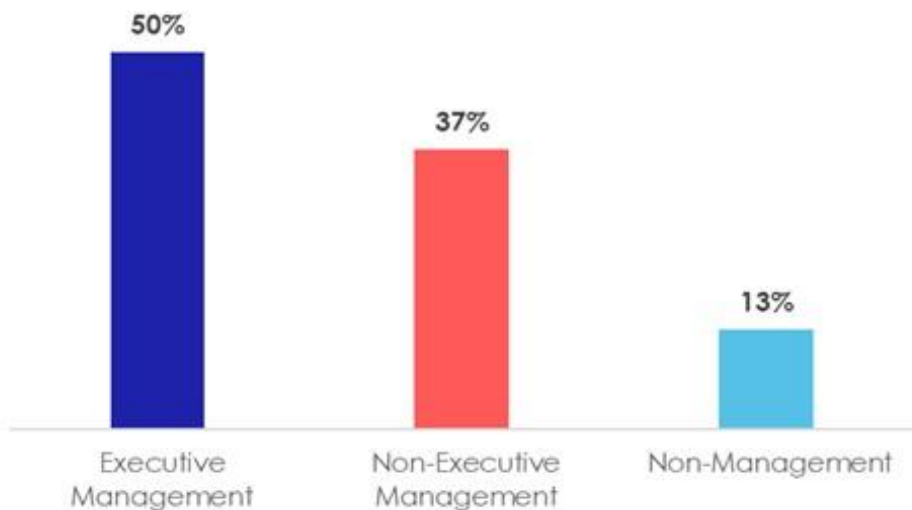
Methodology

The data for this survey was collected between November 6 and December 16, 2024. Questions asked respondents about their perspectives, knowledge, and experiences over the past 12 months. For simplicity, we refer to this data as "2024" throughout this report. Similarly, data from previous surveys is identified by the year in which it was collected.

Demographics

As shown in Figure 1 below, respondents held various roles, including executive management (50%), non-executive management (37%), and non-management (13%). Executive management included individuals in the C-suite, non-executive management comprised senior management, and non-management encompassed analysts and specialists.

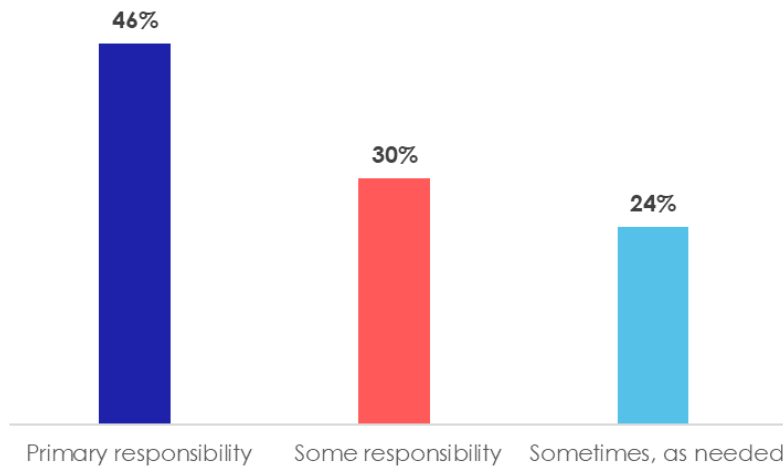
Figure 1: Respondent Roles



Levels of Responsibility

As shown in Figure 2 below, respondents reported varying levels of involvement in their organization's cybersecurity programs. 46% had primary responsibility, 30% shared responsibility, and 24% were involved as needed in the day-to-day operations or oversight.

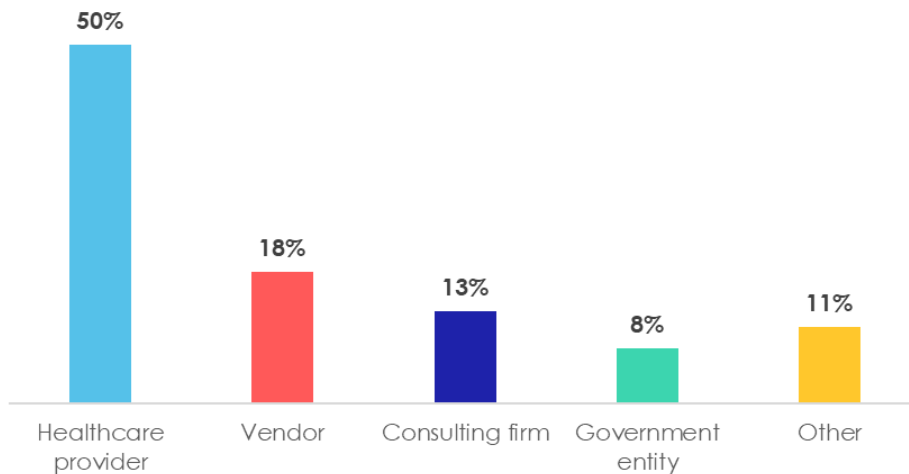
Figure 2: Respondent Cybersecurity Responsibility



Types of Organizations Represented

As shown in Figure 3 below, respondents represented a diverse range of organizations, including healthcare providers (50%), vendors (18%), consulting firms (13%), government entities (8%), and other organizations (11%). Other organizations included academic institutions, non-profits, payors, and life sciences companies.

Figure 3: Types of Organizations



Economics of Healthcare Cybersecurity

Investing in robust cybersecurity measures is no longer optional for healthcare organizations — it is essential. Yet, achieving a strong cybersecurity posture requires sufficient resources, which are often limited by budgetary constraints. Chief Information Security Officers and their teams frequently find themselves balancing the need to address evolving threats with the reality of tight financial resources.

Healthcare organizations with greater financial resources are better equipped to leverage robust cybersecurity solutions. Sufficient cybersecurity funding enables organizations to access advanced tools, hire skilled personnel, and implement comprehensive strategies. Conversely, limited budgets can pose challenges, making it more difficult to address the ever-evolving cyber threat landscape effectively. However, even with modest resources, strategic planning and prioritization can play a critical role.

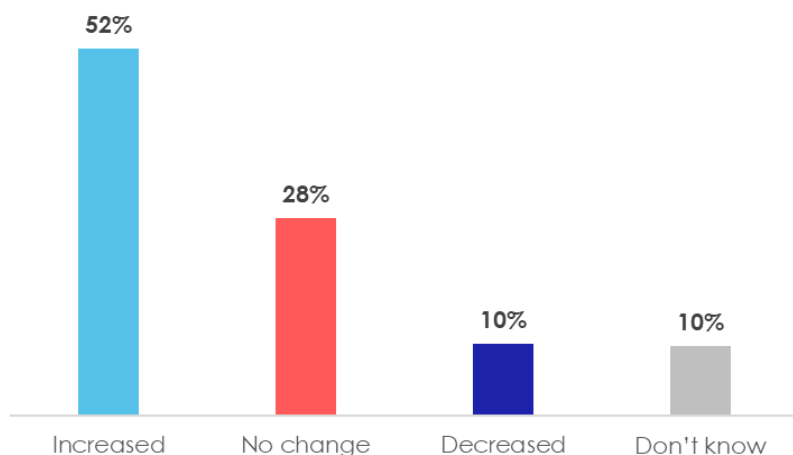
Budgets are Improving

Overall IT Budgets are Modestly Improving

Traditionally, healthcare organizations have generally allocated 6% or less of their IT budgets to cybersecurity, according to aggregate data from the 2018 to 2022 and 2024 HIMSS Healthcare Cybersecurity Surveys. Since cybersecurity budgets are typically carved out of overall IT budgets, this survey examined both the expected changes in overall IT budgets from fiscal year 2024 to fiscal year 2025 and the current allocation of those budgets to cybersecurity.

As shown in Figure 4 below, a slight majority of respondents (52%) reported that their organizations' overall IT budgets would increase during this period, while 10% indicated a decrease. 28% of respondents reported no change in their overall IT budgets. Ten percent of respondents did not know about the anticipated change in IT budget from 2024 to 2025.

Figure 4: Anticipated Change in IT Budget 2024 to 2025

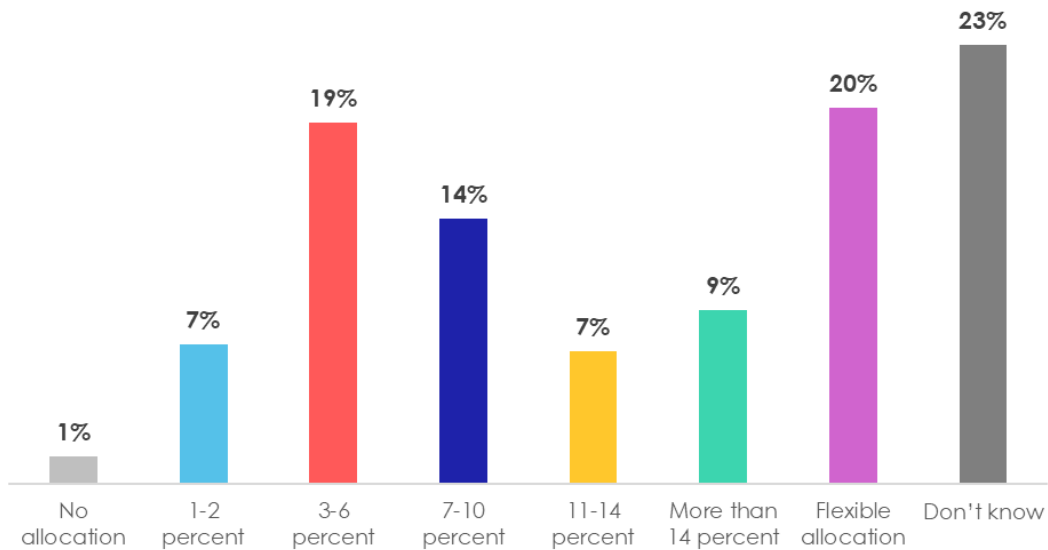


Allocation of current IT budget to cybersecurity

Understanding how organizations allocate their IT budgets to cybersecurity provides valuable insight into their prioritization of security measures. Variability in spending levels highlights differences in how organizations approach protecting their systems and data. These budgetary decisions present opportunities to strengthen defenses and enhance preparedness against evolving threats.

