HIMSS

2023 HIMSS HEALTHCARE CYBERSECURITY SURVEY

HIMSS

2023 HIMSS Healthcare Cybersecurity Survey

Overview

The **2023 HIMSS Healthcare Cybersecurity Survey** provides insight into the state of healthcare cybersecurity based upon feedback from **229** cybersecurity professionals. Our findings generally showed improvements in healthcare cybersecurity, but new challenges have presented themselves in the realm of artificial intelligence. However, a significant number of healthcare organizations are ensuring that they are accountable for their progress in managing cybersecurity risk with appropriate oversight. In this report, we look to not only what is happening at the present time but also what is anticipated in the future.

Workforce development:

- 💼 **Hiring challenges -** Recruiting tops the list.
- ☑ **Retention challenges -** Retention of qualified cybersecurity staff is a challenge.

Cybersecurity budgets:

- ☑ **Increasing budgets -** There are greater budget allocations for cybersecurity.

Incidents:

- 🔍 **Detection -** Detection of incidents is often quick.
- 🎣 **Phishing -** Phishing is the hook for initial compromises.

Ransomware:

- 🚫 **Attacks -** Attacks are attenuated but expected to increase in the future.

Artificial intelligence:

- ⚛ **Generative AI -** A difference of opinion emerged about allowing GenAI (for now).
- ▤ **Policies -** Acceptable use policies may or may not address AI.

Boards of directors:

- ✔ **Oversight -** Boards of directors often have oversight of cybersecurity risk.
- 💼 **Briefings -** Regular briefings on cyber risk are made to boards of directors.

Future Directions:

- 💡 **AI, Quantum, and Beyond -** Technologies will become more embedded.
- ⚙ **Cybersecurity supply chain -** Cyber supply chain programs are needed.
- 🔍 **Frameworks -** Increasing adoption of NIST Cybersecurity Framework is predicted.
- 🔒 **Cyber Performance Goals -** Resilience and preparedness improve with adoption of CPGs.

Methodology and Demographics

The **2023 HIMSS Healthcare Cybersecurity Survey** reflects the responses of **229** healthcare cybersecurity professionals. These professionals had at least some responsibility for day-to-day cybersecurity operations or oversight.

Some respondents (45.85%) had primary responsibility over the healthcare cybersecurity programs at their respective organizations. Others had at least some responsibility (29.69%) or sometimes as needed (24.45%).

Figure 1: Respondent Cybersecurity Responsibility
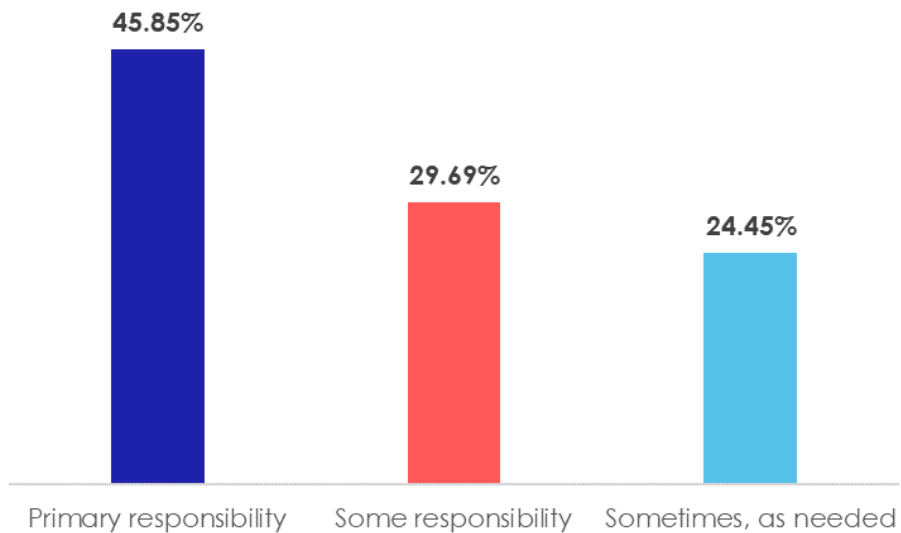
Organization Profile:

Some respondents either worked for healthcare provider organizations (45.41%), vendors (17.03%), consulting firms (13.10%), and government entities (8.73%).

Figure 2: Respondent Organization Type
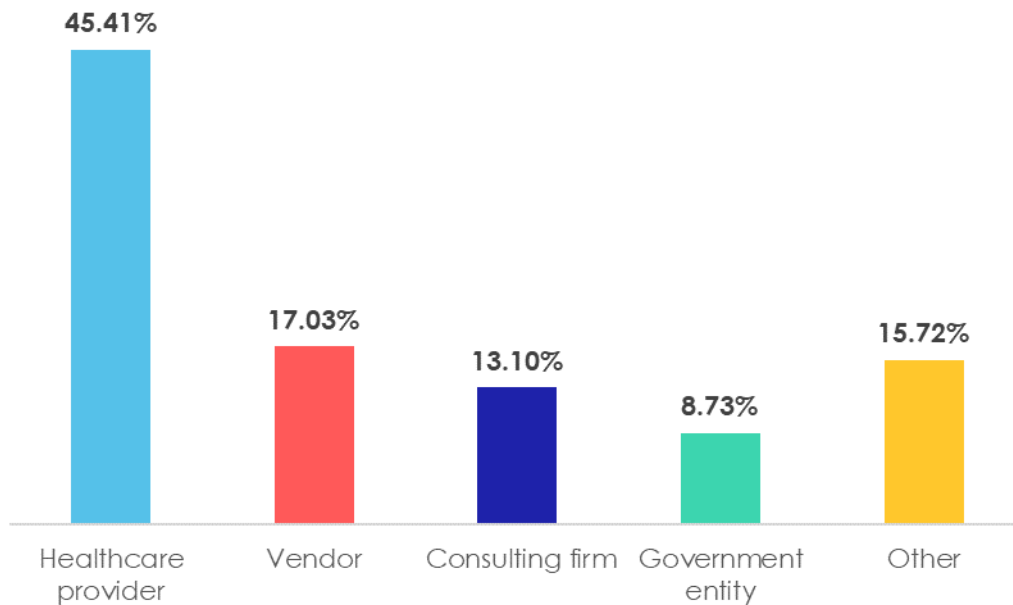
Professional Profile:

Respondents had roles in executive management (49.34%), non-executive management (34.06%), and non-management roles (16.59%).

Figure 3: Respondent Roles
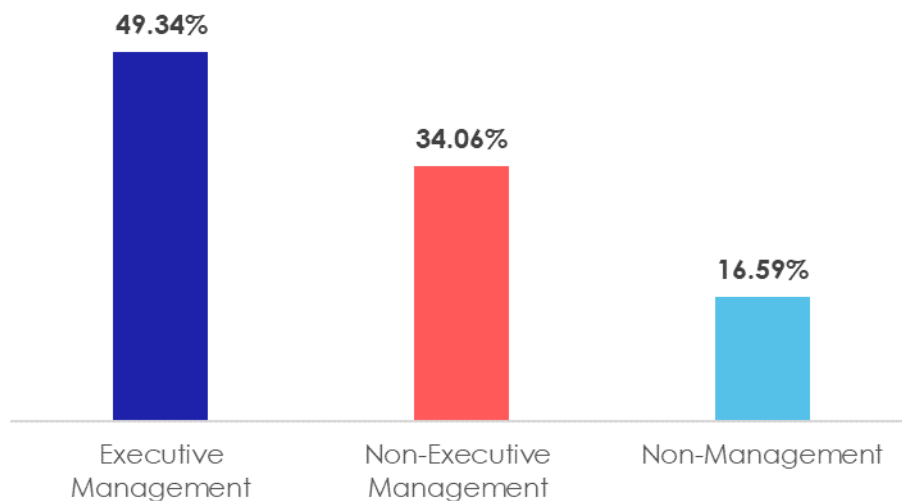
Findings

Section #1: Workforce Challenges

Many healthcare organizations have difficulty hiring qualified cybersecurity professionals. 2023 was no exception, but the challenge of hiring qualified cybersecurity professionals is not unique to the healthcare industry. The current cybersecurity workforce is estimated to be 1.4 million individuals in the United States and 5.5 million individuals around the world. [1] In spite of this, there is a significantly greater demand for cybersecurity professionals than the current supply of cybersecurity professionals. Globally, it is estimated that we need an additional 4 million individuals to fill the workforce. In the United States alone, there is a shortfall of 483,000 individuals. [2] Accordingly, there is significant competition for experienced cybersecurity professionals.

