2022 HIMSS Healthcare Cybersecurity Survey

HIMSS

2022 HIMSS Healthcare Cybersecurity Survey

Table of Contents

Overview

The **2022 HIMSS Healthcare Cybersecurity Survey** provides insight into the state of healthcare cybersecurity based upon the feedback from **159** cybersecurity professionals.

Workforce development:

- **Hiring challenges.** Recruiting and retention top the list.
- **Retention challenges.** Retention of qualified cybersecurity staff is a challenge.

Practical hands-on cybersecurity training:

- **More training.** Training needs to occur more regularly and frequently.
- **Greater inclusion.** Everyone needs to be trained, not just most.

Awareness training:

- **Phishing.** Phishing is pervasive, yet awareness training is not.
- **HIPAA.** Many, but not all, receive HIPAA training.
- **Security.** Most receive security awareness training, but not everyone.
- **Privacy.** Most receive privacy awareness training, but not everyone.
- **Breach & security incident reporting.** Common knowledge for some, but not all.
- **Insider threat.** Relatively few are aware of the insider threat.

Cybersecurity programs:

- **Barriers.** Top barriers are lack of people, budget, and inventory of data assets.

Authentication:

- **Multi-factor authentication.** Multi-factor authentication is not yet ubiquitous.
- **Usernames and passwords.** Many are still using usernames and passwords.

Cybersecurity budgets:

- **Increases in budget.** Some increases in budget are on the horizon.

Situational awareness:

- **Peer to peer.** Peer-to-peer information sharing occurs for some, but not most.

Ransomware:

- **Decline of attacks.** Fewer ransomware attacks targeting the healthcare sector.

Methodology and Demographics

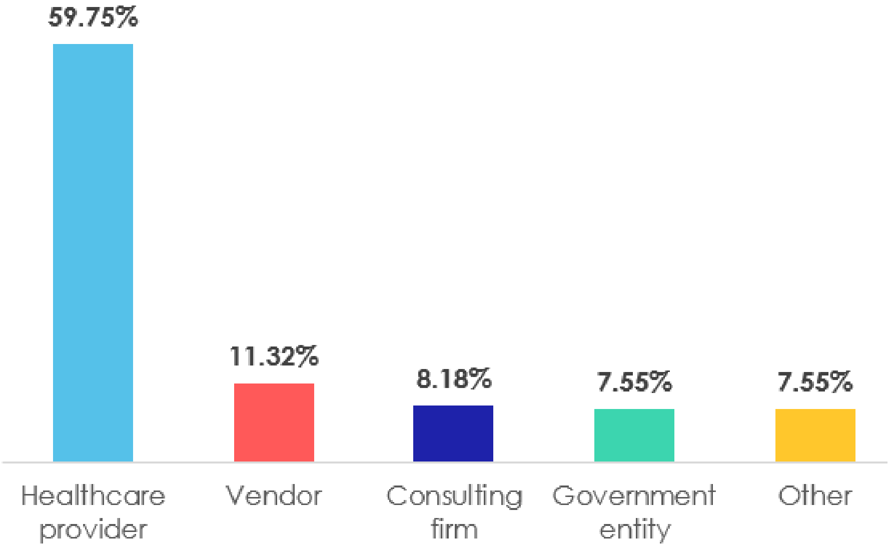
The **2022 HIMSS Healthcare Cybersecurity Survey** reflects the responses of **159** healthcare cybersecurity professionals. These professionals had at least some responsibility for day-to-day cybersecurity operations or oversight.

Most **respondents** (**67.30%**) had **primary responsibility** over the healthcare cybersecurity programs at their respective organizations. **Others** had at **least some responsibilit**y (**20.13%**) or sometimes **as needed** (**12.58%**).

Organization Profile:

Most respondents either worked for **healthcare provider organizations** (**59.75%**), **vendors** (**11.32%**), **consulting firms** (**8.18%**), and **government entities** (**7.55%**).

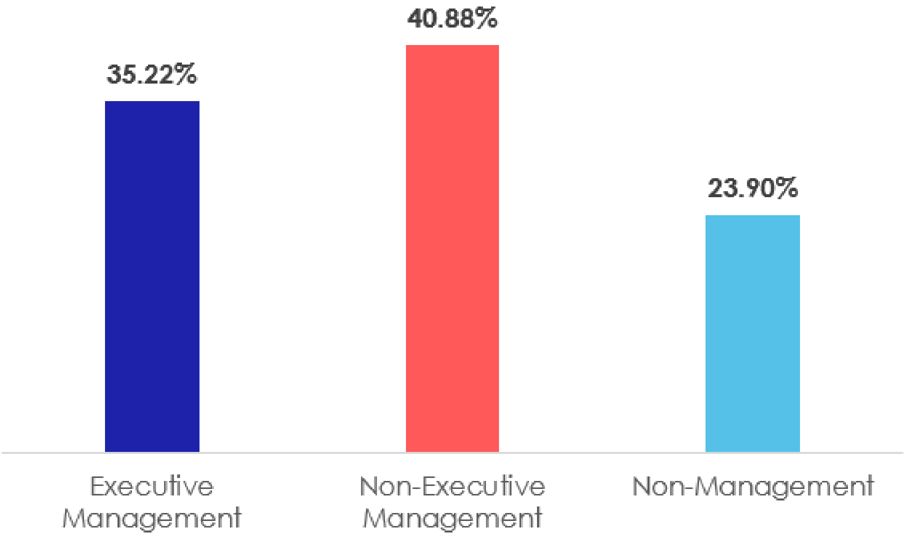
Figure 1: Organization Type



Professional Profile:

Respondents had roles in executive management (35.22%), non-executive management (40.88%), and non-management roles (23.90%).

Figure 2: Roles



Findings

Section #1: It's About the People

A. Workforce Challenges are the Norm

Traditionally, the focus of cybersecurity is on the technical front. But, ask any executive leader within an organization what the main challenge is and there is one common denominator: the people. Simply put, workforce challenges are the norm.

The shortage of cybersecurity talent is well-known.[1] Given the present state of cybersecurity defense, robust cybersecurity programs need qualified cybersecurity professionals. This is also true in the healthcare field where the number one barrier to achieving a robust cybersecurity program is the lack of cybersecurity staff, according to most respondents (61.01%).

As technical solutions, cybersecurity innovation overcomes present limitations in the state of the art. Yet, effective cybersecurity defense requires both strategy and tactical deployment. This, of course, requires adequate cybersecurity staffing and budgets.

[1] See (ISC)² Cybersecurity Workforce Study 2022 https://www.isc2.org/-/media/2A313135414E400FA0DBD364FD74961F.ashx.

Healthcare cybersecurity budgets are only a mere fraction of overall information technology (“IT”) budgets with only some healthcare organizations spending 10 percent or more of the IT budget on cybersecurity needs. Typically, healthcare organizations are spending 6 percent or less of the IT budget on cybersecurity needs based upon the aggregate data from the 2018 HIMSS Healthcare Cybersecurity Survey to the present time.

B. *Hiring is Difficult*

The top hiring challenges in the healthcare cybersecurity field include the following:

- Recruiting qualified cybersecurity staff (83.98%)
- Insufficient budget (54.72%)
- Lack of qualified candidates (45.28%)
- Non-competitive compensation (43.40%)

The most expensive line item of any organization’s budget is typically salaries. Organizations may not hire additional people, despite there being a need for additional staff, due to a lack of budget.

What should organizations do that lack the budget to hire additional cybersecurity staff? Hiring consultants or contractors may be a solution.

But, even if there might be some money to hire more staff, the question then turns to whether the appropriate (i.e., qualified) candidate with the right qualifications can be hired at a non-competitive rate. This is where outsourcing may be a solution. Hiring the right consultant or contractor may be appropriate, if it is feasible within economic constraints.

C. *Retention is Tough*

Yet another consideration is whether the qualified candidate will stay within the position, even when hired. Thus, retention of qualified candidates is also a significant challenge for many organizations (66.54%).

Indeed, cybersecurity staff tends to be precious commodities for healthcare organizations. Many respondents agreed that there is a lack of qualified candidates by the numbers (45.28%) as well as a lack of healthcare-related experience (38.99%) and cybersecurity-related experience (33.96%).

We all play a critical role in protecting patients. But a frequent misconception of those outside of healthcare is that healthcare data is just like any other type of data. But those of us within healthcare know that patient lives are on the line. Indeed, patient lives are in our hands and we are entrusted to care for them. Healthcare cybersecurity is unique because it requires a careful balance regarding the confidentiality, integrity, and availability of information. Access to the right information at the right time for the right patient is critical, especially in times of need.

Despite the unique nexus with patient safety, healthcare cybersecurity has much in common with cybersecurity in general. Some healthcare organizations successfully train cybersecurity professionals from within in order to address the healthcare cybersecurity professional shortage. Informaticists, clinicians, and others are examples of those individuals who now bridge the gap between cybersecurity and healthcare.

D. Cybersecurity Training is Infrequent

Cybersecurity training is essential for healthcare cybersecurity staff of all levels (whether beginning, intermediate, or advanced). Whether an individual is a recent graduate or certificate holder, there is a significant need to keep current. Healthcare organizations, as well as other industries, are under siege.

As mentioned previously, cybersecurity is not just a technical problem, but it is also a people problem. There is currently a patchwork of cybersecurity solutions on the market. With relatively lean budgets (often 6% or less of the IT budget), healthcare organizations must pick and choose which security solutions to procure.

With thousands of vendors on the market, choosing the right vendor for an organization can be overwhelming: governance risk and compliance, data security, network security, identity and access management, endpoint security, managed security service providers, application security, security operations, Internet of Things security, security analytics, fraud prevention, threat intelligence, email security, testing, training, and so on.