When asked about organizational allocation of the current IT budget to cybersecurity, 20% of respondents indicated that their organization had no specific carve-out but spent money on cybersecurity, as shown in Figure 5 below. However, 19% of respondents reported their organizations allocated 3-6% of the overall IT budget to cybersecurity; 14% reported 7-10%; 7% reported 11-14%; 9% reported more than 14%; and 7% reported 1-2%. One percent of respondents — several vendors and a healthcare provider — indicated their organizations do not spend any money on cybersecurity. Notably, 23% of respondents did not know what percentage of their organizations' IT budgets were allocated to cybersecurity.

Figure 5: Percent of Organization's IT Budget Spent on Cybersecurity



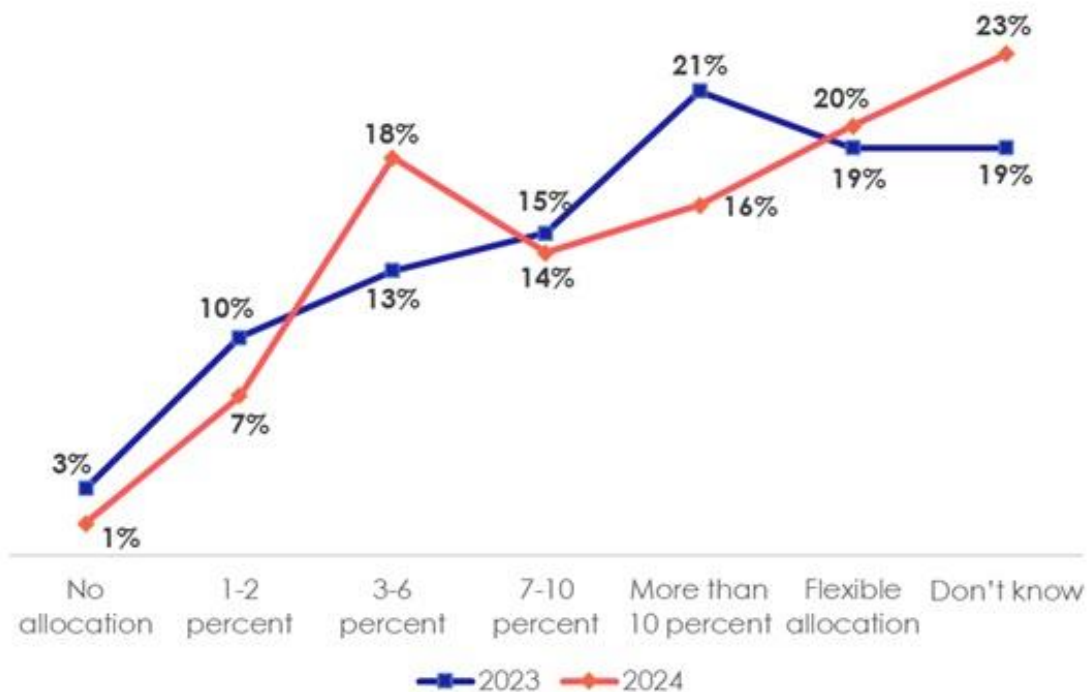
Comparing 2023 to 2024: Cybersecurity Budget Allocations

Data from the 2023 and 2024 HIMSS Healthcare Cybersecurity Surveys reveal a notable shift in cybersecurity budget allocations. The percentage of organizations allocating 3-6% of their IT budgets to cybersecurity increased from 13% in 2023 to 18% in 2024, while those allocating 1-2% decreased from 10% to 7%, as shown below in Figure 6. Allocations between 7-10% were similar, decreasing slightly from 15% of organizations in 2023 to 14% in 2024, while above 10% dropped significantly, from 21% of organizations in 2023 to 16% in 2024, reflecting a possible redistribution of resources or more strategic spending.

The percentage of organizations without a specific carve-out for cybersecurity increased slightly, from 19% in 2023 to 20% in 2024. Additionally, respondents unaware of their organizations' cybersecurity budget allocations rose from 19% in 2023 to 23% in 2024, pointing to potential gaps in communication or governance over cybersecurity spending.

These findings suggest that organizations are optimizing cybersecurity investments, moving toward more moderate budget allocations. However, the increase in respondents unaware of their organizations' cybersecurity budget allocations underscores the need for improved communication around cybersecurity priorities. While executive management respondents were generally aware of cybersecurity budget allocations, non-management and non-executive management respondents demonstrated limited awareness, highlighting an opportunity for better information sharing about organizational cybersecurity programs.

Figure 6: Cybersecurity Budget Allocation, 2023 vs. 2024



Trends in Cybersecurity Budget Allocations

Over the years, cybersecurity budget allocation within IT budgets has shown notable fluctuations, reflecting changes in organizational priorities and resource allocation strategies. As shown in Table 1, organizations reporting no cybersecurity allocation remained steady at 1-3%, while allocations in the 1-2% range peaked at 18% in 2020 but dropped to 7% in 2024. Budgets in the 3-6% range dipped to 13% in 2023 before recovering to 18% in 2024, indicating stability in moderate spending. Allocations in the 7-10% range gradually increased from 10% in 2020 to 14% in 2024, showing growing investment in higher cybersecurity budgets. Budgets exceeding 10% peaked at 21% in 2023 before falling to 16% in 2024, suggesting shifts toward more balanced spending.

The percentage of healthcare organizations with flexible or unspecified cybersecurity budgets declined from 26% in 2019 to 20% in 2024, reflecting improved budgeting practices. However, respondents unaware of their organizations' cybersecurity budgets rose from 18% in 2020 to 23% in 2024, highlighting communication gaps. While modest increases in healthcare cybersecurity budgets are evident, additional investments are critical to address growing threats, protect sensitive assets, and support new technologies. Without sufficient funding, organizations risk disruptions to patient care, loss of trust, and significant financial and reputational harm.

Table 1: Cybersecurity Budget Allocation, 2019-2024

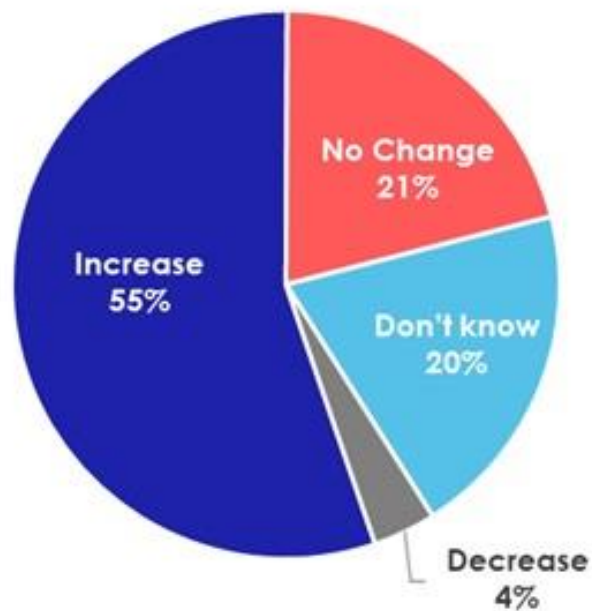
Budget Allocation	2019	2020	2021	2023	2024
No allocation	1%	1%	1%	3%	1%
1-2 percent	9%	18%	18%	10%	7%
3-6 percent	25%	24%	22%	13%	19%
7-10 percent	11%	10%	15%	15%	14%
More than 10 percent	10%	6%	11%	21%	16%
Flexible Allocation	26%	23%	24%	19%	20%
Don't Know	18%	18%	10%	19%	23%

Cybersecurity Budgets Projected to Rise

Changes to cybersecurity budget in 2025

Anticipated changes to cybersecurity budgets provide insight into organizations' evolving priorities and strategies. With the growing complexity of cyber threats, many organizations recognize the need to adjust their spending to stay ahead. These shifts highlight an increasing focus on bolstering defenses and addressing emerging risks. As shown in Figure 7 below, among respondents who reported a specific allocation for their organizations' cybersecurity budgets, a slight majority (55%) anticipated an increase in 2025. Only 4% expected a decrease, while 21% stated their budgets would remain the same. Notably, 20% of respondents indicated they did not know.

