DHA ANALYTICS | CHIME Digital Health most wired Survey

SECURITY TREND REPORT

BEYOND TOOLS TO EFFECTIVE USE

SPONSORED BY

FIRST HEALTH ADVISORY

Digital Health Analytics (DHA) is a global market intelligence and survey research hub for digital health technology. Provided by the College of Healthcare Information Management Executives (CHIME), DHA was created in 2022 as the gateway for provider organizations and companies to better understand how digital technology supports leaders in transforming health and care and delivering data insights that help them make the greatest business impact possible.

The Digital Health Most Wired Survey and Security

In the tumultuous landscape of today's healthcare, the annual CHIME Digital Health Most Wired (DHMW) survey is a significant digital health "North Star" that healthcare organizations (HCOs) have relied upon for years. Widely known for the annual Most Wired recognition awards, the DHMW survey provides healthcare leaders a comprehensive profile of digital health usage among U.S. HCOs and a reliable resource to benchmark their own digital health progression.

Reflecting the digital profiles of approximately 40% of U.S. hospitals, the array of HCOs included in the 2023 DHMW survey can be characterized as representative of the U.S. Health System landscape. As such, the survey serves as a critical resource for helping researchers identify major themes and shifts in the HCO marketplace. For our current DHMW survey, the overarching theme can be characterized as **"The acceleration of data usage."**

In a digital health world shaped by Meaningful Use, HCOs have largely moved on from focusing on data captures and storage capabilities, to improving overall care outcomes. In this environment, leveraging data emerges as a critical activity in the realization of improved operational and clinical outcomes. The acceleration of data usage was evident in all eight sections of the survey, but especially pertinent to the Security section.

Also known as cybersecurity, information technology (IT) security measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization. In the context of accelerating data usage, IT Security plays a critical role in setting the pace to advance the use of data within the healthcare environment.

Table of Contents

4 Cybersecurity Leadership

5 Cybersecurity Governance

6 Cybersecurity Practices - Leveraging External Resources

8 Cybersecurity Practices - Internal Processes

10 Security Insurance

11 Conclusion

First Health Advisors: A Cybersecurity Leader

To help make sense of the Security findings in the 2023 DHMW survey and the cybersecurity market in general, CHIME sat down with leaders from First Health Advisory, an industry-leading digital health risk assurance firm. Using the 2023 DHMW survey as a starting point, we profiled findings from the survey around security leadership, governance, practices, and insurance before leaning on the insights of First Health leaders to provide context and clarity around the many complex issues HCO leaders must navigate to ensure their digital health tools operate within secure and reliable environments.

From this effort, we found that for HCOs to **accelerate data usage**, security must be a priority within the organizational digital health strategy and go beyond simply having the right security tools and processes to using them consistently and effectively.

Defining IT Security

IT security is the practice of protecting critical systems and sensitive information from unauthorized access, such as cyberattacks. As the number of devices and software applications connected to networks continues to grow within healthcare organizations, so does the potential for security incidents and subsequent liability. Security risks — caused by outdated medical devices, poor access management, or wide scope of user devices connected to healthcare networks — impacts information security and patient safety. Access management tools, encryption, and healthcare internet of things (IoT) security reporting tools are a few of the many solutions that can help organizations actively reduce and manage day-to-day risks.

Accounting for **~16%** of the overall DHMW total score, the Security section of the survey plays a consequential role in defining an HCO's digital health progression. In the context of CHIME's 2023 Digital Health Most Wired (DHMW) survey, an HCO's Security profile was adjudicated by assessing the following four factors:

1. Security Leadership
2. Security Governance
3. Security Practices (Leveraging External Resources; Internal Processes)
4. Security Insurance

"While few, if any, industries are exempt from cyber threats, healthcare is one of the most highly targeted industries today given the sheer amount of personal and sensitive information HCOs must traffic and store," said Lorren Pettit, CHIME's Vice President of Digital Health Analytics (DHA), on the weighting assigned to DHMW's Security section. "The simple fact is providers can't afford to go without critical care and other medical records at the ready. Accordingly, Our DHMW scoring algorithm reflects the importance cybersecurity practices and oversight play in adjudicating the digital health performance of HCOs."