Cybersecurity education which is knowledge-based can be valuable. It is important to understand how and why things occur. But practical, hands-on training is what professionals in the healthcare sector (and any sector) desperately need. Practical, hands-on training may include cyber ranges, simulations, and capture the flag exercises.

According to an English translation of *The Art of War* by Sun Tzu: “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.”[2] This is why practical, hands-on cybersecurity training is important. It is equally important for an incident response team to understand what they are seeing and how to appropriately handle the incident.

The cyber threat landscape is changing by the day. New vulnerabilities are found and new exploits are continuously crafted. In an ideal world, we learn something new each day and yet time is the enemy. Most (61.01%) are finding that there is indeed a lack of time to do cybersecurity training. Thus, there is a missed opportunity (for some) to learn and keep current about what is happening today and a lack of understanding of what could happen tomorrow.

Interestingly, though, the economics associated with cybersecurity training is not a perceived barrier. Only some indicate barriers relating to cost, such as the employer does

[2] Sun Tzŭ, The Art of War (Lionel Giles, translator), https://www.gutenberg.org/files/132/132-h/132-h.htm.

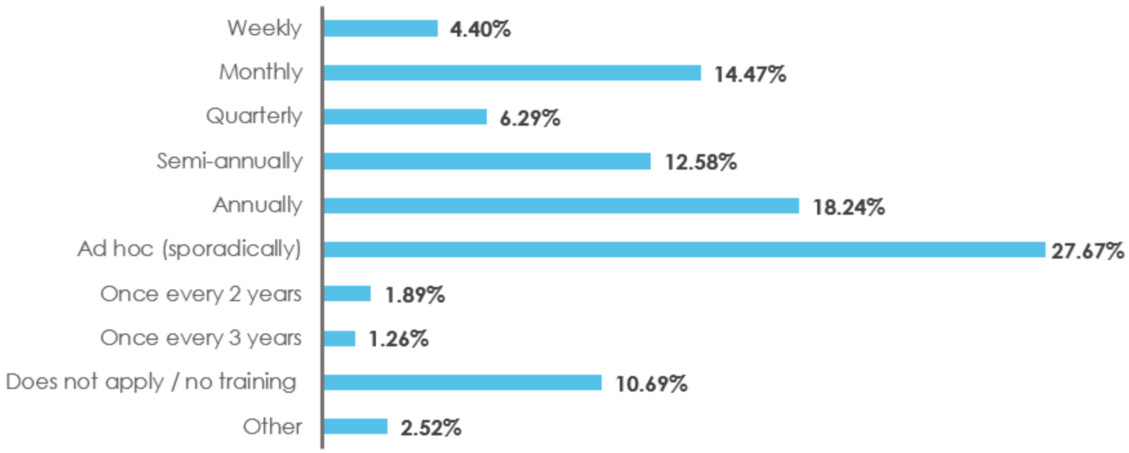
not pay for the training at all (22.64%) or some of the costs are subsidized by the employer but not all (20.13%). Thus, there is perceived value in cybersecurity training. For many, the value that they realize from cybersecurity training makes it worthwhile.

Table 1: Barriers to Receiving Practical/hands-on Cybersecurity Training from an External Cybersecurity Training Provider

Barriers	Percent
Lack of time to do the training	61.01%
Employer does not subsidize costs	22.64%
Employer subsidizes some costs, but not enough	20.13%
Lack of quality training	13.21%
Employer does not grant time off for training	6.29%

In terms of the cadence of cybersecurity training, one size does not fit all in the healthcare sector. Instead, some are partaking of cybersecurity training on an ad hoc, sporadic basis (27.67%), while others are doing it annually (18.24%), monthly (14.47%), or semi-annually (12.58%). (Consistent with this is our finding that developing the skills of current cybersecurity staff was deemed to be at least a moderate concern for most.) Only a slim minority (10.69%) are not receiving any cybersecurity training at all.

Figure 3: Frequency of Cybersecurity Training from an External Provider



The bottom line is that healthcare stakeholders need to increase the frequency of practical, hands-on cybersecurity training for cybersecurity staff. This will better enable them to defend their systems and assets against adversaries.

E. *Security Awareness Training Should Include Everyone*

Security awareness training is often given to information technology and cybersecurity staff. This is typical across all sectors, including in healthcare. But, the extent to which other stakeholders within an organization are involved in security awareness training can vary from organization to organization.

Yet, administrators, accounting staff, C-suite executives, communications/public relations staff, facilities management professionals, clinicians, and legal professionals are also frequently the target of phishing and other social engineering attacks. It is significant that many of these professionals are receiving cybersecurity training.

Even though it is a positive trend that many staff members are receiving security awareness training, we need to make every effort to ensure that we include everyone in our security awareness training programs. Otherwise, the risk can be high and we have done nothing proactive to mitigate that risk.