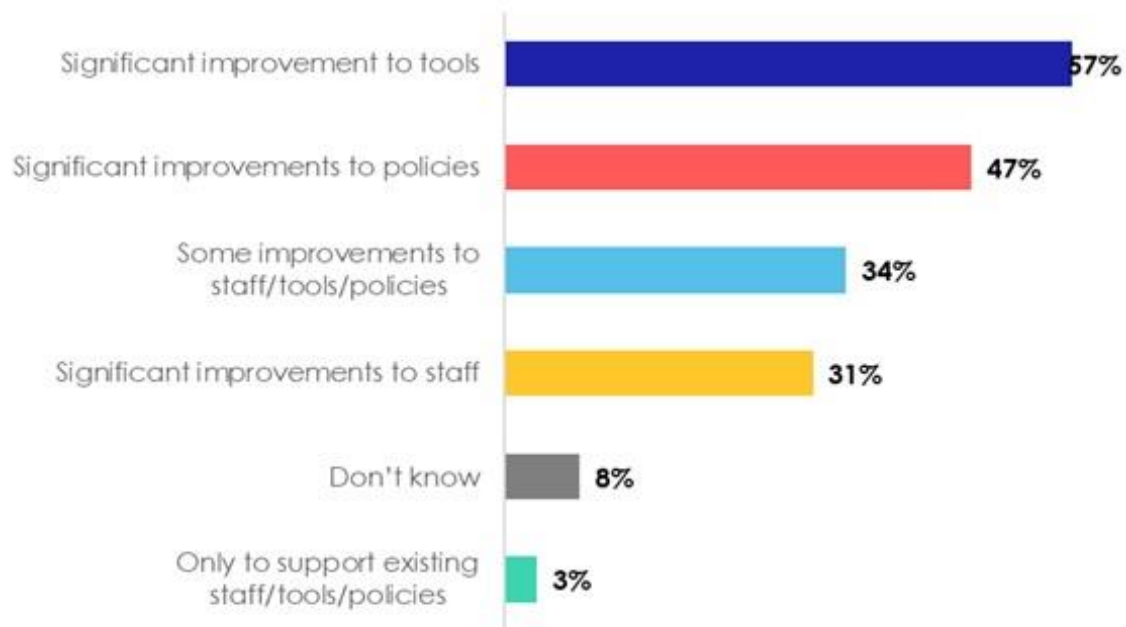
Figure 7: Change to Cybersecurity Budget in 2025



Effect of Cybersecurity Budget Increases in 2025

Among respondents who indicated that their cybersecurity budgets would increase, we asked whether the increase enabled their organizations to make meaningful improvements, such as investing in additional staff, tools, and/or policies. As shown in Figure 8, a majority (57%) reported significant improvements to the tools they use, 47% reported significant improvements to policies, and 31% reported significant improvements to staff. Notably, 34% stated that the increase allowed for only some improvements across staff, tools, and policies. Three percent indicated that the increase merely maintained existing support for staff, tools, and policies, and 8% of respondents stated that they did not know.

Figure 8: Impact of Increase in Cybersecurity Budget for 2025



Security Awareness

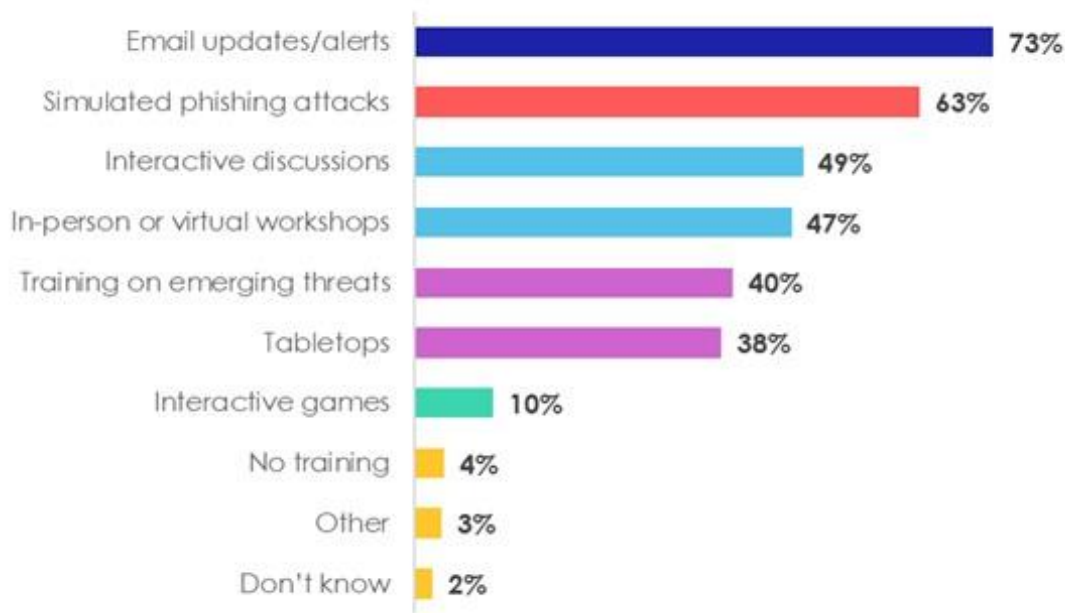
Security Awareness Programs

Effective security awareness training is vital for helping employees recognize and respond to cybersecurity threats. Organizations use a variety of methods to engage their workforces and reinforce key concepts, tailoring their approaches to address their specific risks. Understanding the strategies employed provides valuable insight into how organizations prioritize education as part of their overall defense strategies.

As shown in Figure 9 below, respondents reported using a variety of methods for security awareness training, with 73% citing regular email alerts and communications, 63% using simulated phishing, 49% using interactive discussions, and 47% holding in-person or virtual workshops. Incident response exercises like tabletops were used by 38%, while 10% engaged in interactive games. Notably, 4% reported no training, 2% were unaware if training occurred, and 3% used alternate methods like video-based training or compliance activities, which are not equivalent to effective cybersecurity training. Only 40% addressed emerging threats like deepfakes, quishing (QR code phishing), and smishing (SMS phishing), highlighting the need for comprehensive, up-to-date training programs to counter evolving threats.

Organizations may need to develop custom training programs since off-the-shelf security awareness training might not adequately address emerging threats. Tailored approaches ensure that training is relevant and comprehensive, equipping teams to effectively identify and respond to sophisticated attacks.

Figure 9: Methods for Security Awareness Training



Effectiveness of security awareness programs

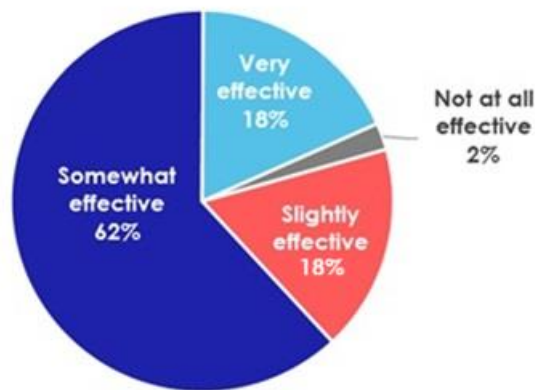
Security awareness programs are a key element of organizational defense, designed to educate employees on recognizing and responding to potential threats. As cybersecurity risks continue to evolve, the effectiveness of these programs is critical in reducing vulnerabilities and preventing incidents. Evaluating how well these programs perform can highlight areas for improvement and ensure they remain aligned with the changing threat landscape.

As shown in Figure 10 below, we asked respondents whose organizations conduct security awareness programs to assess the effectiveness of these programs. A majority (62%) indicated their programs are somewhat effective, while 18% described them as very effective. Another 18% reported their programs are only slightly effective, and 2% stated they are not effective at all. The relatively low percentage of respondents rating their programs as very effective (18%) suggests a need for enhanced strategies. It is suggested that organizations focus on key areas for improvement, including addressing emerging threats and mitigating risks from new and emerging technologies. Strengthening these security awareness programs could better equip organizations to stay ahead of evolving cybersecurity challenges and bolster their overall defenses.

Proactive measures, such as gamification, tabletop exercises, and interactive workshops, can help educate the workforce about both basic and advanced threats. These approaches can engage employees effectively, fostering practical skills and awareness.

Social engineering remains a dominant attack method, making it crucial for security awareness programs in healthcare organizations to address emerging threats such as deepfakes (image, audio, video), smishing, and quishing.

Figure 10: Effectiveness of Security Awareness Training Programs



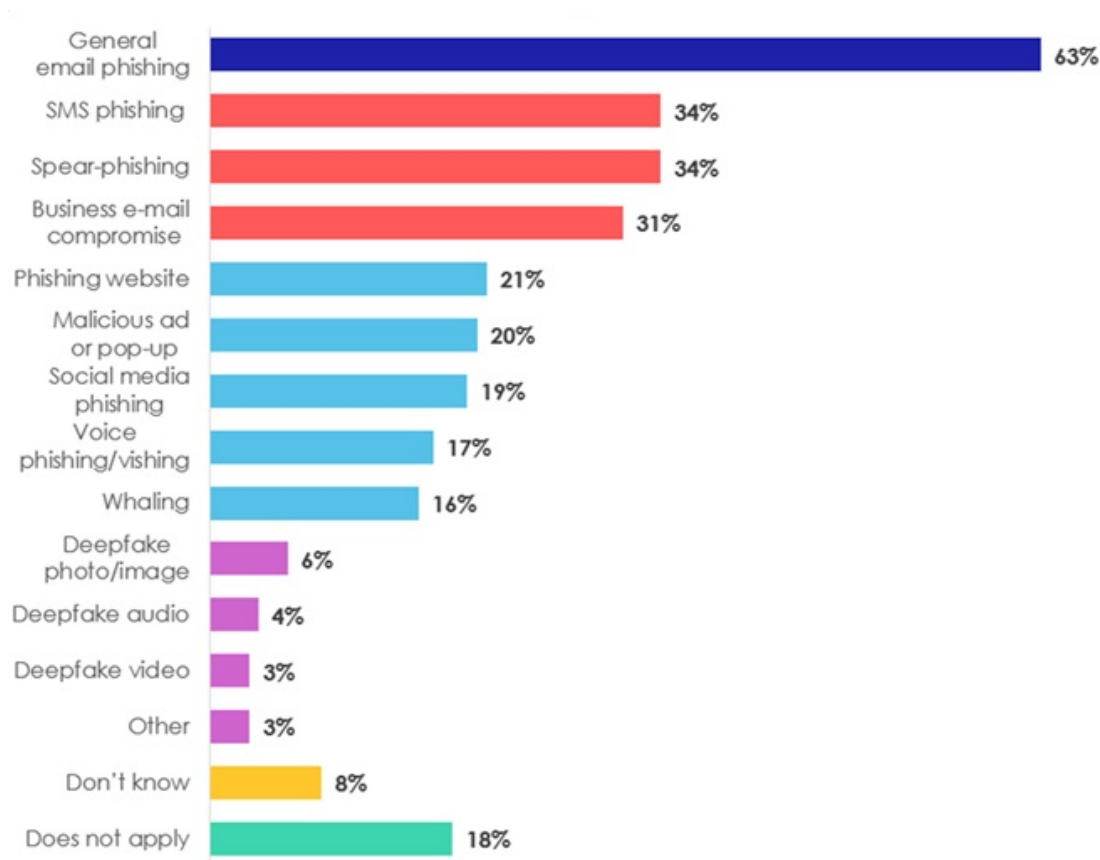
Security Incidents

Significant Security Incidents

Initial Points of Compromise

Understanding initial points of compromise is key to identifying vulnerabilities and strengthening defenses since they often serve as gateways for attackers. Addressing these weaknesses can significantly reduce the risk of breaches and improve security posture. As shown in Figure 11 below, we asked respondents to identify initial points of compromise for significant security incidents in the past year. General email phishing (63%), SMS phishing and targeted spear-phishing (each 34%), business email compromise (31%), phishing websites (21%), malicious ads (20%), social media phishing (19%), vishing (voice phishing) (17%), and whaling (also known as executive impersonation) (16%), deepfake images (6%), audio deepfakes (4%), video deepfakes (3%), distributed denial of service (DDoS) attacks (3%), and privacy breaches (3%) were reported. Eight percent did not know. Eighteen percent reported no significant security incidents,