Former CISO David Finn, Vice President, CHIME for Association for Executives in Healthcare Information Security (AEHIS), drove home the fact that security is a critical component to a modern healthcare provider: "I just don't even know how you talk digital health without security."

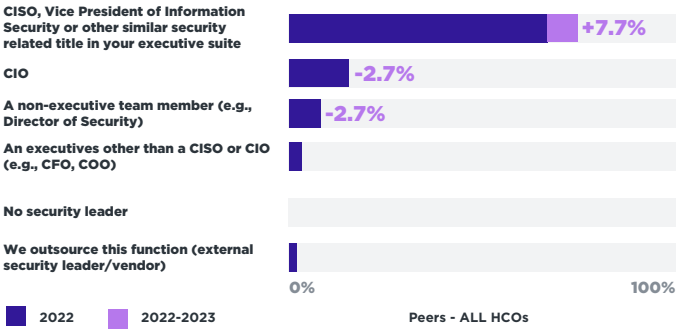
1 Cybersecurity Leadership

The first category considered in the Security section of the DHMW survey addresses cybersecurity leadership. A legacy question of the DHMW survey, provider participants are asked to identify who on their executive team is primarily responsible for leading information security within their organization.

As revealed in the following two graphics, most HCOs (67%) lean on a dedicated security leader (e.g., CISO) to guide their cybersecurity efforts. This is a position an increasing percentage of HCOs are adopting (up 8% over the 2022 DHMW survey). Yet, there are notable variances in the type of HCOs leveraging CISOs or similar. As evidenced in Chart 2, almost 90% of large HCOs (1,000 or more beds) have a CISO as opposed to smaller HCOs (<250 beds), where only about one-third have a CISO.

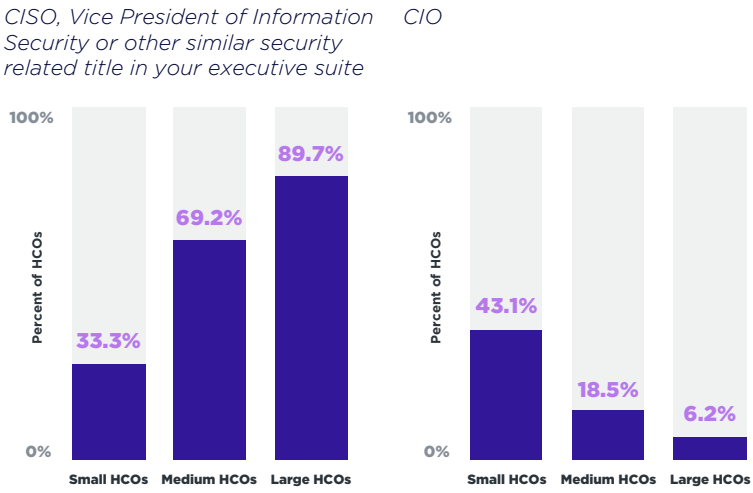
Question 9

Which on your executive team is primarily responsible for leading information security in your organization?



Question 9

Whom on your executive team is primarily responsible for leading information security in your organization?



Often in smaller organizations, the CISO is also the CIO, but this can create a conflict of interest, according to Finn. "The CIO's job is to keep the operations up and running, and the CISO's job is to secure and protect those data assets. There is conflict between those two roles, which creates even a more difficult situation for the small HCOs who don't have the cyber security expertise to start with and probably are in a budget crunch."

Under HIPAA, organizations are required to have a named security officer and privacy officer, which are often the same person in smaller organizations. Finn added that "They don't have to the have the CISO title, but they need to be designated for those roles."