Although this is not the case at every healthcare organization, clinicians and legal staff are not necessarily included in security awareness training. Not including these critical stakeholders in security awareness training means that these professionals may be more vulnerable to phishing and other social engineering attacks. They may not be necessarily aware of who to contact in the event of a suspected security incident. A delay in incident reporting will result in delayed incident response and, thus, potentially more harm to the organization.

Table 2: Security Awareness Training Among All Staff

Staff Role	Received Training
Information technology staff	91.82%
Administrators	82.39%
Accounting staff	77.36%
C-suite executives	76.73%
Communications/public relations staff	73.58%
Facility management professionals	72.33%
Clinicians	69.18%
Legal staff	66.67%
Contractors	44.65%
Vendors	28.93%
Other	10.69%

F. Security Awareness Training Must Include Cybersecurity Staff

Phishing tends to be the primary way in which cyber adversaries get into our systems. Interestingly, only 89.31% of healthcare cybersecurity professionals are getting the training they need on how to detect and mitigate phishing. While we did not explore why this is the case, there are open-source tools and other free resources that can be leveraged to educate cybersecurity professionals and others on phishing. Without a doubt, healthcare organizations need to ensure that everyone is receiving security awareness training on phishing.

Another surprising trend is that only 83.02% of healthcare cybersecurity professionals are receiving training in regard to HIPAA compliance. This is very surprising since virtually all healthcare organizations in the United States are regulated by HIPAA and the HIPAA Security Rule is not new. This is another area in which all healthcare cybersecurity professionals should be receiving training.

Awareness training regarding data protection responsibilities is only taught to about 80% of healthcare cybersecurity professionals. But, it is important for healthcare cybersecurity professionals to understand how patient information and other sensitive information should be protected in light of privacy and cybersecurity concerns. Not providing training on data protection also increases risk for the organization. In the case of healthcare, patient lives are at stake and unmitigated risks such as these can potentially affect patient safety.

Ensuring that healthcare cybersecurity professionals are aware of social engineering tactics is also crucial, yet only 74.84% of healthcare cybersecurity professionals are receiving such training. This is very concerning as social engineering attacks are increasing (e.g., phishing, smishing, vishing, etc.). Additionally, the next frontier of social engineering is deepfake phishing. Deepfake phishing is more sophisticated and may involve the misappropriation of an individual's voice and/or likeness or it may involve a fictional individual (who does not exist at all – i.e., a synthetic identity). But, regardless of which social engineering tactic is used, we are more at risk than ever due to the increased reliance on virtual communications (compared to in person meetings, communication by telephone, etc.). Healthcare organizations need to train all staff (not just healthcare cybersecurity staff) on what social engineering attacks look like and how to report them.

But, perhaps most concerning is that only 46.54% of healthcare cybersecurity professionals are trained on insider threat detection and mitigation. This is alarming because insider threat is on the rise and it can be the most dangerous. Insider threat activity generally goes unnoticed for a significant amount of time before it is detected. Not having training on the insider threat means that it may go unnoticed for quite a lengthy period of time. Undetected and unmitigated insider threat activity essentially means that the risk to the organization is greatly increased. And, in the case of healthcare organizations, the patients may potentially suffer as a result.

Table 3: Types of Security Awareness Training Received

Type of Training	Percent
Phishing – how to detect/mitigate	89.31%
HIPAA compliance	83.02%
Data protection responsibilities – security of information	81.13%
Data protection responsibilities – privacy of information	79.87%
Social engineering – how to detect/mitigate	74.84%
Procedures for reporting a breach or other suspected security incident	73.58%
Insider threat – how to detect/mitigate	46.54%

G. Third-Party Vendors' Capabilities Augment the Cybersecurity Team

Whether due to a changing cyber threat landscape and environment (e.g., due to the COVID-19 pandemic) or because internal resources simply cannot keep up, more healthcare organizations are working with third party vendors to outsource their needs.

Perhaps due to the success of ethical hackers evangelizing the need for robust penetration testing, 66.67% of healthcare cybersecurity professionals' organizations are working with penetration testers. Interestingly, this is over and above other numbers such as the outsourcing of risk assessments and risk management (44.65%) and security audits (54.09%). In light of these findings, we recommend more healthcare organizations use third party vendors to assess and manage risk and conduct security audits. The reason is that a third party is neutral, whereas stakeholders within the same organization may paint a rosier picture about the cybersecurity posture or practices of the organization.