Figure 11: Initial Points of Compromise for Significant Security Incidents in the Past 12 Months



Testing of Incident Response Plans

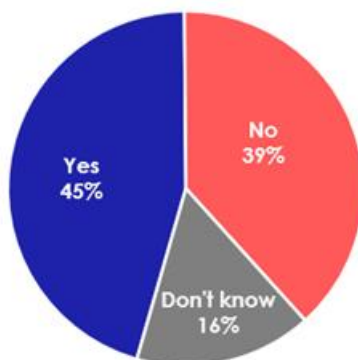
Regular testing of incident response plans is essential to ensure organizations are prepared to handle cybersecurity incidents effectively. Tabletop exercises play a critical role in identifying gaps, improving coordination, and strengthening overall response capabilities. Understanding how frequently organizations engage in these exercises provides insight into their level of preparedness and commitment to mitigating potential risks.

We asked respondents whether their organizations conduct tabletop exercises to test the capabilities of their incident response programs. As shown in Figure 12 below, 45% of respondents indicated that their organizations do conduct tabletop exercises, while 39% reported they do not. Sixteen percent stated that they were unsure whether their organizations conduct tabletop exercises.

These findings highlight a mixed level of preparedness among organizations, with many failing to test their incident response plans by using tabletop exercises. Tabletop exercises are critical for simulating various scenarios, identifying gaps in response capabilities, and strengthening overall incident response strategies.

The 16% of respondents unaware of whether their organizations conduct these exercises points to potential gaps in communication and participation. This underscores the importance of including all relevant stakeholders — regardless of their role — in tabletop exercises. Improving communication and transparency about incident response efforts can help ensure broader organizational awareness and more effective preparedness for potential incidents.

Figure 12: Organizations Conducting Tabletop Exercises for Incident Response Testing



Stakeholder Participation in Tabletop Exercises

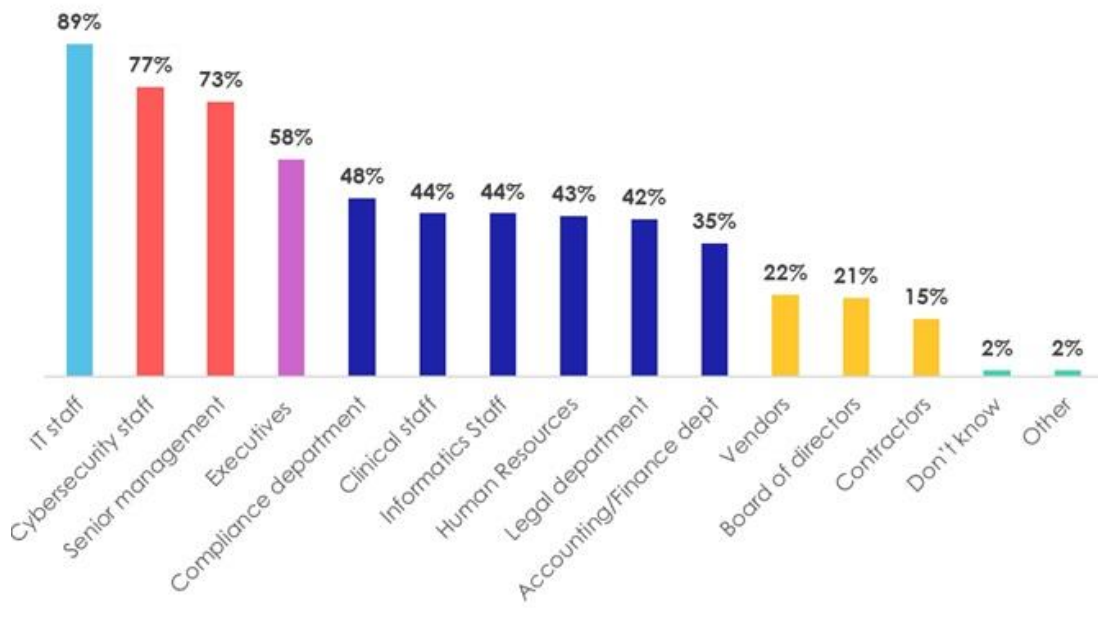
Respondents whose organizations conduct tabletop exercises identified participants. The results show a diverse range of participants but also highlight gaps in participation. As shown in Figure 13 below, IT staff (89%) and cybersecurity staff (77%) were the most frequently involved stakeholders, reflecting their critical roles in managing and responding to incidents. Senior management participation was reported at 73%, while executives, including C-suite leaders, participated in 58% of cases, demonstrating robust level of leadership engagement.

Other departments within healthcare organizations were involved in tabletop exercises:

- Compliance (48%)
- Clinicians (44%)
- Informatics (44%)
- Human resources (43%)
- Legal (42%)
- Accounting and finance (35%)

External parties, such as vendors (22%) and contractors (15%), had low participation rates. This may point to an area for improvement, given their potential involvement when incidents occur. Additionally, the board of directors participated in only 21% of cases, despite their critical role in overseeing cybersecurity risk. Two percent of respondents stated they did not know which stakeholders participate, while another 2% reported that other stakeholders, such as emergency preparedness professionals, were involved on an *ad hoc* basis.

Figure 13: Tabletop Exercise Participants



What's Happening with Ransomware

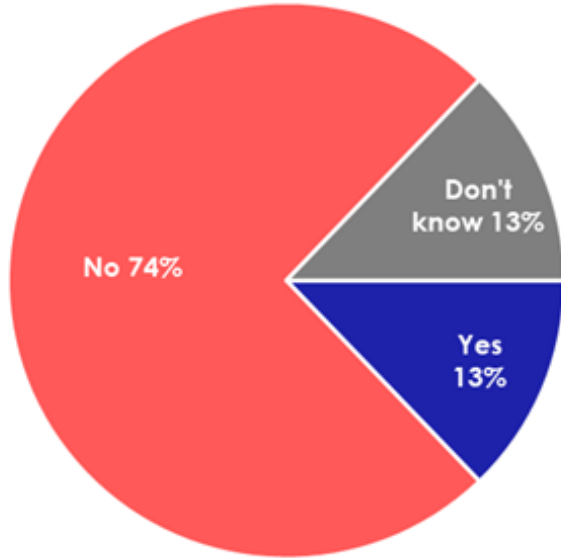
Present State

Ransomware attacks continue to be a significant threat. Often state sponsored, these attacks are highly organized and sophisticated. Healthcare organizations experienced aggressive attacks since at least 2018, and the threat remains as persistent as ever.¹ Ransomware leak sites are prevalent.² Healthcare providers, payors, vendors, and other entities across the healthcare ecosystem have been targeted. Ransomware remains a critical issue, highlighting the need for robust defenses and effective response strategies.

2024 Ransomware Trends

Healthcare organizations appear to be prepared to prevent and defend against ransomware attacks in 2024. As shown below in Figure 14, a majority of respondents (74%) indicated that their organizations had not experienced ransomware attacks in the past 12 months. However, 13% reported that their organizations had been targeted, underscoring the ongoing risk ransomware poses to the healthcare and public health sector. Thirteen percent of respondents — primarily from non-executive management and non-management roles — stated they did not know whether their organizations had experienced such an attack.

Figure 14: Ransomware Attack in 2024



¹ U.S. Department of Health and Human Services. Ransomware Trends in Healthcare. [hhs.gov, https://www.hhs.gov/sites/default/files/ransomware-healthcare.pdf](https://www.hhs.gov/sites/default/files/ransomware-healthcare.pdf). Accessed Jan. 24 2025.