Another wrinkle in the CISO position is oversight and accountability, according to Buddy Hickman, Chief Strategy Officer for First Health Advisory, who noted some organizations may have the CISO report to a compliance officer or legal officer. "Those individuals do not have the technical understanding that go along with the role of overseeing a CISO," Hickman said, noting that some CISOs in this situation are allowed to assess their own progress, potentially exposing the organization. "The compliance officers are wholly reliant on the CISO, for example, on the status and quality of an implementation. But it's the CIO who has the right knowledge to assess an implementation, so it them become crucial for these roles to work together for optimal outcomes."

It makes IT better to build the discipline and controls required for security into IT, Finn explained "The Healthcare Corporate Compliance Association (HCAA) has said there is a noticeable trend of organizations moving security out from compliance or regulatory." Likewise, Finn recommended the person writing the rules and controls for security should not be in IT, because it can create conflicts of interest.

"You can have leadership from wherever it needs to be, but there must be comprehensive governance. The two areas of healthcare where we don't see this enough are for security and data," Finn said.

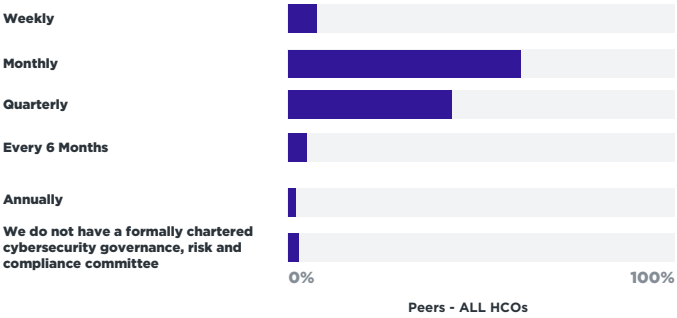
2 Cybersecurity Governance

Cybersecurity reports help to foster data-driven communication between boards, executives, security practitioners, and security and risk leaders to ensure that all parties are working together to enhance security programs and mitigate enterprise risk. Hence the second category of questions in the Security section of the DHMW survey focus on cybersecurity governance.

More specifically, survey participants were asked to report on the cadence of cybersecurity governance, risk and/or compliance meetings; formalized reports to varied HCO leaders; and specific security reports to the HCO's executive team.

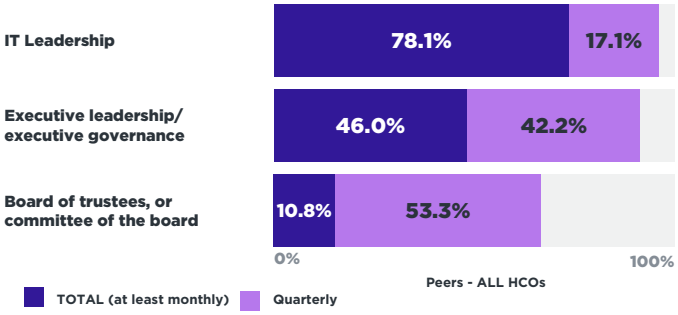
Question 10

How often does your organization's formally charted cybersecurity governance, risk and/or compliance committee meet?



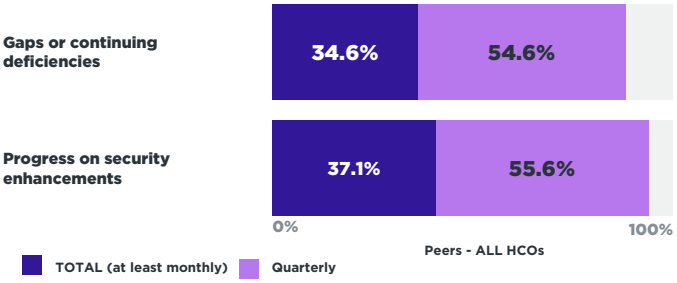
Question 11

How often do the following groups receive a formal report regarding your organization's information security efforts?