A. Recruiting is the Toughest Challenge

Recruiting qualified cybersecurity professionals was a significant workforce challenge for the majority of respondents (74.16%). There are many reasons for this. For instance, almost half of respondents (47.16%) to this year's survey indicated that the lack of cybersecurity related experience or skills was a challenge in hiring cybersecurity professionals. Notwithstanding this, almost half of respondents (42.79%) also indicated that their organizations lack sufficient budget to hire qualified healthcare cybersecurity professionals.

Another significant challenge was that some candidates had a lack of healthcare-related experience (37.99%). This is important because healthcare cybersecurity is directly correlated to patient safety.[3] Additionally, healthcare organizations are typically very complex and fast-paced environments that warrant not only robust cybersecurity practices, but also a recognition that timely access to patient information is vital. Laws and regulations, including HIPAA, also add to the complexity of securing the environment and ensuring appropriate use of sensitive information, such as but not limited to patient information.

Non-competitive compensation was also a challenge in hiring qualified healthcare cybersecurity professionals according to 27.95% of respondents. Not only can this be a challenge in hiring the right Chief Information Security Officer, but it can also be a

---

[1] ISC2. " ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce " 2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

[2] ISC2. " ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce." 2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf.

[3] U.S. Food and Drug Administration (FDA). "FDA. Medical Device Cybersecurity: Helping to Keep Patients and Medical Devices Safe." https://www.fda.gov/media/172737/download.

challenge in hiring specialized cybersecurity professionals, such as threat hunters and experienced security operations center (SOC) analysts and managers.

Table 1: Challenges to Hiring Healthcare Cybersecurity Professionals

Hiring Challenges	Percent
Insufficient budget	42.79%
Lack of healthcare-related experience	37.99%
Lack of qualified candidates	37.12%
Non-competitive compensation	27.95%
Lack of cybersecurity-related experience	26.64%
Lack of skills	20.52%
Non-competitive benefits package	13.97%
Lack of certifications	12.23%
Lack of alignment with organization's culture and values	9.61%
Lack of degrees	6.55%

B. Difficulties of Retaining Talent

Yet another consideration is whether the qualified cybersecurity professional who is doing well at the healthcare organization will actually stay. The retention of qualified candidates is a significant challenge for many organizations (57.32%). Reasons for dissatisfaction among cybersecurity professionals can include the lack of professional growth opportunities, a lack of executive support, stress, burnout, and inadequate compensation. Some cybersecurity professionals are also concerned about the loss of their jobs due to breaches. [4] Thus, there are many complex reasons why it may be difficult to retain otherwise qualified cybersecurity professionals. But with adequate support from executives, meaningful work, and contributions to the organization that are valued, cybersecurity professionals will thrive.

Section #2: Cybersecurity is a Matter of Economics

Robust cybersecurity measures require substantial investment in cybersecurity resources. Shoestring budgets typically cannot afford much. It is not uncommon for Chief Information Security Officers to be constrained by their budgetary limitations. However, having more money available to invest in cybersecurity can certainly make a difference. In other words, healthcare organizations that lack adequate funding for their cybersecurity programs will likely struggle to keep up with evolving threats. On the other hand, healthcare organizations that have adequate funding may be able to invest in solutions that are on the cutting edge. The answer to who wins in cyberspace is the party that has

---

[4] Heidrick & Struggles. "2023 Global Chief Information Security Officer Survey." 2023. https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2023-global-chief-information-security-officer-survey.pdf.

done more to prepare and has greater knowledge about the inner workings of systems, devices, and data. In essence, stronger cyber defense requires greater investment.

A. Cybersecurity Budgets are Improving

Fortunately, budgets are on the rise for many organizations compared to previous years. Most respondents to this year's survey indicated that their budgets increased (55.31%), and others reported that their budgets stayed the same (23.46%). A very small minority (2.79%) indicated that their budgets decreased. This is indeed a positive trend. Compared to an analysis of historical data from 2021 to 2022, more respondents are enjoying increased budgets. Historically, only a slight majority (51.57%) reported an increased budget for the 2021 to 2022 time period.

Figure 4: Changes to Cybersecurity Budget from 2022 to 2023
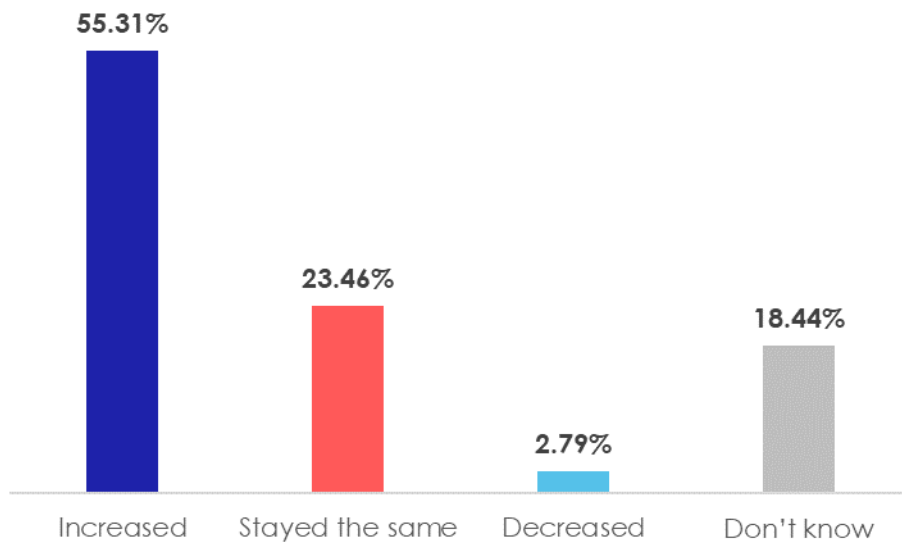
Traditionally, healthcare organizations have tended to spend 6 percent or less of the IT budget on cybersecurity needs based upon the aggregate data from the 2018 HIMSS Healthcare Cybersecurity Survey, 2019 HIMSS Healthcare Cybersecurity Survey, 2020 HIMSS Healthcare Cybersecurity Survey, and the 2021 HIMSS Healthcare Cybersecurity Survey.

Table 2: Percent of IT Budget Allocated to Cybersecurity 2018-2021

Budget Allocation	2018	2019	2020	2021
No money is spent on cybersecurity	3%	1%	1%	1%
1-2 percent	21%	9%	18%	18%
3-6 percent	21%	25%	24%	22%
7-10 percent	7%	11%	10%	15%
More than 10 percent	7%	10%	6%	11%
No specific carve out of cybersecurity within IT budget (but money is spent on cybersecurity)	27%	26%	23%	24%
Don't Know	15%	18%	18%	10%

The 2020 HIMSS Healthcare Cybersecurity Survey data was collected during the height of the COVID-19 pandemic. (The World Health Organization officially declared the COVID-19 pandemic several months prior on January 31, 2020.) Many clinicians, administrators, and others were working from home. Telework, and telemedicine became the norm, not the exception. Chief Information Security Officers at healthcare organizations had to change their strategy to keep up with this new decentralized and virtual way of working.

Fast forward several years to 2023, and the COVID-19 pandemic was officially over, according to the World Health Organization and other health authorities around the world, including the United States. However, many people are still teleworking, and telemedicine visits comprise a significant number of patient visits. Because of this changing environment, in addition to the increasing numbers of cyber-attacks on healthcare organizations generally, healthcare organizations have significantly increased their budgets as shown in the table below. Healthcare organizations are finally spending, on average, at least 7 percent or more on cybersecurity. This allocation is based on the overall information technology (IT) budget.