Table 4: Third Party Vendor Use

Type of Third-Party Services Used	Percent
Penetration testing	66.67%
Endpoint security	56.60%
Security audits	54.09%
Threat intelligence	50.94%
Risk assessments and risk management	44.65%
Cloud security	42.77%
Identity and access management	39.62%
Digital forensics (post-incident)	35.85%
Infrastructure security	33.96%
Incident response	32.70%
Application security	30.19%
Compliance	29.56%
Security operations	28.30%
Threat hunting	26.42%

Furthermore, while the utilization of third-party vendors for the following areas was relatively low, we urge healthcare organizations to consider retaining competent third-party vendors that can help them in these traditionally weak areas:

- Security operations (28.30%)
- Threat hunting (26.42%)
- Application security (30.19%)
- Cloud security (42.77%)
- Endpoint security (56.60%)
- Incident response (32.70%)
- Digital forensics (post-incident) (35.85%)

Healthcare organizations may not necessarily have the capabilities or budget to stand up a 24x7x365 security operations center. Thus, leadership at these organizations may wish to consider potentially outsourcing security operations. This may also include retaining a virtual chief information security officer (vCISO) to assist with cybersecurity planning and strategy.

Having a proactive security posture can include threat hunting (26.42%). While relatively few healthcare organizations are actively looking for threats that may have slipped pass traditional cybersecurity defenses, there are some entities that are innovating in their own way through constant exploration and the questioning of assumptions. Proactive threat hunting is a significant countermeasure to especially sophisticated cyber adversaries, such as nation-state and non-state sponsored actors and cybercriminals.

With new vulnerabilities discovered each day, it is understandable as to why some healthcare organizations (30.19%) are turning to application security vendors for help. There is no technology that is one-hundred percent secure. Additionally, our understanding of the vulnerabilities of today can be quite different from our understanding of the vulnerabilities of tomorrow. Thus, it is important to be cognizant of weaknesses in our applications and also have mitigations in place to address those weaknesses.

Without a doubt, more healthcare organizations have relied on cloud computing since the inception of the COVID-19 pandemic. But, even before that, many healthcare organizations were already using software as a service ("SaaS") solutions. Many electronic health record systems are SaaS and everyday things such as e-mail and productivity software are hosted in the cloud as well. As a result, it makes sense that more healthcare organizations (42.77%) are turning to cloud security vendors. Indeed, many cloud providers put the onus on the healthcare organizations to ensure that their data in the cloud is secure. Accordingly, healthcare organizations that do not wish to be in the headlines due to leaky cloud storage buckets are now retaining cloud security vendors to help mitigate the risk of cloud computing and exposing organizational data within the cloud computing environment.

On a positive note, more healthcare organizations (56.60%) are relying on third party vendors to improve their endpoint security. This is a sound approach, since the end user has trusted access and emails, web surfing, and other activities can unwittingly put the healthcare organization at risk.

Two areas that need improvement, though, are incident response (32.70%) and digital forensics (post-incident) (35.85%). It is likely that healthcare organizations are not responding to incidents as they should, whether in a timely enough manner or ensuring that the incident is quickly contained and eradicated or simply just understanding what they have and how best to respond to it. Thus, it is important for healthcare organizations to ensure that it has a vendor that specializes in incident response and digital forensics (post-incident) just in case it encounters an event that is unusual and is unsure how to respond to such an event.

Section #2: Challenges and Progress

A. Towards Robust Healthcare Cybersecurity

Achieving robust healthcare cybersecurity is a challenge for many organizations. A lack of people (60.01%) and a lack of budget (50.31%) tend to be the chief complaints. But, hiring more people or creating more complex organizational infrastructure does not necessarily solve things. On a related, equally important note, investing in the latest and greatest security solution may not be a panacea because there is no single universal solution that will solve all of the cybersecurity challenges.

Insufficient budgets negatively impact the ability to acquire new security solutions and security risk management processes, based upon the findings of our 2021 HIMSS Healthcare Cybersecurity Survey. Fortunately, though, most respondents to this survey indicated that their budgets were either increasing or at least remaining the same—both for 2021 to 2022 and 2022 to 2023.

Table 5: Changes to Cybersecurity Budget from 2021 to 2022

Cybersecurity Budget Change	Percent
Budget increase	51.57%
Budget remained the same	17.61%
Budget decrease	6.92%
Unsure	22.64%

Table 6: Changes to Cybersecurity Budget from 2022 to 2023

Cybersecurity Budget Change	Percent
Budget increase	47.17%
Budget remained the same	22.64%
Budget decrease	5.03%
Unsure	23.90%

How much money is enough for a healthcare cybersecurity budget? This answer can vary, but it is not unusual for healthcare organizations to have budgets that range from under $100,000, $500,000, $1,000,000 or $5,000,000 or more and it is anticipated that cybersecurity budgets will increase for most healthcare organizations. Of course, the magnitude of the budget does have some relevancy in terms of the security solutions that an organization can afford. But, more money does not necessarily mean that there will not be misconfigurations and other errors that may lead to an inevitable breach. It is a matter of when – not if.

But, regardless of the economic reality of the organization, all healthcare organizations bear the same responsibility: to protect patients and their sensitive information. How each healthcare organization accomplishes this depends upon the fiscal constraints and capabilities. In other words, some measures may be possible to implement for a large healthcare organization with a healthy cybersecurity budget whereas a critical access hospital may need to rely on less robust (but still adequate) security solutions and leverage things such as open-source software and tools.