Question 12

How often are the results of the following reported to your organization's executive team?



The responses from HCOs revealed that most of them share cybersecurity information with their varied stakeholders at least once a quarter.

The frequency of cybersecurity reporting to governance groups varied on several factors, such as the size and complexity of the organization, the industry in which it operates, and relevant regulatory requirements.

HMW showed smaller HCOs provided security updates to their boards more frequently than larger organizations. "Smaller organizations are closer to their boards than larger organizations tend to be, so that makes it easier to more frequently talk to communicate with each other about cybersecurity and other important matters," Groome said.

The NIST Cybersecurity Framework (CSF), a voluntary set of standards, guidelines, and best practices for managing organizational risk, does not recommend a specific cadence of security reporting. It merely suggests that "organizations should communicate their cybersecurity risk management practices and performance to their governance bodies regularly." This communication should be tailored to the specific needs of the organization and its governance bodies.

More explicit in the CSF is the importance of a multilayered approach to cybersecurity, which Finn also recommended. In this method, HCOs establish multiple security controls to protect their systems and data. CSF is based on five core functions: Identify, Protect, Detect, Respond, and Recover. The layers recommended by CSF include:

- **Physical security** measures to protect physical assets, such as servers, data storage devices, and networks.
- **Network security** measures protect networks from unauthorized access, use, disclosure, disruption, modification, or destruction.
- **Application security** measures protect applications from vulnerabilities that could be exploited by attackers.
- **Host security** measures protect individual computers and devices from malware and other threats.

- **Data security** measures protect data from unauthorized access, use, disclosure, disruption, modification, or destruction.

Another governance quandary occurs when decision-making across the organization becomes isolated by different departments with teams who fail to collaborate on a regular basis. "HCOs recognize the need for governance around AI, digital health, IT, data, cybersecurity, and other areas," Hickman said. "These often end up as separate, siloed governance, when there is a natural interdependency there around digital health. HCOs need to look at breaking down those siloes and moving toward shared digital health governance."

3 Cybersecurity Practices - Leveraging External Resources

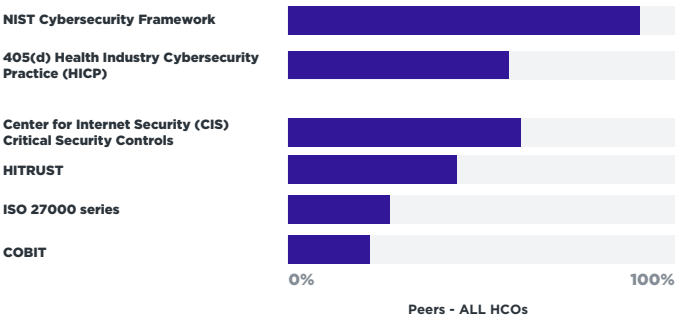
The third category of the Security section assesses the cybersecurity practices of HCOs, which were considered in two parts, the **leveraging of external resources and internal processes.**

With respect to the leveraging of external resources, survey participants were presented with three questions:

1. *Which information security frameworks are used to guide the HCO's information security program?*

Question 14

Which of the following information security frameworks does your organization use to guide your information security program?



Nearly all DHMW participants use the NIST CSF to guide cybersecurity efforts, with more than half also using 405(d) Health Industry Cybersecurity Practices (HICP), which is based partially on the NIST CSF but adds guidance specific to the unique cybersecurity risks facing healthcare.

HCOs should consider their accreditation when choosing a security framework to follow. "If you look at the cybersecurity standards laid out in the DNV commission, it points to 405(d) HICP, not to NIST CSF," Hickman advised, adding that he was a CIO who favored CSF. "But if you are paying attention to your accreditation, you've got to pay attention to 405(d)."