Figure 5: Percent of Organization's IT Budget Spent on Cybersecurity
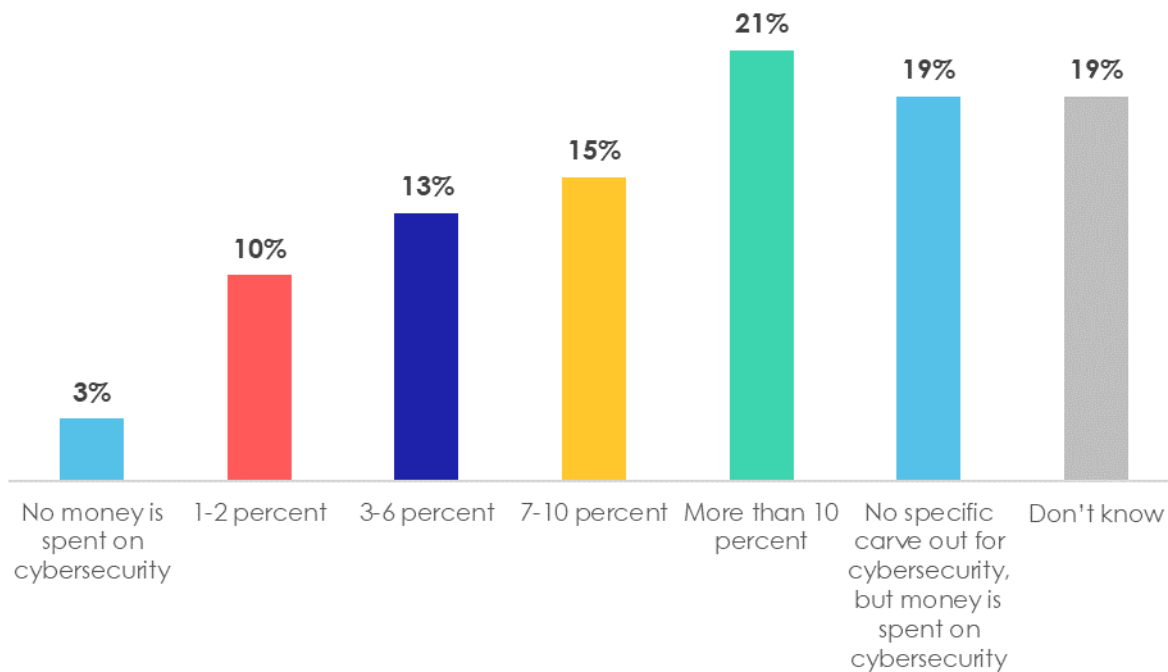
Cybersecurity expenditures are typically commensurate with the size of security teams, number of employees of the organization, and amount of annual revenue. Thus, it is likely that while organizations have generally experienced an increase in the available cybersecurity dollars, whether this is sufficient is yet another question entirely. Nonetheless, the positive increase in cybersecurity budgets for healthcare organizations of all types, including healthcare providers, consulting firms, and government entities, is a notably encouraging trend.

B. Cybersecurity Budgets Projected to Rise

Significantly, too, the increase in cybersecurity budget is expected to increase in 2024 with a majority of respondents (57.54%) anticipating this change. Only 17.32% of respondents expect that the budget will stay the same, and a very small minority (2.79%) are expecting a decrease in the cybersecurity budget.

Figure 6: Anticipated Changes to Cybersecurity Budget from 2023 to 2024
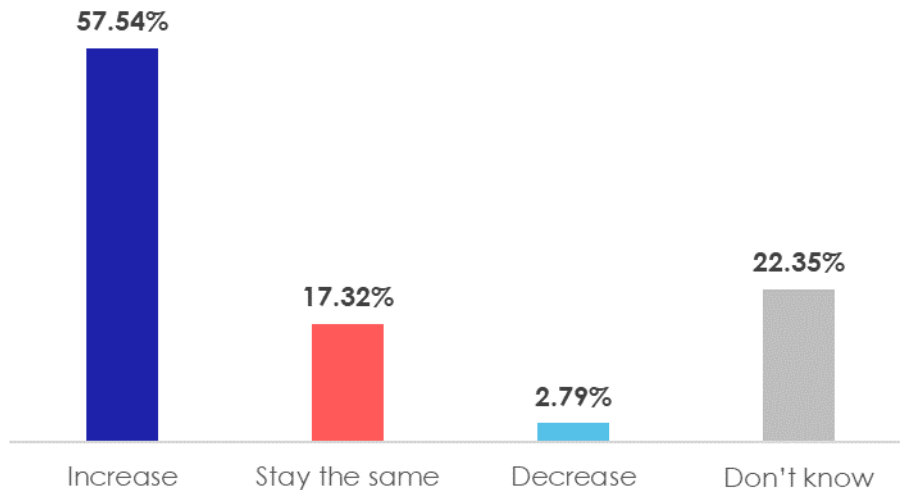
Section #3: Incidents

A. Most Significant Security Incidents

Incident detection is critical to every healthcare organization. The quicker an incident can be detected, the sooner the incident can be contained and eradicated. We asked survey respondents about how long it took the organization to detect its most significant security incident in the past 12 months.

Time to Detect the Most Significant Security Incident

It is important to note that about one third of respondents (32.31%) indicated that their organization did not experience any significant security incidents in the past 12 months, and 13.10% of respondents did not know whether there was a significant security incident. However, the majority of respondents (54.59%) reported that their organization experienced a significant security incident in the past 12 months.

For organizations that experienced a significant security incident in the past 12 months, almost half of the respondents (49.35%) indicated that it took them one week or less to detect the incident. Specifically, the top three responses were as follows: (1) within 24 hours (31.88%), (2) 24 to 48 hours (9.17%), and (3) less than one week (6.55%).

Table 3: Time to Detect Most Significant Security Incident

Amount of Time to Detect	Percent
Within 24 hours	31.88%
24-48 hours	9.17%
Less than 1 week	6.55%
1 week	1.75%
2 weeks	0.87%
3 weeks	0.87%
1 month	0.87%
2 months	1.31%
3 months	0.44%
More than 6 months	0.87%
Does not apply	32.31%
Don't know	13.10%

Materiality of Cybersecurity Incidents

Being able to determine the materiality of a cybersecurity incident is important in determining how an incident should be managed, mitigated, and contained. It may also impact whether and how certain stakeholders are notified, such as affected individuals, regulators, and/or the media.

Healthcare organizations are required to report breaches to the U.S. Department of Health and Human Services pursuant to the HIPAA Breach Notification Rule. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) also imposes new reporting requirements for covered entities that experience covered cyber incidents, namely, substantial cyber incidents that meet the definition and criteria as established by the director of U.S. Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) in the published CIRCIA final rule, which is expected to be published in early 2024. It is important to note that CISA will require any covered cyber incidents to be reported by covered entities within 72 hours from the time that the entity has a reasonable belief that the incident actually occurred. Ransom payments are required to be reported to CISA within 24 hours of making any such payments as a result of a ransomware attack.[5]

B. *Phishing as an Initial Point of Compromise*

It only takes one successful phishing attempt to cause a significant security incident. A successful phishing attack can lead to the leaking of sensitive, proprietary, or confidential information, a malware infection (such as ransomware), or other types of security

---

[5] Cybersecurity and Infrastructure Security Agency. "Cyber Incident Reporting Critical Infrastructure Act of 2022 (CIRCIA)." https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

compromises (e.g., manipulation of data, credential theft, business email compromise, breaches, and others).

A majority of respondents (58.52%) reported that general email phishing was the initial point of compromise of their organization's most significant security incident. This was followed by spear-phishing (31.44%) and SMS phishing (28.82%) as the top points of compromise.

Table 4: 2023 Security Incidents: Initial Points of Compromise

Points of Compromise	Percent
General email phishing	58.52%
Spear-phishing	31.44%
SMS phishing	28.82%
Phishing website	21.40%
Business e-mail compromise	20.52%
Malicious ad or pop-up	20.52%
Social media phishing	17.03%
Whaling	12.66%
Voice phishing/vishing	11.79%
Virtual private network (VPN) spoofing	7.42%
Pharming	6.99%
Don't know	5.24%
Watering hole attack	4.37%
Deepfake audio, video, or image	3.93%
Other (please specify)	2.18%
Does not apply – no significant security incidents during the past 12 months	24.02%

Spear-phishing involves the crafting of tailored messaging for specific targets. Large language models excel at tailoring messaging in various formats, including written and spoken language. Moreover, they possess the capability to seamlessly translate between languages, regardless of proficiency levels in the target language.[6] Large language models can be superior to other readily available language translation tools, not only in terms of grammar but also syntax and sentiment analysis. With minimal knowledge about a foreign language, threat actors can leverage large language models to refine translated text and produce convincing communications.