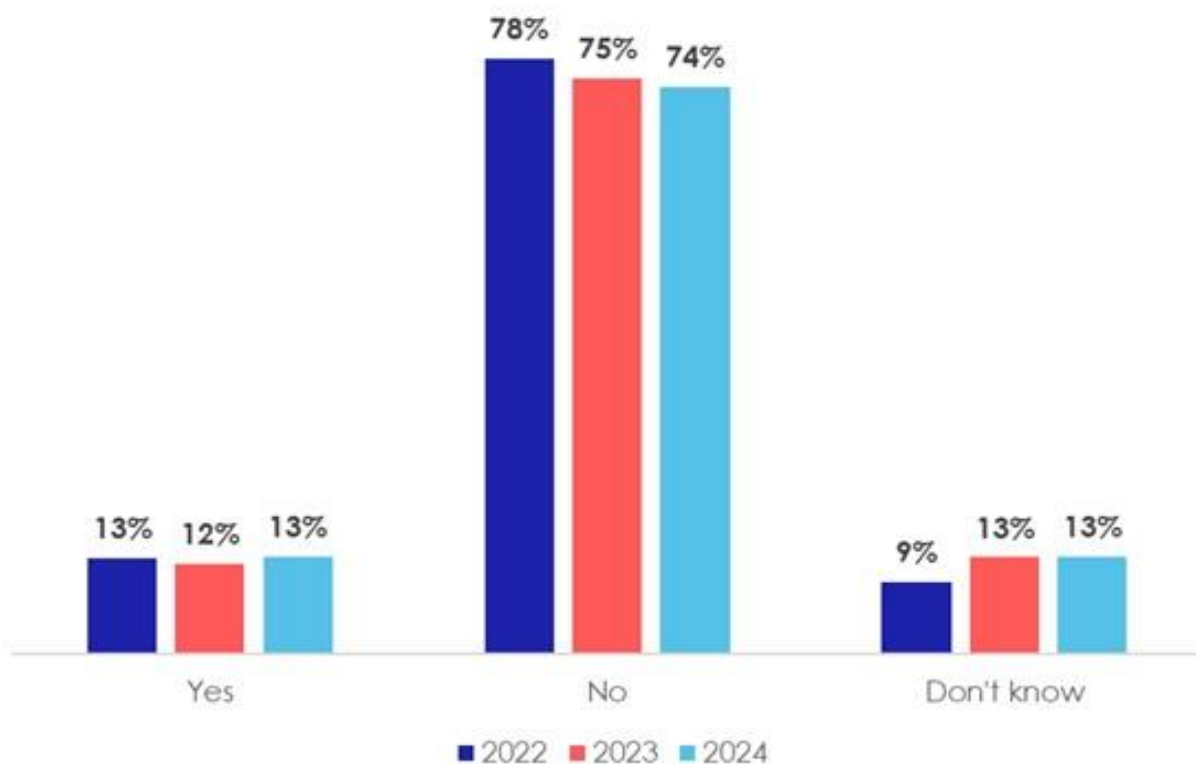
² Palo Alto Networks. Unit 42 Ransomware Leak Site Data Analysis. Palo Alto Networks, <https://unit42.paloaltonetworks.com/unit-42-ransomware-leak-site-data-analysis/>. Accessed Jan. 24 2025.

Ransomware Trends: 2022-2024

The percentage of respondents reporting that their organizations experienced ransomware attacks has remained relatively consistent in recent years. As shown in Figure 15 below, in 2024, 13% indicated their organizations had experienced a ransomware attack, slightly higher than the 12% reported in 2023 and matching the 13% reported in 2022. Similarly, the percentage of respondents reporting no ransomware attacks remained steady at 74% in 2024, compared to 75% in 2023 and 78% in 2022. Respondents who did not know whether their organizations experienced a ransomware attack were 13% of respondents in 2023 and 2024, compared to 9% in 2022.

These findings highlight the importance of improving visibility and transparency regarding ransomware incidents. Even when organizations are not directly impacted, the persistent threat of ransomware necessitates constant vigilance, proactive planning, and robust defenses to safeguard sensitive assets and ensure operational and clinical continuity.

Figure 15: Ransomware Attacks from 2022-2024



To Pay or Not to Pay – Ransomware Payments

Ransomware victims face the tough decision of whether to pay, based on their specific circumstances. Among healthcare organizations victimized in 2024, 62% of respondents reported not paying a ransom, 11% paid the ransom, and 27% did not know, as shown in Figure 16. In 2023, 30% of respondents stated that their organizations paid the ransom, while 52% did not, and 18% did not know, as shown below in Figure 17. Paying a ransom not only has the potential to embolden threat actors but also increases the likelihood of repeated targeting or additional attacks on other healthcare organizations. There is a need for better coordination, planning, and information sharing to improve resilience.

Figure 16: Ransomware Payments in 2024

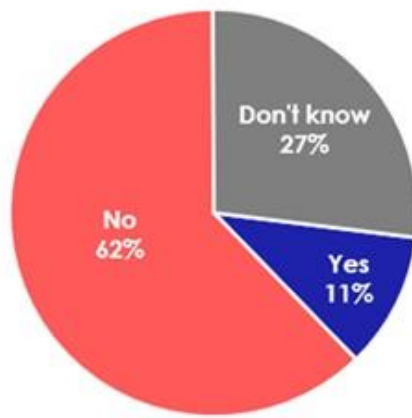
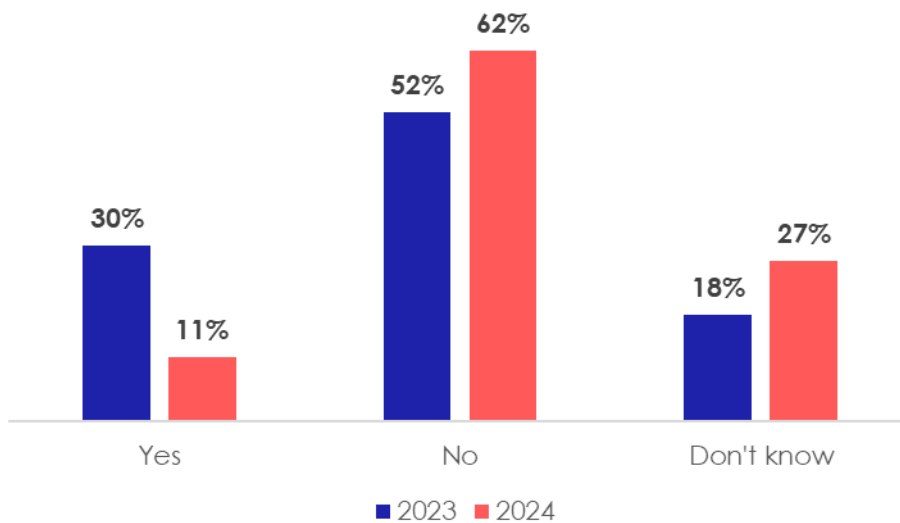


Figure 17: Ransomware Payments in 2023-2024



Proactive vs. Reactive Security Measures

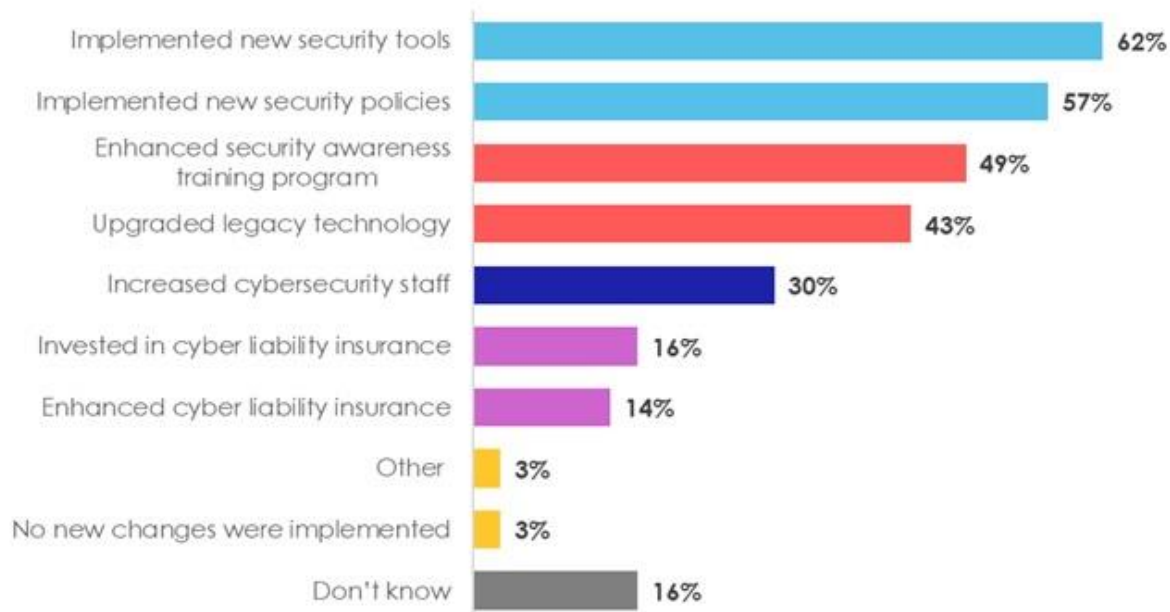
Organizations reported a range of proactive and reactive security measures in response to evolving cyber threats. As shown below in Figure 18, the most common actions included implementing new security tools (62%) and establishing new security policies (57%), emphasizing the importance of strengthening both technical defenses and governance frameworks.

Nearly half of respondents (49%) reported enhancing their security awareness training programs, underlining the critical role of workforce education in recognizing and mitigating potential threats. Other significant measures included upgrading legacy technology (43%) and increasing cybersecurity staff (30%), both essential for maintaining operational resilience in the face of sophisticated attacks.

A smaller percentage of respondents reported investing in cyber liability insurance (16%) or enhancing existing coverage (14%), reflecting a less common but still important strategy for managing the potential financial impacts of cyber incidents.

While these findings indicate a predominantly proactive stance among healthcare organizations, they also highlight areas for improvement. Notably, 16% of respondents stated they were unaware of what measures had been implemented, and 3% reported that no new changes were made — an approach that aligns more closely with reactive security practices. Additionally, 3% focused solely on device lifecycle management, which, while important, may not adequately address the broader risks posed by today's evolving threat landscape.

Figure 18: Post-Ransomware Attack Changes



Future State

Ransomware attacks are likely to continue evolving, with an increase in both frequency and sophistication. Emerging technologies, such as artificial intelligence and, in the future, quantum computing, are expected to accelerate this trend.³ However, greater information sharing within and across organizations can strengthen the resilience of the healthcare sector.

The development of Central Bank Digital Currencies (CBDCs), including those in the United States and other nations, may also help mitigate cybersecurity risks. By offering secure, regulated alternatives to cryptocurrencies, CBDCs could reduce the appeal of untraceable payments often exploited by ransomware attackers. While their adoption is still debated, CBDCs have the potential to disrupt the ransomware economy and improve defenses against cyber threats.