As healthcare cybersecurity professionals, we are uniquely concerned about ensuring the confidentiality, integrity, and availability of information. While the confidentiality of patient information is very important, the information must – without a doubt – be reliable and also be available on demand whenever it is needed (but especially under exigent circumstances). A key tenet to keep in mind is that we can only protect what we know. In accordance with this tenet, it is surprising that less than half have a data inventory (44.65%) or data classification (38.36%) (e.g., PHI, PII, IP, etc.). The consequences of not having these things are enormous. But, they include significant risks to the organization such as, but not limited to, data leaks and weak or insufficient controls.

That is why we as healthcare cybersecurity professionals need to ensure that our knowledge and skills are kept up to date. A barrier to robust cybersecurity reported by some is the lack of specialized skills (37.74%). Cyber ranges, simulations, and other practical hands-on exercises are necessary to ensure that we are keeping up with the latest threats of today and tomorrow.

Table 7: Barriers to Achieving More Robust Cybersecurity

Barriers	Percent
Lack of cybersecurity staff (inadequate numbers)	61.01%
Lack of budget	50.31%
Lack of data inventory (knowing what kind of data we have & where)	44.65%
Lack of data classification (e.g., PHI, PII, IP, etc.)	38.36%
Lack of certain specialized skills for cybersecurity staff	37.74%
Lack of cooperation by people within the organization	31.45%
Policies and procedures do not reflect current practices	30.82%
Lack of awareness about policies and procedures	29.56%
Lack of executive buy-in	22.64%
Lack of interdisciplinary teams	21.38%
Lack of leadership	15.09%
Policies and procedures are difficult to understand	13.84%
Other	2.52%
None – no barriers are present	10.69%

B. Towards Robust Multi-Factor Authentication

Multi-factor authentication is one of the best ways to help ensure that the individual or entity that is accessing a system or resource is who he or she claims to be. Phishing-resistant multi-factor authentication (also called passwordless multi-factor authentication) is the gold standard for multi-factor authentication.[3] Yet only 9.43% of healthcare cybersecurity stakeholders are using passwordless multi-factor authentication. Further, there is a trend in the IT industry towards embracing passwordless multi-factor authentication and ditching passwords altogether.[4] Healthcare needs to adopt passwordless multi-factor authentication as too many compromises happen nowadays involving passwords with as many as 921 passwords compromised each second. [5] [6]

Healthcare stakeholders are now implementing multi-factor authentication across the enterprise. Most commonly, healthcare organizations have implemented multi-factor authentication with a password and an authenticator application (79.87%). But, the use of a password and SMS code for multi-factor authentication is used by 58.49% of healthcare stakeholders. This is closely followed by the use of usernames and passwords (57.23%).

Table 8: Type of Authentication Implemented

Authentication Type Implemented	Percent
Multi-factor authentication – Password + Authenticator app	79.87%
Multi-factor authentication - Password + SMS code	58.49%
Basic authentication - usernames and passwords	57.23%
Multi-factor authentication - Password + Phone Call (for receiving code)	35.22%
Multi-factor authentication – Password + Hardware token	34.59%
Multi-factor authentication – Password + Biometric factor	18.87%
Biometric authentication (single factor)	16.98%
Multi-factor authentication – Passwordless	9.43%
Other	4.40%

In 2016, only 39% of healthcare stakeholders were using multi-factor authentication.[7] Significant progress has been made since this time in adopting multi-factor authentication. Multi-factor authentication is typically more secure than basic authentication (i.e., usernames and passwords) – but only if the factors are kept secure. This is why the use of a password and an authenticator app is helpful – but because so many passwords have already been compromised and/or can be

[3] https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
[4] https://www.microsoft.com/en-us/security/blog/2022/05/05/this-world-password-day-consider-ditching-passwords-altogether/
[5] https://www.microsoft.com/en-us/security/blog/2022/05/05/this-world-password-day-consider-ditching-passwords-altogether/
[6] https://haveibeenpwned.com/
[7] https://www.himss.org/sites/hde/files/d7/081516_CybersecurityCheckup.pdf

cracked, we need to look at adopting more advanced technologies such as passwordless multi-factor authentication (PKI-based or FIDO-based).

C. More Information Sharing is Needed

In 2018, we asked healthcare organizations about their cyber threat intelligence sources. 68.6% of healthcare cybersecurity professionals shared cyber threat intelligence by word of mouth (i.e., peer to peer). This year, however, only 52.83% of healthcare cybersecurity professionals are sharing cyber threat indicators and mitigation information with their peers and 36.48% of healthcare cybersecurity professionals are not sharing any cyber threat intelligence/mitigation information at all with their peers.