But threat actors are not just limited to the English language, as large language models can be leveraged to translate any number of languages. This opens up the world to the

---

[6] NBC News. "NSA official warns of hackers using AI to perfect their English in phishing schemes: NSA Cybersecurity Director Rob Joyce said the language used in hacking and phishing schemes was becoming more sophisticated and convincing."
https://www.nbcnews.com/tech/security/nsa-hacker-ai-bot-chat-chatgpt-bard-english-google-openai-rcna133086.

possibility of effective international phishing campaigns. If the tactics, techniques, and procedures are effective, there is little reason to change what works.

And yet the threat landscape changes with innovation. Artificial intelligence platforms, such as large language models, have multimodal capabilities that can understand and generate text, speech, images, and other content. Beneficial and malicious content can be created using these platforms. When used for malicious purposes, convincing fake content like deepfakes can be created. It is therefore very important to ensure that security awareness training is regularly updated to stay ahead of these evolving threats.

Security awareness training should include education about current phishing, smishing, and vishing techniques, as well as training on deepfake phishing. A recent trend in security awareness training is game application so that workforce members are more engaged in the training and retain the content better. Notwithstanding this, certain phishing techniques are relatively new, and exercises can be organically developed to keep pace with this changing threat landscape, especially with deepfakes and smishing.

Above all, it is important to ensure that the healthcare organization has a culture of encouraging robust internal information sharing at the appropriate levels. Therefore, it is a good idea to have an established protocol for sharing suspected phishing attempts with the security team. It is also beneficial for workforce members to see actual examples of phishing attempts, especially since some of these may be uniquely tailored to the organization. Actual intelligence is the best intelligence.

Additionally, with the rise of artificial intelligence in 2023 and the growing adoption of artificial intelligence in healthcare, more sophisticated attacks from all angles are occurring, especially smishing and other forms of phishing.[7] To help combat the rise in smishing, the Federal Communications Commission (FCC) released on February 23, 2023, an FCC Fact Sheet on "Targeting and Eliminating Unlawful Text Messages."[8] Around this time, a notable spike was observed across industries in terms of unwanted smishing messages. Further, the U.S. Department of Health and Human Services released a bulletin on August 10, 2023, with the title "Multi-Factor Authentication & Smishing."[9]

But with new trends, such as artificial intelligence, come new threats. Deepfake audio, video, and images have been increasingly circulated in the wild.[10] A few respondents

---

[7] U.S. Department of Health & Human Services. "Ransomware & Healthcare." January 18, 2024. https://www.hhs.gov/sites/default/files/ransomware-healthcare.pdf. U.S. Department of Health & Human Services. August 10, 2023. "Multi-Factor Authentication & Smishing."https://www.hhs.gov/sites/default/files/multi-factor-authentication-smishing.pdf.
[8] FCC. February 23, 2023. FCC Fact Sheet: Targeting and Eliminating Unlawful Text Messages. https://docs.fcc.gov/public/attachments/DOC-391239A1.pdf.
FCC. November 22, 2023. FCC Fact Sheet: Combatting Illegal Texas Messages. https://docs.fcc.gov/public/attachments/DOC-398661A1.pdf.
[9] U.S. Department of Health & Human Services. August 10, 2023. "Multi-Factor Authentication & Smishing." https://www.hhs.gov/sites/default/files/multi-factor-authentication-smishing.pdf.
[10] U.S. National Security Agency, Federal Bureau of Investigation, and Cybersecurity and Infrastructure Security Agency. Contextualizing Deepfake Threats to Organizations. https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF.

(3.93%) indicated that a deepfake was responsible for significant security incidents in the past 12 months at their healthcare organizations. However, the fact that deepfakes had led to a significant security incident is very concerning.

It is relatively easy to create an audio deepfake of someone's voice with just a few minutes of the individual speaking. Tools are readily available to do this, and it does not take much compute time, let alone computer resources. It is also fairly easy to create a convincing deepfake image. That said, deepfake videos are a bit more challenging to create, as there may be inconsistencies seen in the deepfake videos such as lighting, unusual body shape, or movements. It is anticipated that deepfakes will become much more sophisticated as computers are better equipped with more powerful processors (e.g., AI on a chip). Nonetheless, it is important to incorporate security awareness training and education around deepfake phishing, as these incidents will undoubtedly increase.[11]

Section #4: What's Happening with Ransomware

A. Present State

Ransomware attacks are often state-sponsored and highly organized and sophisticated. Since as early as 2018, healthcare organizations have been concerned about ransomware attacks.[12] 2023 was no exception, as the number of ransomware leak sites divulging sensitive information, such as patient information, have greatly increased. Hospitals, other healthcare organizations, and vendors have been the unfortunate victims of ransomware attacks in 2023. It is not just a problem for the healthcare sector, but a problem across all sectors and industries. But only a minority of respondents (11.79%) reported that their organizations experienced ransomware attacks. A strong majority (75.55%) reported that their organizations did not experience a ransomware attack. A minority of respondents (12.66%) did not have any knowledge one way or another. This general trend appears to be largely consistent with our data from the 2022 HIMSS Healthcare Cybersecurity Survey.

[11] https://crsreports.congress.gov/product/pdf/IF/IF11333.
[12] https://www.hhs.gov/sites/default/files/ransomware-healthcare.pdf.
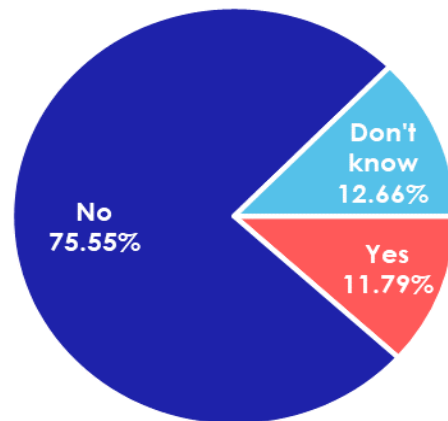
Figure 7: Experienced a Ransomware Attack in the Past Year

Table 5: Percent of Organizations Experiencing Ransomware Attack 2022 and 2023

Experienced Ransomware Attack	2022	2023
Yes	12.58%	11.79%
No	77.99%	75.55%
Unsure	9.43%	12.66%

When asked about the specific ransomware variants that ransomware victims in the healthcare sector fell prey to, several respondents indicated that they experienced the LockBit variant.[13] As part of a growing trend, ransomware attackers are leveraging Ransomware as a Service (RaaS) providers. LockBit is one prominent example of a RaaS provider (with over 2,000 victims) that was recently shut down by law enforcement.[14] Active ransomware variants include Cl0p[15], Blackbyte,[16] and Quantum[17] ransomware strains. Newly active ransomware variants targeting the healthcare sector include Blacksuit ransomware, for which there is currently no known ransomware decryptor.[18]

---

[13] TechRepublic. August 19, 2023. "Akamai report: LockBit, Cl0P expand ransomware efforts." TechRepublic. https://www.techrepublic.com/article/akamai-report-lockbit-cl0p-expand-ransomware-efforts/.

[14] U.S. Department of Justice. "U.S. and UK Disrupt LockBit Ransomware Variant." February 20, 2024. https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant. Internet Crime Complaint Center. "LockBit Victim Reporting Form." February 20, 2024. https://lockbitvictims.ic3.gov/.

[15] U.S. Department of Health & Human Services. "New Data Breaches from Cl0p and Lockbit Ransomware Groups." April 28, 2023. https://www.hhs.gov/sites/default/files/cl0p-lockbit-new-data-breaches-sector-alert.pdf.

[16] Microsoft Security Blog. July 6, 2023. "The five-day job: A BlackByte ransomware intrusion case study." Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2023/07/06/the-five-day-job-a-blackbyte-ransomware-intrusion-case-study/.

[17] Darktrace. October 6, 2022. "When Speedy Attacks Aren't Enough: Prolonging Quantum Ransomware." https://it.darktrace.com/blog/when-speedy-attacks-arent-enough-prolonging-quantum-ransomware.

[18] U.S. Department of Health & Human Services. November 6, 2023. "Blacksuit Ransomware." https://www.hhs.gov/sites/default/files/blacksuit-ransomware-analyst-note-tlpclear.pdf.