³ 2025 Cyber Security Predictions: The Rise of AI-Driven Attacks, Quantum Threats, and Social Media Exploitation. DEVOPSDigest, Nov. 26 2024, <https://www.devopsdigest.com/2025-cyber-security-predictions-the-rise-of-ai-driven-attacks-quantum-threats-and-social-media>. Accessed 24 Jan. 2025.

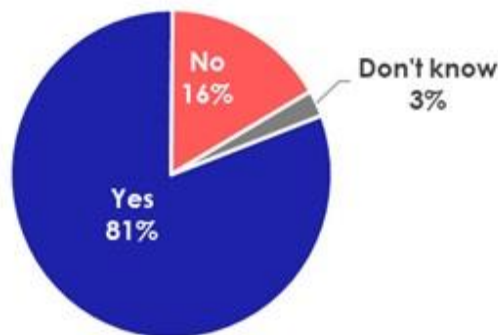
Cyber Resilience of the Central Bank Digital Currency Ecosystem." International Monetary Fund, Aug. 27 2024, <https://www.imf.org/en/Publications/fintech-notes/Issues/2024/08/27/Cyber-Resilience-of-the-Central-Bank-Digital-Currency-Ecosystem-554090>. Accessed Jan. 24 2025.

AI Adoption in Healthcare

Allowing the Use of AI in Healthcare

Artificial intelligence (AI) is becoming increasingly ubiquitous in healthcare. We asked respondents whether their organizations currently allow the use of AI technology. As shown in Figure 19 below, 81% of respondents indicated that their organizations allow the use of AI. 16% reported that their organizations do not currently permit AI use, and 3% stated they were unsure whether AI is allowed in their organizations.

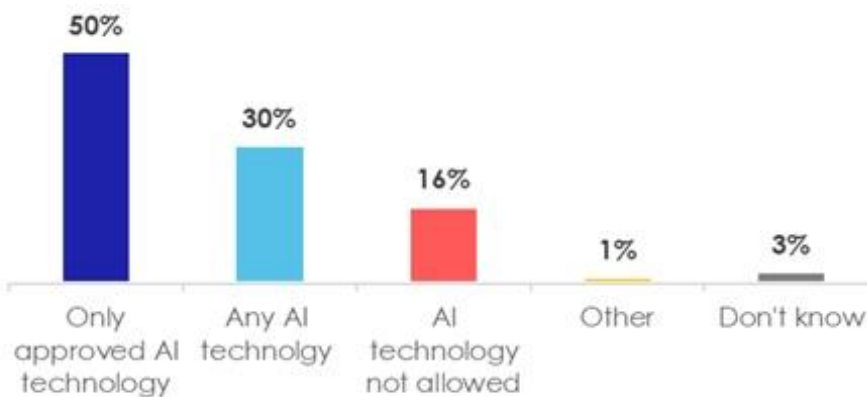
Figure 19: Allowing the Use of AI Technology



To Govern or Not: Organizational Approaches to AI

As shown in Figure 20 below, half (50%) of respondents said their organizations permit only approved AI technologies, while 30% allow AI without formal restrictions, and 16% prohibit AI use entirely. A small group (1%) reported active measures like developing AI policies or implementing guardrails, while 3% were unsure of their organizations' stance.

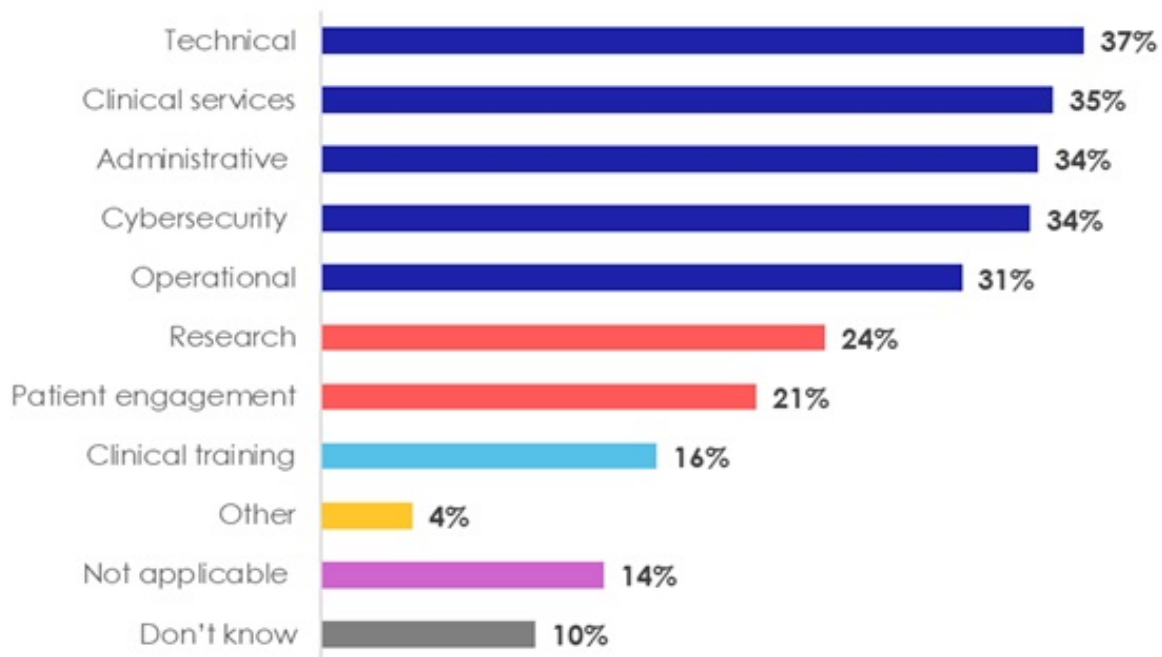
Figure 20: AI Technology Restrictions



AI Technology Use Cases

Artificial intelligence is being utilized in various ways across healthcare organizations. As shown in Figure 21, 37% of respondents reported using AI for technical tasks like support and data analytics, 35% for clinical services such as diagnostics, and cybersecurity and administrative tasks (each 34%). AI is also used in healthcare operations (31%), research (24%), patient engagement (21%), and clinical training (16%). Four percent noted niche applications like virtual meeting transcription and content creation. Ten percent were unaware about AI technology use in their organizations. Fourteen percent stated that this did not apply to them. More AI technology use cases are anticipated for the future as AI becomes more prevalent.

Figure 21: AI Technology Uses in Organizations



AI Guardrails

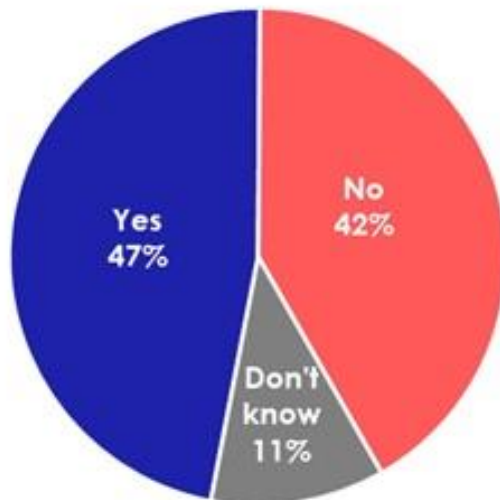
Guardrails are essential for ensuring the responsible and secure use of AI technology. In this context, guardrails refer to the policies, processes, or measures designed to manage the risks associated with AI.

Approval Process for AI Technology

An approval process serves as a proactive guardrail by vetting AI technologies before adoption, reducing the likelihood of unauthorized or inappropriate use. Meanwhile, monitoring AI usage functions as a reactive guardrail, providing ongoing oversight of AI activities to identify and address potential misuse, compliance issues, or security risks.

We asked respondents whether their organizations have approval processes in place for AI technologies, such as for users seeking to implement new solutions that have not been officially approved. As shown in Figure 22 below, nearly half (47%) indicated that their organizations do have approval processes, while 42% reported that they do not. An additional 11% were unsure whether such processes exist within their organizations.

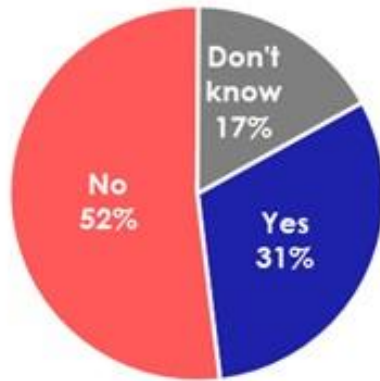
Figure 22: Approval Process for AI Technology



Active Monitoring of AI Technology

As shown in Figure 23 below, only 31% of respondents reported their organizations actively monitor AI usage across systems and devices, while 52% said they do not, and 17% did not know. The lack of monitoring poses risks such as data breaches and others. There is a need for robust monitoring strategies to ensure safe and responsible use of AI technologies.

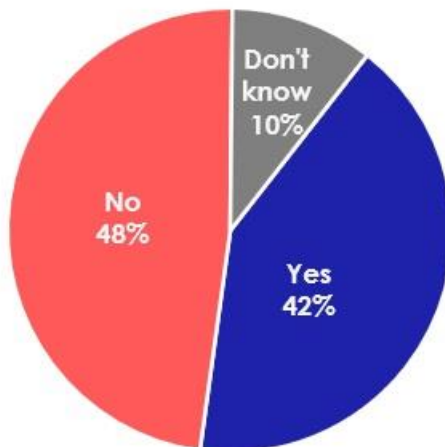
Figure 23: Active Monitoring of AI Technology Usage Across Enterprise Systems



Acceptable Use Policy for AI Technology

An acceptable use policy (AUP) sets clear guidelines for the safe and responsible use of technology, including AI, and can be standalone or integrated into a general policy based on the organization's AI adoption. As shown below in Figure 24, 42% of respondent stated that their healthcare organizations have written AUPs for AI, 48% indicated they do not, and 10% did not know.