Section 405(d) of the Health Insurance Portability and Accountability Act (HIPAA) requires healthcare organizations to adopt and implement reasonable and appropriate security measures to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). HHS has issued guidance on how healthcare organizations can comply with this requirement but it's not mandatory.

Still, given the HIPAA requirement, Groome advised HCOs to give more serious consideration of 405(d) HICP as a pathway to compliance. Further, as state departments grapple with how to regulate cybersecurity, especially in healthcare, the fear is that they might each start to cobble together their own frameworks, Hickman warned.

"Instead of just codifying and existing framework like 405(d), they may pull from various frameworks, leaving different rules across different states," he explained.

HITRUST is also based on CSF and healthcare-specific standards and provides a comprehensive risk management framework and certification program specifically designed for the healthcare sector. Nearly half of DHMW organizations said they use HITRUST in some way.

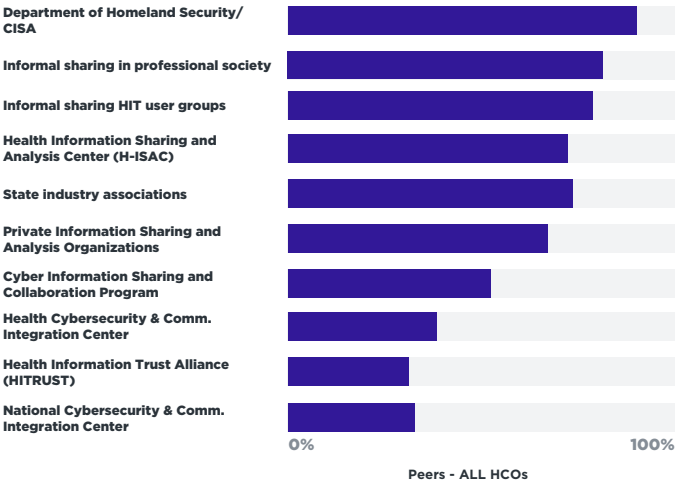
Due to the certification demands, Hickman noted that larger HCOs are the primary HITRUST customer. "For the costs incurred to be able to manage a high stress certification, most smaller and medium organizations can't afford it," he said.

As HITRUST is a paid certification program, it is much harder to adopt one or parts as is possible with voluntary frameworks like CSF or HICP, Groome noted.

2. *Which cybersecurity threat information sharing and analysis organizations does the HCO utilize?*

Question 10

How often does your organization's formally charted cybersecurity governance, risk and/or compliance committee meet?



The main takeaway from the DHMW data is that HCOs are leaning on an array of organizations to identify threats and vulnerabilities, which reflects what First health Advisory is seeing in the industry. "Everyone that we know, work with, and advise are using multiple streams in terms of information sharing," Groome confirmed.

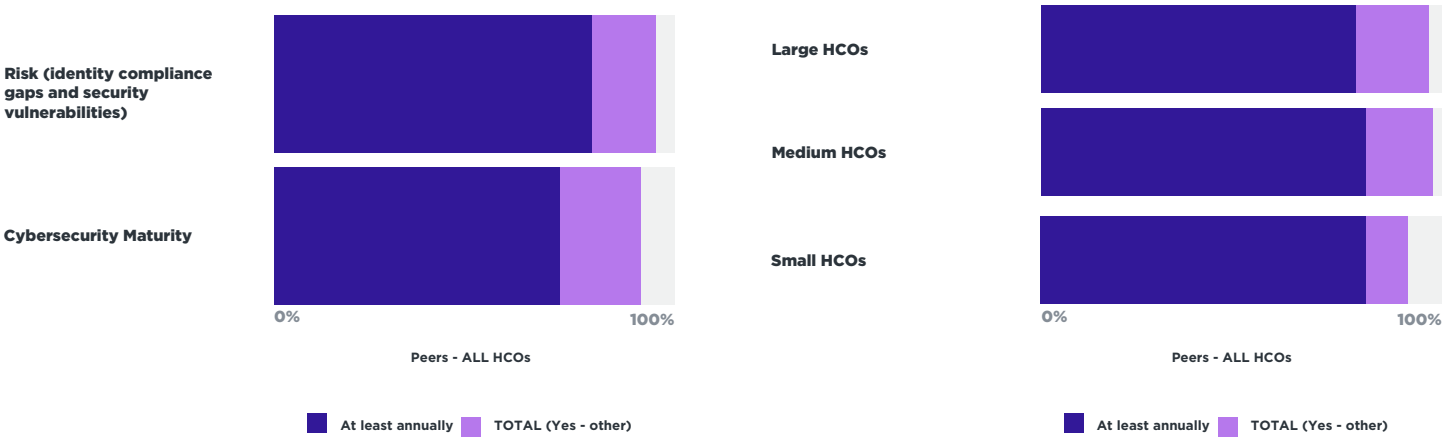
However, there's also a need for a better safe harbor for HCOs to share when they have a security incident. "I It's crippling our sector's ability to respond," Groome said. "I think this is why, as shown in the DHMW findings, organizations are turning to informal or private sharing opportunities."