Of those that fell victim to ransomware in 2023, about one-quarter of respondents (25.93%) acknowledged that they paid ransom in response to the attack. On the other hand, a significant number (51.85%) did not pay the ransom. At least one respondent indicated, however, that their healthcare organization paid the ransom, but only after mitigation measures were implemented such as involving the services of a ransomware negotiator. This data is encouraging, as paying the ransom may embolden the threat actor to potentially victimize the healthcare organization again or target other healthcare organizations. To date, there are over 1,000 known ransomware variants that are in active circulation.[19]

In terms of recent developments, several ransomware decryptors have been recently released. Newly released ransomware decryptors include Blackcat and Black Basta ransomware.[20] The Babuk Tortilla ransomware decryptor was also recently released.[21] Additional decryptor tools may be found on reputable sites such as No More Ransom, which has hundreds of ransomware decryptors for specific ransomware variants.[22] It is also important to note that RagnarLocker was taken down in an international sweep in October 2023 by Europol.[23]

B. Future State

It is likely that ransomware attacks will continue to evolve and that we will see many more of them. Artificial intelligence and, in the future, quantum computing will significantly accelerate this trend. However, greater levels of information sharing will help to increase the resilience of the healthcare sector. Furthermore, the development of digital currency by central banks, including in the United States and elsewhere, may help to protect

---

[19] MalwareHunterTeam. "ID Ransomware." https://id-ransomware.malwarehunterteam.com/.
[20] U.S. Department of Justice. December 19, 2023. "Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant." https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.

However, the effectiveness of the Black Basta ransomware decryptor may be limited for newer attacks after December 2023.) Bleeping Computer. December 30, 2023. "New Black Basta Decryptor exploits ransomware flaw to recover files." https://www.bleepingcomputer.com/news/security/new-black-basta-decryptor-exploits-ransomware-flaw-to-recover-files/.

Other recently released ransomware decryptors include Akira - https://decoded.avast.io/threatresearch/decrypted-akira-ransomware/ and MortalKombat - https://www.bitdefender.com/blog/labs/bitdefender-releases-decryptor-for-mortalkombat-ransomware/.
[21] Talos Intelligence Blog. January 9, 2024. "New decryptor for Babuk Tortilla ransomware variant released." https://blog.talosintelligence.com/decryptor-babuk-tortilla/.
[22] No More Ransom. "Decryption Tools." https://www.nomoreransom.org/en/decryption-tools.html.
[23] Europol. October 20, 2023. "Ragnar Locker ransomware gang taken down in international police swoop." https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop.

against cybersecurity risks, safeguard sensitive information, and potentially minimize the risks of otherwise illicit financial transactions.[24]

Section #5: Artificial Intelligence Adoption in Healthcare

A. Allowing the Use of GenAI

Almost half of respondents (49.78%) indicated that their organizations allow the use of generative artificial intelligence (GenAI) technology, such as but not limited to ChatGPT. About one third of respondents' (34.50%) organizations do not allow GenAI at all.

Table 6: Percent of Organizations that Currently Allow the Use of GenAI Technology

Allow GenAI in Organization	Percent
Yes	49.78%
No	34.50%
Other	6.55%
Unsure	9.17%

However, it is anticipated that many more healthcare organizations will deploy generative artificial intelligence in their organizations in the future. This prediction is based on the increasing presence of artificial intelligence in technology, ranging from productivity software and operating systems to specialized AI chips.[25]

B. Acceptable Use Policy for GenAI

Surprisingly, only 40.71% of respondents whose organizations allow the use of GenAI technology indicated that they have an acceptable use policy for GenAI, while 52.21% respondents reported that their organizations did not. Thus, a majority of respondent organizations that are allowing the use of GenAI are seemingly not restricting how GenAI can be used. This lack of governance can significantly raise the potential for data leaks, among other things. Not only is this a risk regarding patient and financial information, but also confidential and/or proprietary information, such as intellectual property and other valuable intangible assets.

---

[24] The White House. September 16, 2022. "FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets."
[25] The following are examples of generative AI tools. Microsoft blog. September 21, 2023. "Announcing Microsoft Copilot, Your Everyday AI Companion." https://blogs.microsoft.com/blog/2023/09/21/announcing-microsoft-copilot-your-everyday-ai-companion.
Microsoft. "Discover the Power of AI with Copilot in Windows." https://www.microsoft.com/en-us/windows/copilot-ai-features.
Adobe. "Welcome to Generation AI." https://www.adobe.com/sensei/generative-ai.html.
Intel. Overcome Critical Performance, Scalability, and Cost Challenges. https://www.intel.com/content/www/us/en/artificial-intelligence/processors.html.

Figure 8: Allow the Use of GenAI Technology & Have Acceptable Use Policy
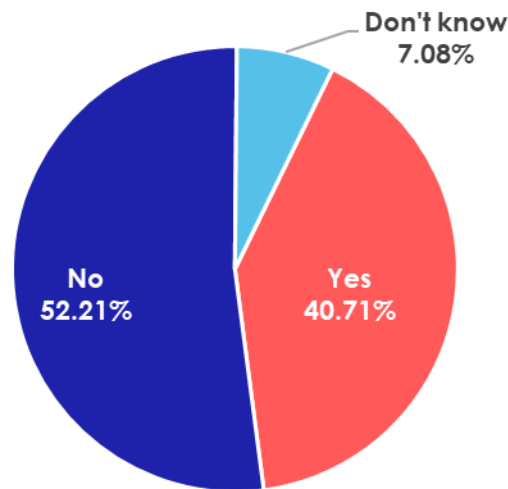
For example, GenAI can be leveraged by programmers, administrators, clinicians, finance professionals, and others. But workforce members still need to be educated on the safe and responsible use of GenAI, and one way of accomplishing this is with an acceptable use policy. Security awareness training can also be used to raise awareness about any applicable GenAI policies, as well as best practices for use of GenAI.

Notwithstanding this, GenAI is not yet at a state of maturity where the output can be completely relied upon. There is certainly a possibility that GenAI can make mistakes or otherwise provide false information. GenAI is not without risks. Thus, there is a need for all healthcare organizations to update their acceptable use policies in line with their position on the use of GenAI. Also, to the extent that GenAI is not allowed, it should be made clear in these policies.

C. GenAI Approval Process

Of those respondents that indicated that their healthcare organizations allow the use of GenAI, less than half of respondents (43.36%) reported that they have an approval process regarding GenAI technology. Additionally, 47.79% of respondents indicated that they had no approval process for GenAI technology at all. This lack of governance means that the organization may be exposed to significant risks. This can include potential leaks of information. Additionally, GenAI technology can be vulnerable to exploitation, just like any other software.

Table 7: Percent of Organizations that Have a GenAI Approval Process

Have GenAI Approval Process	Percent
Yes	43.36%
No	47.79%
Don't know	8.85 %

D. Actively Monitoring GenAI Usage

We asked all respondents about whether their organizations actively monitored GenAI usage. This question is critical for all organizations, regardless of their position on allowing the use of GenAI.

Organizations that do not allow GenAI at all want to ensure that no workforce member is using GenAI. These organizations are typically the ones that are more highly regulated or are more conservative in terms of risk posture.

For organizations that do allow the use of GenAI, actively monitoring GenAI usage gives organization insights into what is normal and abnormal activity regarding the use of GenAI, and specific user activity that may be prohibited or otherwise disallowed under applicable policies.

A majority of organizations are not actively monitoring GenAI technology usage (51.53%), while a minority of respondents (30.13%) are proactively monitoring GenAI usage.

Figure 9: Does Your Organization Actively Monitor GenAI Use
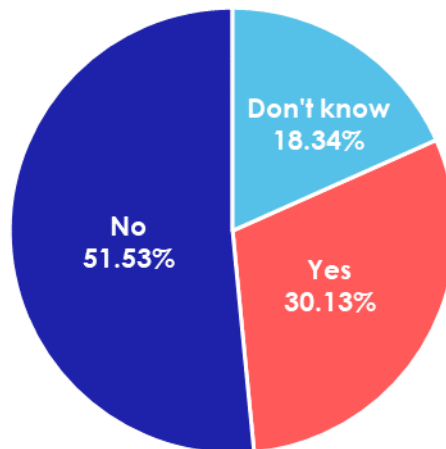
E. Concerns Regarding GenAI

Concerns regarding GenAI varied. However, data privacy (65.94%), data leaks (52.40%), data breaches (47.60%), intellectual property theft (43.67%), bias (47.60%), and patient

safety (51.97%) were top concerns. Deepfakes and other social engineering were also concerns (34.06%).