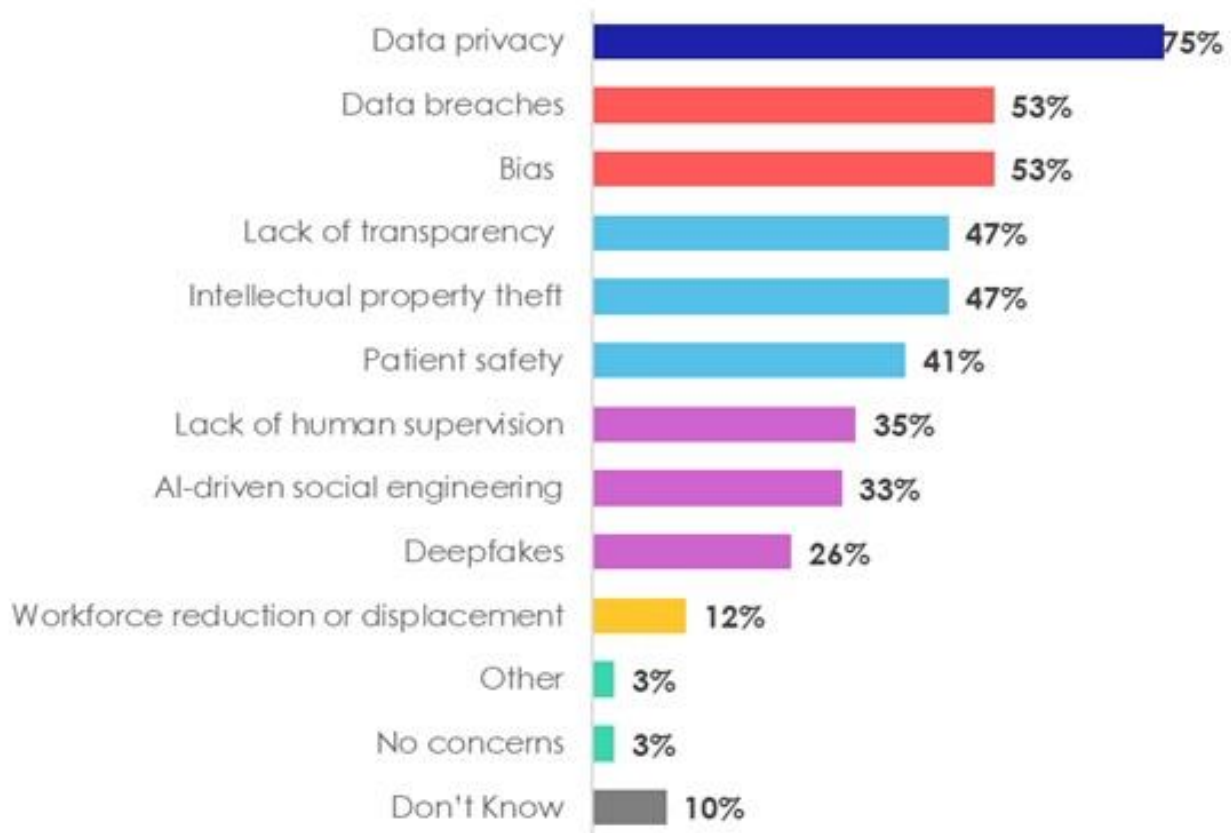
Figure 24: Acceptable Use Policy for AI Technology



Future Concerns Regarding AI

As AI reshapes healthcare in the future, its adoption raises concerns. As shown below in Figure 25, 75% of respondents cited data privacy as a top concern, followed by data breaches (53%) and bias in AI systems (53%). Nearly half expressed concerns about intellectual property theft (47%) and lack of transparency (47%), while 41% highlighted patient safety risks. Other concerns included lack of human supervision (35%), AI-driven social engineering (33%), and deepfakes (26%), with 12% noting workforce displacement. These findings underscore the need for robust safeguards, ethical frameworks, and proactive measures to address the risks.

Figure 25: Future Concerns for AI



Managing Third-Party Risks

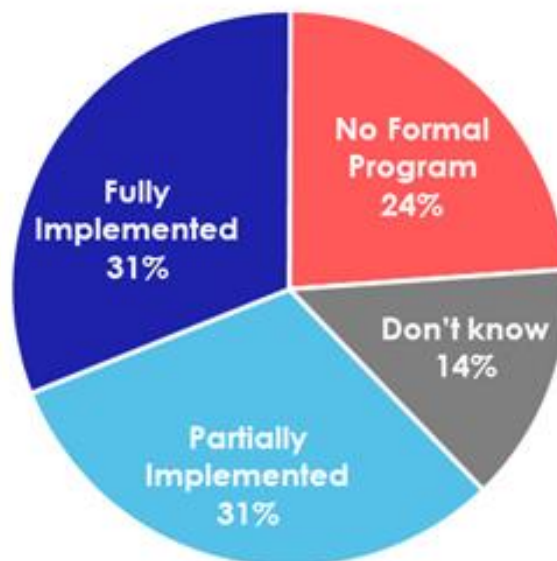
Healthcare organizations have become increasingly reliant on third-party vendors and service providers to support their security operations and infrastructure. This dependence has driven efficiency, fostered innovation, and enhanced organizational capabilities. However, it has also introduced new risks. Significant security events involving third parties have led to financial repercussions, disruptions to clinical operations, and reduced availability of electronic health records and other critical systems.

Third-Party Risk Management Programs

We asked respondents how their healthcare organizations are managing third-party risks, including those tied to vendors, suppliers, and service providers. A formal third-party risk management program provides a structured process to identify, assess, and address risks associated with third parties, ensuring consistent policies and procedures are followed.

However, as shown below in Figure 26, only 31% of respondents reported having a fully implemented formal third-party risk management program, while 31% indicated their program is partially implemented. Another 24% stated they do not have a program in place, and 14% were unsure whether their organizations have implemented a formal third-party risk management program.

Figure 26: Healthcare Organizations with Formal Third-Party Risk Management Program



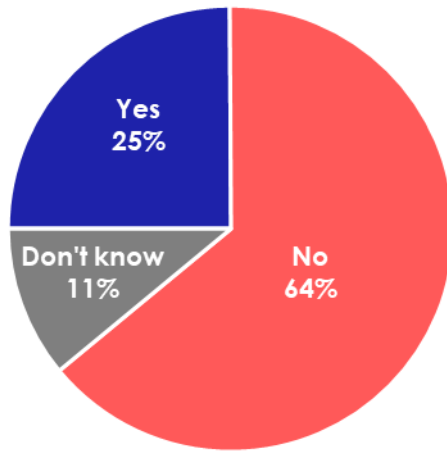
Third-Party Security Incidents

The cascading and far-reaching impacts of third-party security incidents have underscored the critical importance of effective third-party risk management, as highlighted by numerous media reports. To better understand the impact of these incidents, we asked respondents about their experiences with significant third-party security breaches.

As shown in Figure 27, a quarter of respondents (25%) reported that their organizations had experienced a major security incident involving a vendor, supplier, or service provider. These incidents resulted in financial losses, operational disruptions, and/or delays. In contrast, the majority (64%) indicated that their organizations had not encountered any significant third-party security incidents in the past 12 months. However, 11% of respondents were unsure whether their organizations had been affected.

Notably, non-management respondents were more likely to report uncertainty compared to executives and non-executive management, suggesting potential gaps in communication or visibility regarding third-party security issues.