Not sharing information about cyber threat intelligence and mitigation information with others in healthcare means that many healthcare stakeholders are not situationally aware. Entities such as HC3/HHS,[8] H-ISAC, Cyber Health Working Group, InfraGard, and others play a critical role in ensuring that healthcare stakeholders know what is happening to others in the sector. The advantage of information sharing is that the cyber threat intelligence and mitigation information is, in essence, crowdsourced. There is no reason why information sharing with peers should not happen, especially when these peers have been vetted and information is shared within a trusted community.

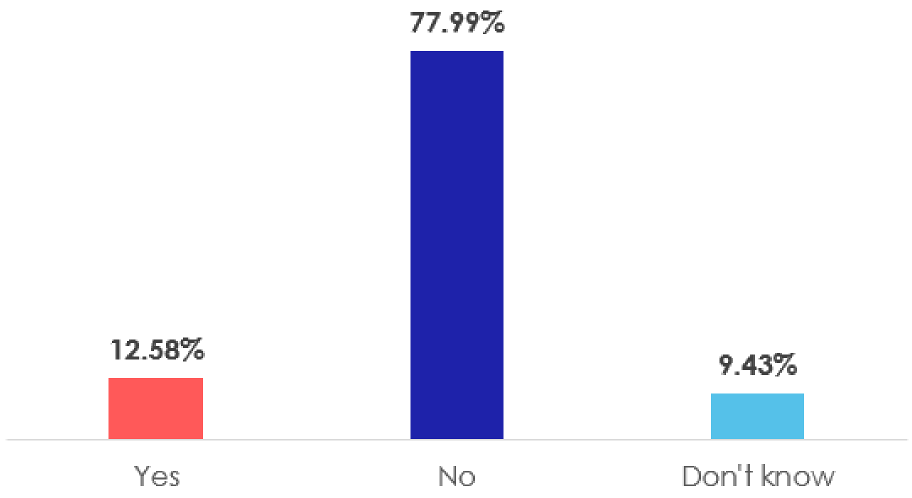
[8] https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

Section #3: What's Happening with Ransomware

A. Present State

Since at least 2018, healthcare organizations have been concerned about ransomware attacks. Across industries, however, U.S. officials and cybersecurity analysts report a drop in ransomware attacks as of 2022.[9] [10] Only 12.58% of healthcare stakeholders reported experiencing a ransomware attack in the past year and an overwhelming majority (77.99%) stated that their organizations did not experience a ransomware attack in the past year.

Figure 4: Ransomware Attack in the Past Year



[9] https://www.comparitech.com/ransomware-attack-map/
[10] https://www.wsj.com/articles/ransomware-attacks-decline-as-new-defenses-countermeasures-thwart-hackers-23b918a3

Some trends contributed to the decline in ransomware attacks:[11]

- Law enforcement's takedown of cybercriminals[12] [13]
- Office of Foreign Assets Control (OFAC) rules prohibiting the payment of sanctioned groups[14]
- Economic downturn of cryptocurrency[15]
- Fewer ransomware victims paying the ransom[16]

However, some healthcare organizations have been the target of ransomware attacks. Although not always, a ransomware attack may involve a public leak of the data (e.g., Cobalt Strike, Karakurt, LockBit 3.0), depending upon the tactics deployed by the ransomware gang. Furthermore, a ransomware attack may involve the encryption of data but this is not always the case. Some examples of ransomware attacks that have been reported involving the encryption of data include the following: Cobalt Strike, LockBit 3.0, and others.

Active ransomware strains that are currently impacting the healthcare sector include the following:

- BianLian[17]
- Blackcat & Royal[18]
- Cobalt Strike[19]
- LockBit 3.0[20]
- Karakurt[21]
- RansomHouse[22]
- Zeppelin[23]

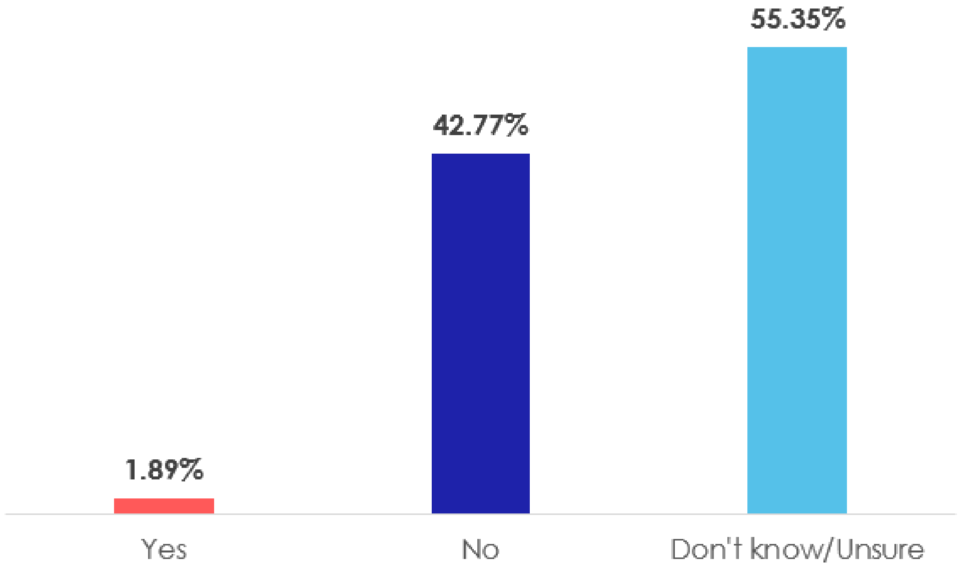
[11] https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf
[12] https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
[13] https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov
[14] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
[15] https://www.protocol.com/fintech/crypto-crash-ransomware
[16] https://www.zdnet.com/article/fewer-ransomware-victims-are-paying-up-but-theres-a-catch/
[17] https://decoded.avast.io/threatresearch/decrypted-bianlian-ransomware/
[18] https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf
[19] https://www.hhs.gov/sites/default/files/cobalt-strike-tlpwhite.pdf
[20] https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html
[21] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-152a
[22] https://www.healthcareitnews.com/news/roundup-royal-warning-ransom-house-strikes-and-doppelpaymer-assets-seized
[23] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-223a