HCOs should also consider sharing information with the FBI, which is highly motivated to forge relationships with HCOs, viewed as key assets in the community that need to be protected. "As a CIO, I had a strong relationship with my local FBI field office, and I knew many other CIOs did as well," he said, adding that the FBI wants to be proactive, to visit and talk to researchers and leadership. "If you are in the middle of a security event, you can send them information they will process through their own security operations center (SOC) to give you careful advice. They can be a big asset."

3. *Does the HCO use a 3rd party to conduct key security assessments?*

Question 17

Does your organization use the services of a 3rd party to conduct the following assessments?



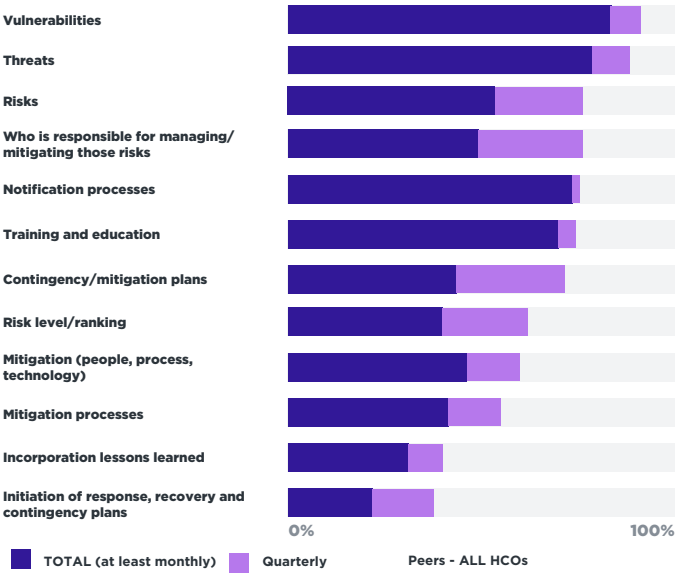
4 Cybersecurity Practices – Internal Processes

The second type of security practice considered in the DHMW survey focuses on specific processes HCOs implement to ensure the safety of their organization's data. Petitte explained that the emphasis here is on — not just having the capability to review and update programs -- but doing so on a regular basis.

Among the internal processes, DHMW looked at the *cadence by which select components of the HCO's risk management program are reviewed/updated,* and the *cadence by which select security practices are conducted.*