Figure 27: Significant Security Incident Involving a Third-Party

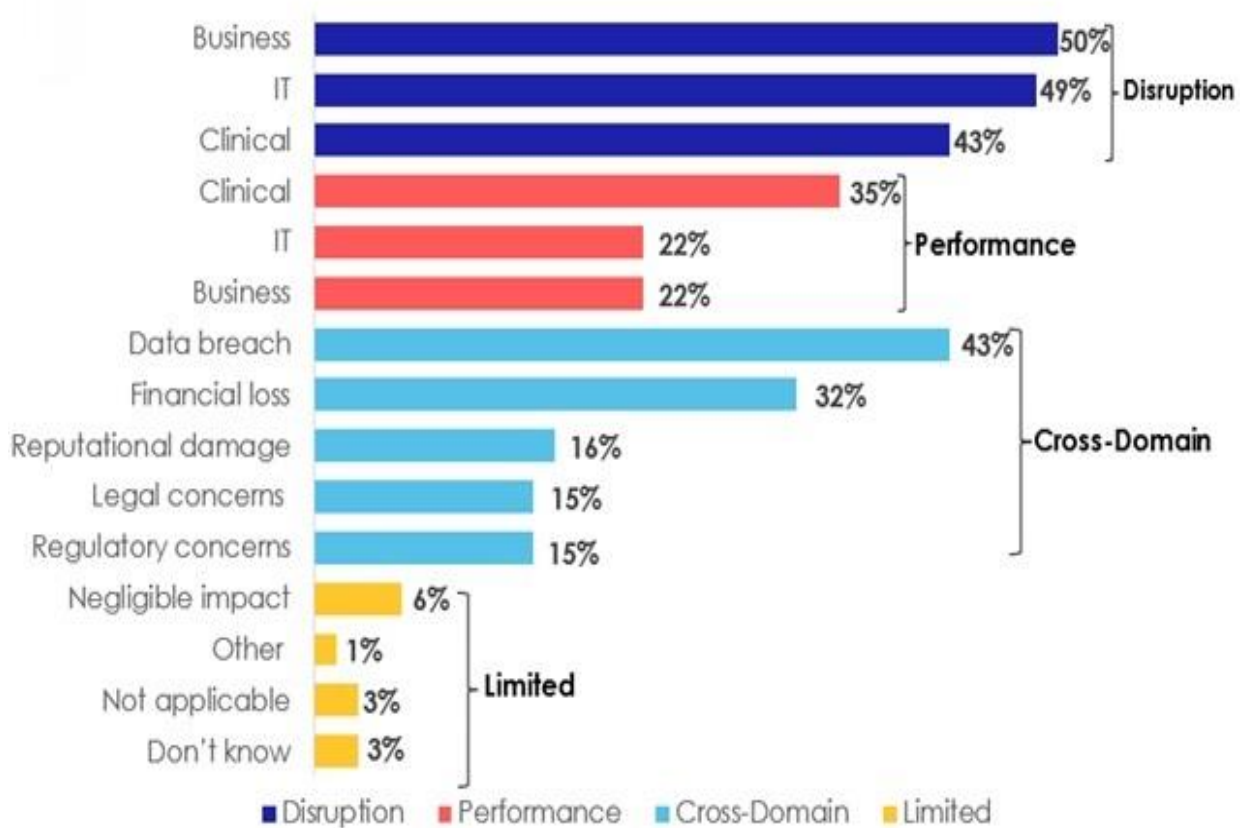


Impacts of Third-Party Security Incidents

In 2024, significant security incidents involving third parties highlighted critical vulnerabilities in supply chain integrity and the need for strong risk management practices. Vendors and service providers with trusted access to sensitive systems exposed healthcare organizations to disruptions across multiple domains. As shown in Figure 28, 50% of respondents reported business disruptions, 49% cited IT disruptions, and 43% experienced clinical service disruptions. Additionally, 35% noted diminished clinical productivity, while 22% reported reduced effectiveness in IT and business operations.

Cross-domain impacts included data breaches (43%), financial losses (32%), reputational damage (16%), and legal or regulatory concerns (15%). While 6% reported negligible effects, 3% noted no consequences, and another 3% were unsure of the impacts. There is a need for healthcare organizations to enforce stringent security requirements and improve oversight to reduce the cascading risks posed by third-party failures.

Figure 28: Significant Security Incident Involving a Third-Party



Insider Threat Programs

Insider threats remain a critical challenge for organizations, requiring proactive measures to identify and mitigate risks from within. A robust insider threat program can help organizations detect and address malicious and negligent actions before they result in serious consequences, thereby staying ahead of the threat. Understanding the prevalence and maturity of such programs provides valuable insight into how organizations are prioritizing internal security risks and safeguarding their operations.

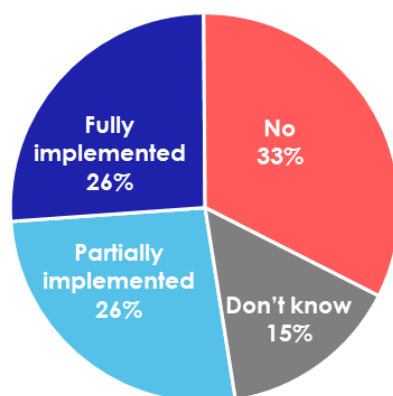
Formal Insider Threat Programs

We asked respondents whether their organizations have formal insider threat programs, including written policies, processes, and other key elements. As shown in Figure 29 below, just over a quarter of respondents (26%) reported that their organizations have fully implemented formal insider threat programs, while another 26% indicated their programs were only partially implemented. However, 33% of respondents stated that their organizations do not have a formal insider threat program, and 15% reported that they did not know whether such a program exists.

Not having a formal insider threat program leaves organizations vulnerable to unchecked malicious insider activity, which can result in significant breaches or incidents. Additionally, negligent insider activity can go unnoticed, further increasing the risk of data loss, operational disruptions, and compromised security.

Insider threats often remain undetected for extended periods, and the damage they cause can surpass that of external attacks. Healthcare organizations should implement robust insider threat programs that include comprehensive policies, processes, and monitoring to effectively mitigate these risks.

Figure 29: Formal Insider Threat Programs



Insider Threat and AI

As healthcare organizations increasingly adopt AI, understanding its role in insider threat incidents becomes essential. AI can amplify risks, making it important to assess how negligent or malicious activities involving AI can impact security. It is anticipated that the number of insider threat incidents involving AI will grow in the future.

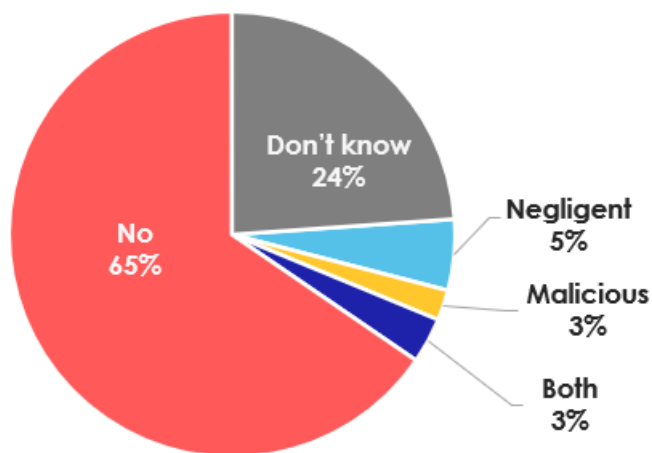
We also asked respondents whether their organizations had experienced insider threat incidents involving the use of AI. As shown in Figure 30 below, a small percentage of respondents reported negligent insider threat activity (5%), malicious insider threat activity (3%), or both negligent and malicious insider threat activity (3%). While these numbers may seem small, it is likely that many organizations have not yet implemented monitoring specifically for AI-driven insider threats, leaving potential risks undetected.

The majority of respondents (65%) indicated that their organizations had not experienced such incidents, while 24% stated that they did not know. Notably, one respondent mentioned that their board was aware of insider threat incidents specifically related to AI.

As AI becomes more pervasive in organizational operations, insider threat activity involving AI is expected to increase. The growing reliance on AI tools and systems introduces new opportunities for both negligent and malicious insider activity, which can amplify risks to sensitive data and operational integrity.

Given these emerging challenges, it is critical for healthcare organizations to proactively monitor and mitigate insider threats involving AI by implementing robust oversight measures, conducting regular audits, and fostering a culture of accountability and security awareness.

Figure 30: Incidence of Insider Threats Involving AI



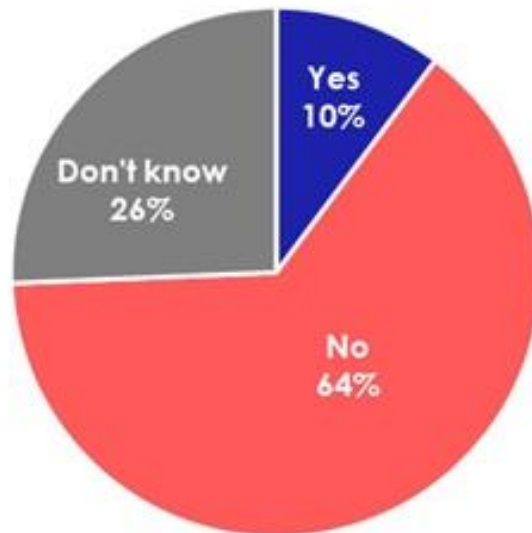
Insider Threat Activity Involving Third Parties

Third parties with trusted access to an organization's systems or facilities can introduce unique insider threat risks. These external entities, such as vendors, suppliers, or service providers, often have privileged access, making it essential to understand the extent to which organizations monitor and address potential incidents involving them. Exploring this issue sheds light on the challenges and opportunities for strengthening oversight of third-parties.

We asked respondents whether their organizations had experienced insider threat incidents involving an external party with trusted virtual or physical access, such as vendors, suppliers, or service providers. As shown below in Figure 31, 64% of respondents reported that their organizations had not encountered such incidents, while 10% confirmed that they had. Notably, 26% of respondents stated they did not know whether such incidents had occurred.

This uncertainty highlights the challenges organizations face in detecting and attributing insider threats involving external parties. It underscores the need for enhanced monitoring, reporting, and access management strategies to address these risks effectively. Additionally, the lack of awareness may reflect the absence of, or inadequately developed, formal insider threat programs within healthcare organizations.

Figure 31: Insider Threat Incidents Involving Third Parties



Conclusion

The findings of the 2024 HIMSS Healthcare Cybersecurity Survey show that healthcare organizations are making significant progress in strengthening their security posture. This survey report highlights critical areas for improvement, such as developing robust insider threat programs, improving third-party risk management, and monitoring AI. As the threat landscape evolves, healthcare organizations must stay vigilant, while ensuring that cybersecurity enables business and clinical care.

By implementing more robust cybersecurity defenses, healthcare organizations are better equipped to protect patient data and patient safety. Continued adaptation and innovation will be essential for navigating an increasingly digital world.

About HIMSS

Vision

To realize the full health potential of every human, everywhere.

Mission

Reform the global health ecosystem through the power of information and technology.

HIMSS (Healthcare Information and Management Systems Society) is a global advisor, thought leader and member-based society committed to reforming the global health ecosystem through the power of information and technology. As a mission-driven nonprofit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research and digital health transformation to advise leaders, stakeholders and influencers across the global health ecosystem on best practices. With a community-centric approach, our innovation engine delivers key insights, education and engaging events to healthcare providers, payers, governments, startups, life sciences and other health services organizations, ensuring they have the right information at the point of decision.

HIMSS has served the global health community for more than 60 years, with focused operations across North America, Europe, the United Kingdom, the Middle East and Asia-Pacific. Our members include more than 125,000 individuals, 430+ provider organizations, 500+ nonprofit partners and 550+ health services organizations.

How to Cite this Survey

Individuals are encouraged to cite this report in publications or any other medium, if the information is attributed to the **2024 HIMSS Healthcare Cybersecurity Survey**.

How to Request Additional Information

HIMSS
Marketing & Communications
press@himss.org