Figure 10: Concerns Regarding GenAI Technology

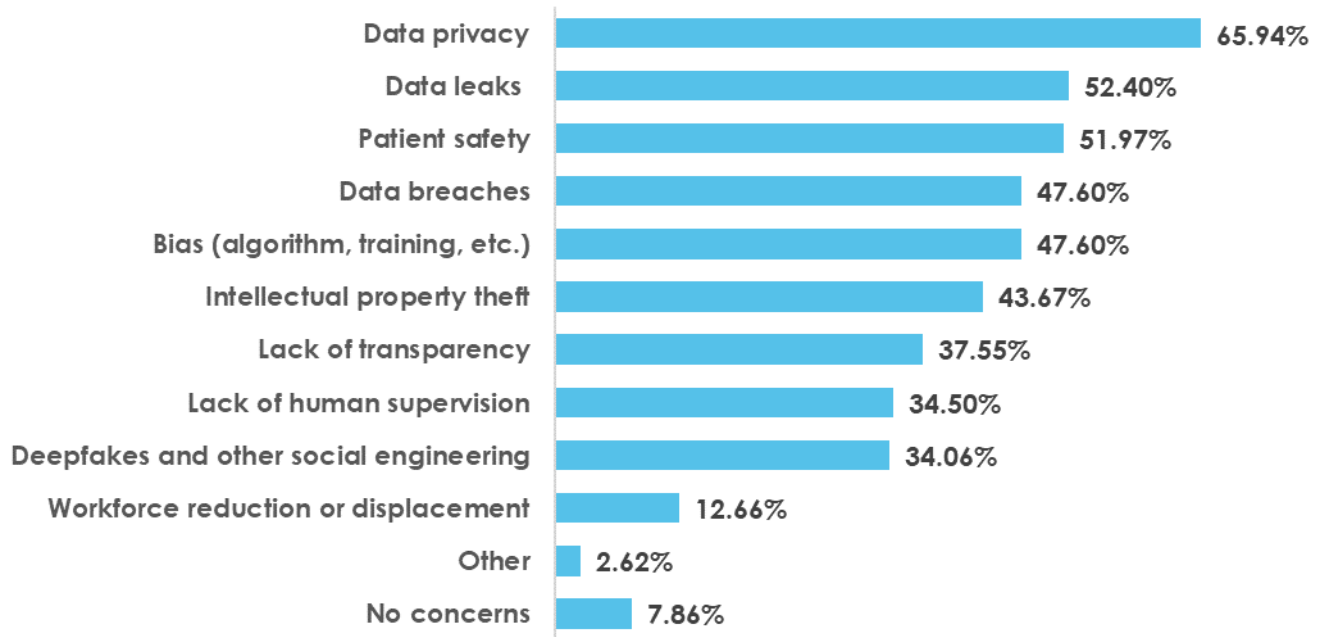| Concern	Percentage
Data privacy	65.94%
Data leaks	52.40%
Patient safety	51.97%
Data breaches	47.60%
Bias (algorithm, training, etc.)	47.60%
Intellectual property theft	43.67%
Lack of transparency	37.55%
Lack of human supervision	34.50%
Deepfakes and other social engineering	34.06%
Workforce reduction or displacement	12.66%
Other	2.62%
No concerns	7.86%

F. Future Use of GenAI

Respondents that indicated that their organizations did not currently allow GenAI reported that they likely will allow GenAI in the future (57.76%). A small minority of respondents (12.07%) indicated that they did not anticipate their organizations allowing GenAI in the future. But almost one-third of respondents were unsure (30.17%). It is highly likely that more healthcare organizations will eventually adopt GenAI since it is now featured in recently released operating systems, software, and embedded within hardware (e.g., AI on a chip), thereby making AI accessible to businesses and consumers alike in terms of their devices, operating systems, and other software.[26]

---

[26] Some examples can be found here.
NVIDIA. "NVIDIA Brings Generative AI to Millions, With Tensor Core GPUs, LLMs, Tools for RTX PCs and Workstations." https://nvidianews.nvidia.com/news/generative-ai-rtx-pcs-and-workstations.
Intel Corporation. " Intel Accelerates AI Everywhere with Launch of Powerful Next-Gen Products." https://www.intel.com/content/www/us/en/newsroom/news/ai-everywhere-core-ultra-5th-gen-xeon-news.html.
Google. "Google Tensor is a milestone for machine learning." https://blog.google/products/pixel/introducing-google-tensor/.
Ars Technica. December 21, 2023. "Apple Wants AI to Run Directly on Its Hardware Instead of in the Cloud." https://arstechnica.com/apple/2023/12/apple-wants-ai-to-run-directly-on-its-hardware-instead-of-in-the-cloud/.
Arm. " Arm is Powering Innovation through Artificial Intelligence." https://www.arm.com/markets/artificial-intelligence.
Microsoft. "Discover the power with Copilot in Windows." Microsoft, https://www.microsoft.com/en-us/windows/copilot-ai-features.

Table 8: Percent of Organizations That Do Not Currently Allow the Use of GenAI Technologies but Anticipate Allowing It in the Future

| Allow the Use of GenAI in the Future	Percent
Yes	57.76%
No	12.07%
Don't know	30.17 %

Section #6: Board of Directors Oversight

Boards of directors play a pivotal role in the success or failure of companies. Directors and an organization's officers are ultimately responsible for the acts and omissions of the company. Cybersecurity is now an integral part of business as all healthcare organizations need to safeguard the confidentiality, integrity, and availability of information.

Thus, boards of directors can significantly contribute to the company's culture in regard to cybersecurity adoption and enforcement. Boards of directors are also uniquely positioned to advise the company in regard to present and future risks.

A majority of respondents (61.57%) acknowledged that there is board oversight in regard to cybersecurity risks. The remainder of respondents (38.43%) indicated that their board of directors either did not have oversight of cybersecurity risks or that they were unaware of it.

Figure 11: Percent of Organizations Whose Board of Directors have Oversight of Cybersecurity Risk

61.57%
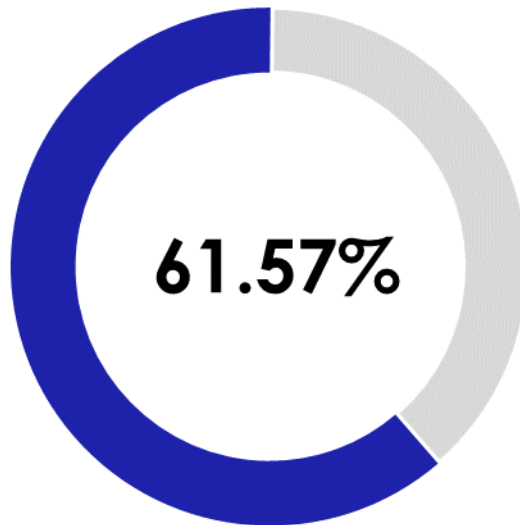
However, the Securities and Exchange Commission (SEC) adopted new cybersecurity disclosure rules for public companies that are subject to reporting requirements of the Securities Exchange Act of 1934. In accordance with these amendments, SEC registrants

Adobe. "Welcome to Generation AI." https://www.adobe.com/sensei/generative-ai.html.

must describe the board of directors' oversight of risks from cybersecurity threats, among other requirements. Accordingly, publicly traded healthcare organizations that are required to file annual 10-K reports must ensure that their board of directors has oversight of the cybersecurity program.

Some organizations are rethinking their governance, structure, and internal reporting mechanisms in light of anticipated new scrutiny over their cybersecurity processes, management, and oversight.[27]

But many healthcare organizations are not-for-profit entities. Nonetheless, having board oversight of the organization's cybersecurity posture, major cybersecurity events, and relevant progress are key components to flourishing in today's business and technical environment. Because cybersecurity is an integral part of business, cybersecurity should be a regular topic that is discussed at every board meeting.