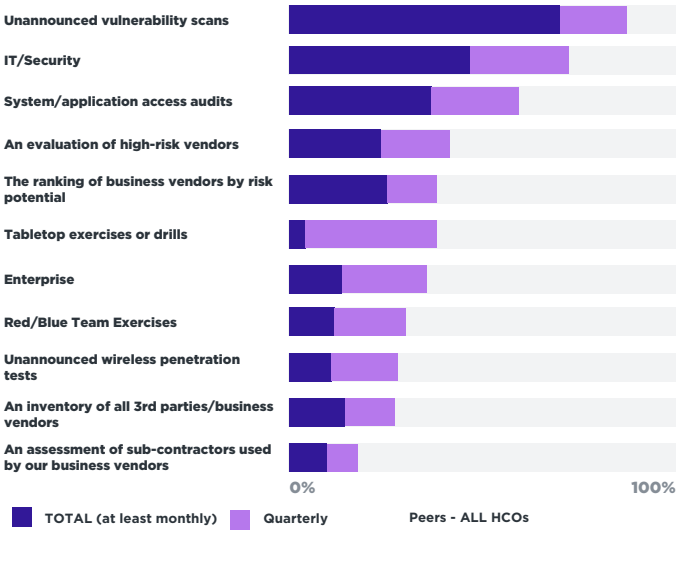
Question 13

How often are the following components of your risk management program reviewed and/or updated?



Question 16

How often does your organization conduct each of the following?

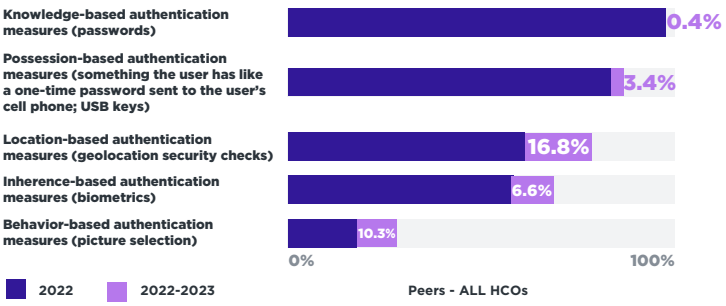


When prioritizing programs and determining cadence, HCOs should consider how these programs align with their security frameworks, suggested Hickman: "If you look at the threats outlined in HICP, for example, which programs mitigate these threats?"

One of the most common entry points into an organization by cybercriminals is via users and their devices. As such, authenticating users and devices is top priority for HCOs, and multifactor authentication (MFA) is the most recommended approach.

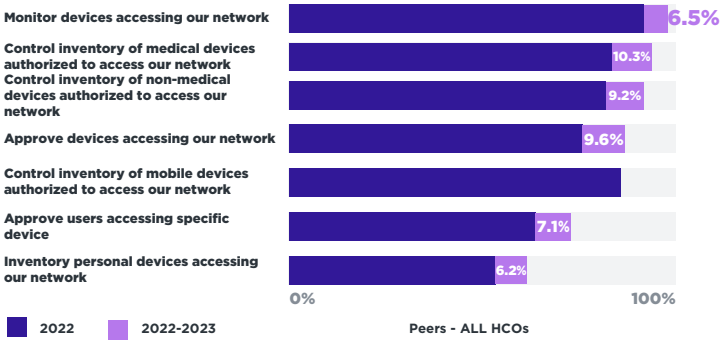
Question 18

Which of the following types of security authentication measures does your organization currently use to authenticate/manage authorized users?



Question 19

Which of the following security controls does your organization currently use to authenticate/manage devices accessing your network?



Nearly all DHMW organizations use *knowledge-based authentication measures* like passwords to identify users, but there was significant year-over-year (YOY) growth in usage of other types of authentication measures that are often used as additional factors, including *location-based authentication*, such as geolocation security checks (17% rise YOY), *inherence-based authentication* like biometrics (6.6%), and *behavioral-based authentication* like picture selection (10/3%).

Hickman expressed hope that moving forward, HCOs will increasingly use higher-level authentication including MFA, and rely less on passwords. Groome agreed, "We'll see this MFA use grow in healthcare as it follows the broader cybersecurity sector trend."

But MFA needs to be used appropriately, Finn added, as a caveat. "For example, an HCO might have MFA applied to its EMR but not on its email system," he suggested. "As far as I know, there has not been a direct attack on an EMR database. However, email is the number one direct attack point, and now adversaries can spoof email."