B. *Future State*

Although there has been a recent dip in ransomware activity, it is likely that ransomware operators will change tactics and leverage social engineering and artificial intelligence to infiltrate healthcare organizations and other targets that are perceived to be of high value.[24]

Many healthcare cybersecurity leaders at healthcare organizations claim that their organizations would not pay the ransom in the event of a ransomware attack (42.77%). But others do not know whether their organizations would pay the ransom (55.35%). Only a few are certain that their healthcare organizations would pay the ransom (1.89%).

Figure 5: Willingness to Pay the Ransom (Ransomware Attack)



[24] https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=51f79b2219db

Section #4: Improving the Current State

Based upon the foregoing, it is clear that healthcare organizations need to implement proactive measures such as the following:

Workforce:

- More frequent, practical cybersecurity training for everyone
- Broader awareness training for everyone
- Hiring and retaining qualified cybersecurity professionals

Technical:

- Passwordless multi-factor authentication
- Robust incident response teams
- Digital forensics (post-incident)
- Third party vendors – leveraging third party expertise to reduce organizational risk
- Information sharing about threats and mitigations with peers
- Insider threat detection

In the future, artificial intelligence and language-learning models (LLMs) in particular will move us forward. New ways of working, thinking, and planning will be forged. Healthcare cybersecurity as we know it will undergo a profound revolution at a time of much needed change.

The economics of every organization is often a limitation in terms of what can be accomplished. But with more efficient ways of working and performing tasks, the economics of tomorrow will be vastly different from today. We will have more tools at our disposal. This will increase our sophistication and know-how – hopefully to a place where we can defeat cyber adversaries with greater ease and skill – while protecting our infrastructure, assets, and people.

Section #5: Resources

The following is a curated list of a few resources that may be helpful to your organization.

Technical

- CISA Bulletins[25]
- Internet Crime Complaint Center (IC3)[26]
- ID Ransomware[27]
- Stop Ransomware[28]
- No More Ransom[29]
- Abuse.ch[30]
- DNS Trails[31]
- Malpedia[32]

Workforce

- NICE Framework[33]
- (ISC)^2 2022 Cybersecurity Workforce Study[34]
- National Cybersecurity Alliance[35]
- Stop. Think. Connect.[36]

Organizations

- InfraGard[37]
- H-ISAC[38]
- HITRUST Alliance[39]

[25] https://www.cisa.gov/news-events/bulletins
[26] https://www.ic3.gov/
[27] https://id-ransomware.malwarehunterteam.com/
[28] https://www.cisa.gov/stopransomware
[29] https://www.nomoreransom.org/en/index.html
[30] https://abuse.ch/
[31] https://securitytrails.com/dns-trails
[32] https://malpedia.caad.fkie.fraunhofer.de/
[33] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
[34] https://www.isc2.org/Research/Workforce-Study
[35] https://staysafeonline.org/
[36] https://www.stopthinkconnect.org/
[37] https://www.infragard.org/
[38] https://h-isac.org/
[39] https://hitrustalliance.net/

Conclusion

The findings of the **2022 HIMSS Healthcare Cybersecurity Survey** suggest that healthcare organizations have made significant progress in improving their healthcare cybersecurity programs, but challenges still exist. These barriers to progress include security budgets, insufficient staff and training, and the growing volume of cyber-attacks and compromises. But perhaps the biggest vulnerability is the human factor. Healthcare organizations should do more to support healthcare cybersecurity professionals and their cybersecurity programs.

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 **2022 HIMSS Healthcare Cybersecurity Survey**.

How to Request Additional Information

Morgan Searles
Strategic Communications Manager
Marketing & Communications
HIMSS
350 N. Orleans St., Suite S10000
Chicago, IL 60654
312-915-9540
morgan.searles@himss.org