Effective governance starts with effective oversight by the board of directors. Boards of directors need to be regularly briefed regarding cybersecurity risk as they cannot oversee what they do not know. While almost two thirds of respondents (67.69%) indicated that their board of directors are regularly briefed regarding cybersecurity risk, this number needs to be higher. Ideally, more healthcare organizations will embark upon the proactive journey of regularly briefing their boards of directors.

Figure 12: Percent of Organizations That Regularly Brief Its Board of Directors Regarding Cybersecurity Risk
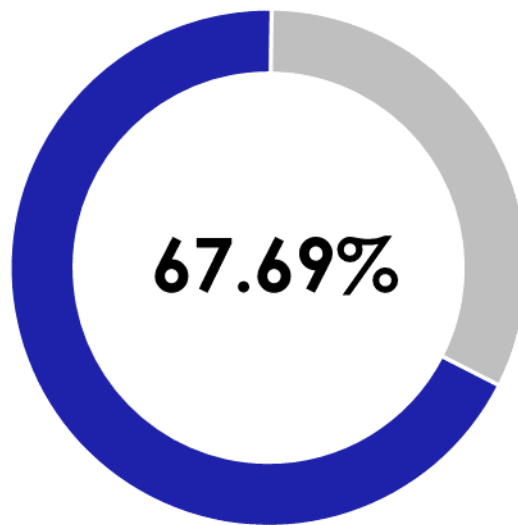
Even today, cybersecurity expertise on the board of directors is a scarce commodity. Therefore, the role of the Chief Information Security Officer, or executive designate, is to educate and inform the board regarding security awareness matters and actual

[27] U.S. Securities and Exchange Commission. "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure." https://www.sec.gov/corpfin/secg-cybersecurity.

intelligence about cybersecurity events that are happening to the organization and in industry. Boards of directors often want to understand how the organization stacks up against peers in industry as well. Furthermore, when there is a significant business transaction for development, such as the release of a new product or service or a potential merger or acquisition, cybersecurity should necessarily be a key consideration and point of discussion for the board.

Section #7: Future Directions

A. Artificial Intelligence, Quantum Computing, and Beyond

Artificial intelligence is on the rise. AI is being embedded in standard chips within personal computers, medical devices,[28] and mobile devices.[29] Similar to the integration of multifactor authentication at the hardware level of computers, it is likely that artificial intelligence will become a normal part of our everyday computing lives.

But artificial intelligence is not the only disruptor to bear in mind. Quantum computing is on the horizon. Parallel processing by leveraging the principles of quantum mechanics will greatly increase the power and speed of computers. One key concern of quantum computing is its ability to break encryption that we currently rely on, whether for data at rest, in transit, or in archival storage. Current public-key cryptography is vulnerable to quantum-based attacks. To this end, NIST has announced a new post quantum cryptographic standard. This new post-quantum cryptography standard for use in commercial products is expected to be released later in 2024.[30]

Healthcare organizations can be proactive by planning for a transition now. Specifically, healthcare organizations should be aware of which of its systems are vulnerable to quantum-based attacks and prioritize the systems that are mission-critical and/or those systems that have important or otherwise sensitive information. Healthcare organizations

---

[28]Some examples of AI-powered medical devices can be found here. NVIDIA. "AI-Powered Medical Devices." https://www.nvidia.com/en-us/industries/healthcare-life-sciences/medical-devices/. A listing of artificial intelligence and machine learning enabled medical devices published by the FDA may be found here. U.S. Food and Drug Administration. "Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices." FDA, https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-aiml-enabled-medical-devices.
Machine learning is a field within artificial intelligence that reflects the capability of a machine to emulate human intelligent behavior. MIT Sloan School of Management. April 21, 2021. "Machine Learning Explained."
[29] CNET. January 13, 2024. "AI at CES 2024: Take a Look at the Coolest Tech from the Show." https://www.cnet.com/pictures/coolest-ai-tech-ces-2024-weve-seen-so-far/15/.
[30] U.S. Cybersecurity and Infrastructure Security Agency. "Prepare for New Cryptographic Standard to Protect Against Future Quantum-Based Threats." CISA, 5 July 2022, https://www.cisa.gov/news-events/alerts/2022/07/05/prepare-new-cryptographic-standard-protect-against-future-quantum-based-threats.

also need to know which of its vendors and suppliers are implementing approved post-quantum resistant cryptography solutions.[31]

Virtually all organizations have vendors that they rely upon and place a degree of trust in their products and services. The healthcare industry became keenly aware of the need for robust mobile supply chain integrity and security with the COVID-19 pandemic.[32] Supply chain management is also relevant when thinking about the manufacturing, selling, distribution, and procurement of physical goods, such as personal computers, servers, devices, and equipment.

B. *Cybersecurity Supply Chain Will Become More Important*

Similar to physical products, knowing the origin of software components may be relevant in assessing quality control, safety, and reliability. As such, the software bill of materials (SBOM) can play a major role in cybersecurity supply chain security and integrity. The SBOM provides a listing of the individual components of the software. While typically this is not mandatory for private sector organizations, absent applicable legal requirements, it may be mandatory for public sector organizations. Having a detailed and up-to-date software components list can provide a good starting point for identifying potential vulnerabilities. Recent major cyber-attacks have highlighted the importance of a robust cybersecurity supply chain.

Less than half of respondents (41.92%) to this survey indicated that their organization has established a cybersecurity supply chain risk management program. The remainder of respondents (58.08%) indicated that they either did not have such a program or were unsure. The risk of not having a robust cybersecurity supply chain management program is that there may be too much dependency on one vendor or supplier.

[31] Virtual reality and the metaverse also present a set of new risks for healthcare organizations to contend with. The ability to rely on your senses or pick up on cues may be more challenging. World Economic Forum (WEF). June 28, 2023. "How to Protect Against Immersive Cybersecurity Threats in the Metaverse." https://www.weforum.org/agenda/2023/06/how-to-protect-against-immersive-cyber-security-threats-in-the-metaverse/.
It is anticipated that a combination of security awareness training and technical tools will help to mitigate these risks.
[32] PubMed Central. December 9, 2021. National Center for Biotechnology Information (NCBI). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8695796/.

Figure 13: Percent of Organizations That Have a Cybersecurity Supply Chain Risk Management Program

41.92%
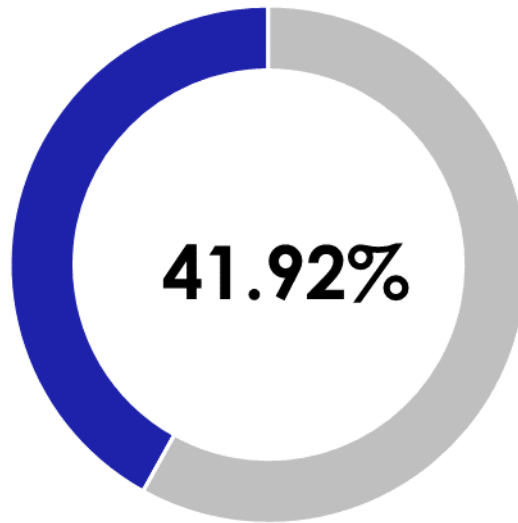
Additionally, if a key vendor supplier were to be compromised, a cascade of failures may result. This is why cyber-attacks that exploit widely used software components are often successful.

Healthcare organizations can enhance their cybersecurity supply chain management programs by having a greater diversity of suppliers and vendors and adopting relevant SBOM requirements. Incident response plans should also be updated to account for the various failures in disruptions that may result. Regular security assessments of vendors and suppliers also proved to be useful in assessing whether and if to move forward with them in terms of procurement and/or extending a multi-year agreement with them.

C. A Framework for the Present and Future

On February 12, 2013, the Obama administration issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." This executive order tasked NIST with developing a voluntary cybersecurity framework in order to reduce cybersecurity risks for critical infrastructure entities. After several public workshops, NIST developed a preliminary draft of the cybersecurity framework in 2013. Version 1.0 of the NIST Cybersecurity Framework was released on February 12, 2014. An update to this framework, NIST Cybersecurity Framework Version 1.1, was released on April 16, 2018, after input from industry.[33]

Since its inception, the NIST Cybersecurity Framework has been adopted by many organizations around the world, including in the healthcare sector. Indeed, the healthcare and public health sector is a recognized critical infrastructure sector.

---

[33] U.S. National Institute of Standards and Technology. "Framework Development Archive." https://www.nist.gov/cyberframework/framework/framework-development-archive.

The NIST Cybersecurity Framework is now a widely accepted cybersecurity framework. The NIST Cybersecurity Framework has been officially translated by the government of the United States into Arabic, French, Greek, Indonesian, Korean, Malay, Norwegian, Portuguese, and Ukrainian. Furthermore, the Information-Technology Promotion Agency of Japan (ITPA) has officially translated the framework into Japanese.[34]

The NIST Cybersecurity Framework Version 2.0 has a new core function: governance. The core functions are govern, identify, protect, detect, respond, and recover. Governance is the number one issue that all organizations grapple with. It necessarily determines the success or failure of any organization's cybersecurity program.

Slightly more than half of the respondents to the survey (51.53%) indicated that they plan to adopt NIST Cybersecurity Framework Version 2.0. The remainder of respondents (48.47%) either did not have any plans to adopt the framework or were unsure.

It is anticipated that more healthcare organizations will adopt the NIST Cybersecurity Framework Version 2.0. In this iteration of the framework, it has more granular guidance and implementation examples in terms of how to adopt and implement the framework. It also builds upon the essential work that was done for Version 1.1 of the NIST Cybersecurity Framework. One such example is the ransomware profile that is intended to be used with the framework.[35]

Another substantial update to the NIST Cybersecurity Framework Version 2.0 is the integration of cybersecurity supply chain risk management (C-SCRM) into all of the core functions of govern, identify, protect, detect, respond, and recover. This is closely tied to third-party fourth-party risk management.[36]

D. Cybersecurity Performance Goals

The U.S. Department of Health and Human Services recently released a set of voluntary cybersecurity performance goals (CPGs) for the healthcare and public health sector. These are voluntary goals that are based on DHS CISA's cross-sector cybersecurity performance goals that were released in 2022.[37] CISA's and HHS' CPGs are both aligned with the NIST Cybersecurity Framework.

The healthcare CPGs have two levels: essential goals and enhanced goals. Essential goals provide a solid foundation for all healthcare organizations. Enhanced goals are meant to

---

[34] U.S. National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.6.jpn.pdf.
[35] U.S. National Institute of Standards and Technology. "NIST 8374 - Ransomware Risk Management: A Cybersecurity Framework Profile." https://csrc.nist.gov/pubs/ir/8374/final.
[36] Fourth parties are the vendors or suppliers of the third parties that we do business with. For example, a vendor is a third-party organization. The vendor's supplier is a fourth-party organization.
[37] U.S. Department of Homeland Security. October 27, 2022. "DHS Announces New Cybersecurity Performance Goals for Critical Infrastructure." https://www.dhs.gov/news/2022/10/27/dhs-announces-new-cybersecurity-performance-goals-critical-infrastructure.
Cybersecurity and Infrastructure Security Agency. "Cross-Sector Cybersecurity Performance Goals." https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

build on the essential goals. The essential goals include the mitigation of known vulnerabilities; reducing risk from common email-based threats such as phishing; multifactor authentication; basic cybersecurity training; strong encryption; revoking credentials for departing workforce members; basic incident planning and preparedness; using unique credentials; separating user and privileged accounts; and vendor/supplier requirements regarding third party risks and mitigations. The enhanced goals include asset inventories; third-party vulnerability disclosures; third-party incident reporting; cybersecurity testing (which includes penetration testing and attack simulations); cybersecurity mitigation; detecting and responding to relevant threats and tactics, techniques, and procedures; network segmentation; centralized log collection; centralized incident planning and preparedness; and configuration management.

Above all, the healthcare CPGs are intended to address attack methods of threat actors that target the healthcare sector. Implementation of the healthcare CPGs will ultimately help improve cyber-preparedness and resiliency.[38]

Section #8: Resources

Technical

- CISA Bulletins[39]
- CISA Insider Threat Mitigation Guide[40]
- Health Care and Public Health Sector (HPH) Cybersecurity Performance Goals[41]
- HC3 Threat Briefs, Sector Alerts, and Analyst Notes[42]
- HHS 405(d) Program[43]
- Mitigation Guide: Health and Public Health Sector[44]
- NIST Cybersecurity Framework[45]

---

[38] States are also doing their part to increase cybersecurity preparedness and resilience. One example is the State of New York.
New York State - Office of Governor Kathy Hochul. "Governor Hochul Announces Proposed Cybersecurity Regulations for Hospitals Throughout New York State." https://www.governor.ny.gov/news/governor-hochul-announces-proposed-cybersecurity-regulations-hospitals-throughout-new-york.
New York State - Office of Governor Kathy Hochul. "Enhancing Cybersecurity in New York State." https://www.governor.ny.gov/programs/enhancing-cybersecurity-new-york-state.
[39] U.S. Cybersecurity and Infrastructure Security Agency. "Bulletins." https://www.cisa.gov/news-events/bulletins. https://www.cisa.gov/news-events/bulletins
[40] U.S. Cybersecurity and Infrastructure Security Agency. "Insider Threat Mitigation Guide. https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide.
[41] U.S. Department of Health & Human Services. "HPH Cybersecurity Performance Goals." https://hphcyber.hhs.gov/performance-goals.html.
[42] U.S. Department of Health & Human Services. "Health Sector Cybersecurity Coordination Center (HC3)." https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html.
[43] U.S. Department of Health & Human Services. "405(d) Program." https://405d.hhs.gov/.
[44] U.S. Cybersecurity and Infrastructure Security Agency. October 2023. "Healthcare and Public Health (HPH) Sector Mitigation Guide." https://www.cisa.gov/sites/default/files/2023-12/HPH-Sector-Mitigation-Guide-TLP-CLEAR._508c.pdf.
[45] U.S. National Institute of Standards and Technology. "Cybersecurity Framework." https://www.nist.gov/cyberframework.

- MITRE ATT&CK Framework[46]
- Internet Crime Complaint Center (IC3)[47]
- ID Ransomware[48]
- Stop Ransomware[49]
- No More Ransom[50]
- Abuse.ch[51]

Workforce

- NICE Framework[52]
- ISC2 2023 Cybersecurity Workforce Study[53]
- National Cybersecurity Alliance[54]
- Stop. Think. Connect.[55]

Organizations

- InfraGard[56]
- Health-ISAC[57]
- HITRUST Alliance[58]

---

[46] MITRE Corporation. "MITRE ATT&CK Framework." https://attack.mitre.org/.

[47] Internet Crime Complaint Center. "Internet Crime Complaint Center (IC3)." https://www.ic3.gov/.

[48] MalwareHunterTeam. "ID Ransomware." https://id-ransomware.malwarehunterteam.com/.

[49] U.S. Cybersecurity and Infrastructure Security Agency. "Stop Ransomware." https://www.cisa.gov/stopransomware.

[50] "No More Ransom Project." https://www.nomoreransom.org/en/index.html.

[51] Abuse.ch. "Fighting Malware and Botnets." https://abuse.ch/.

[52] U.S. National Institute of Standards and Technology. "NICE Framework Resource Center." https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center.

[53] ISC2. " ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce " 2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf.

[54] National Cyber Security Alliance. "Empowering a More Secure, Connected World." https://staysafeonline.org/.

[55] National Cyber Security Alliance. "Stop. Think. Connect." https://www.stopthinkconnect.org/.

[56] InfraGard. "InfraGard. " https://www.infragard.org/.

[57] Health Information Sharing and Analysis Center. "Health-ISAC." https://h-isac.org/.

[58] HITURST Alliance. "HITRUST." https://hitrustalliance.net/.

Conclusion

The findings of the **2023 HIMSS Healthcare Cybersecurity Survey** indicate that significant progress is being made to improve security posture among healthcare organizations. With roadmaps and guidance such as the NIST Cybersecurity Framework and the HPH Cybersecurity Performance Goals, the healthcare sector will realize even further improvement. The technological advances in artificial intelligence, quantum computing, and other areas such as 5G will help increase the capabilities of healthcare organizations for the ultimate benefit of their patients.

About HIMSS

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.

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 **2023 HIMSS Healthcare Cybersecurity Survey**.

How to Request Additional Information

Albe Zakes
Director of Public Relations and Corporate Communications
Marketing & Communications
HIMSS
350 N. Orleans St., Suite S10000
Chicago, IL 60654
albe.zakes@himss.org