HCOs must deal with a sharply increasing number of patient and staff devices accessing the enterprise network and databases. The already high use of device monitoring and inventory methods among DHMW organizations saw solid YOY growth, with the lowest usage for *inventory of personal devices accessing the organizations' networks*, which rose 6.2 percentage points in 2023 to almost 60% adoption.

It may benefit HCOs, Groome said, to look at the challenge of managing these devices or assets holistically. "You may have an inventory or a tool/platform/technology to get that inventory, but then what are you doing with that inventory? How are you integrating that information?" he posited. "For some HCOs, it becomes too complex, and they may give up."

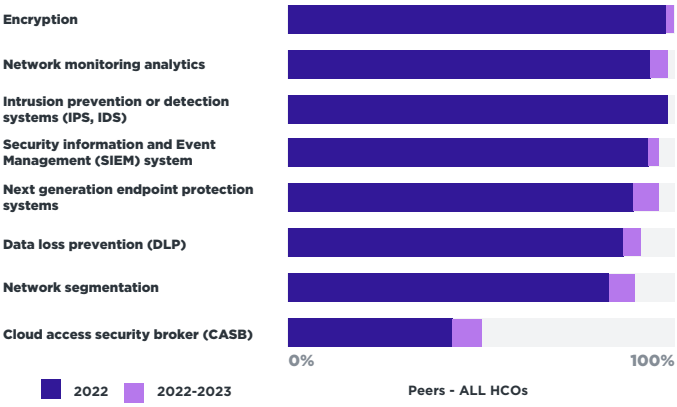
Hickman added that asset management converges with network controls, intelligent discovery tools and several other aspects to arrive at this holistic approach.

Petitte punctuated the challenge to HCOs: "It's a really complex issue that organizations really need to get a handle on and come up with a robust strategy."

A part of this security toolbelt are various methods of safeguarding data and information. Nearly all 2023 DHMW HCOs (>90%) reported the capabilities including *encryption, network monitoring and analytics, intrusion prevention and detection systems* (IPS, IDS), *data loss prevention* (DLP), and *network segmentation*.

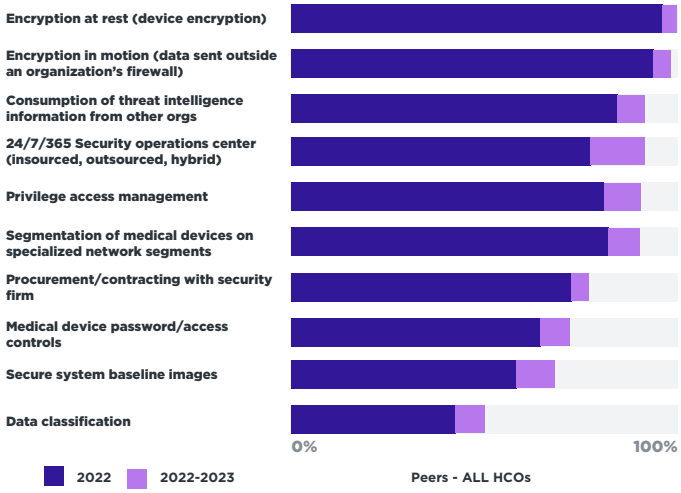
Question 20

Which of the following capabilities has your organization implemented and used as part of your organization's security processes?



Question 21

Which of the following security processes does your organization currently use to safeguard information?



With such tools and capabilities, the devil is in the details. "Every organization is doing some form of network segmentation at the VLAN level," Hickman said. "But micro-segmentation is another level — it's identifying certain device types that have known vulnerability of risk and segregating them from the rest of the traffic to limit any negative impacts from these risky devices." Likewise, there are many different methods of encryption that might be useful, depending on the exact needs or goals outlined in an organization's strategy.

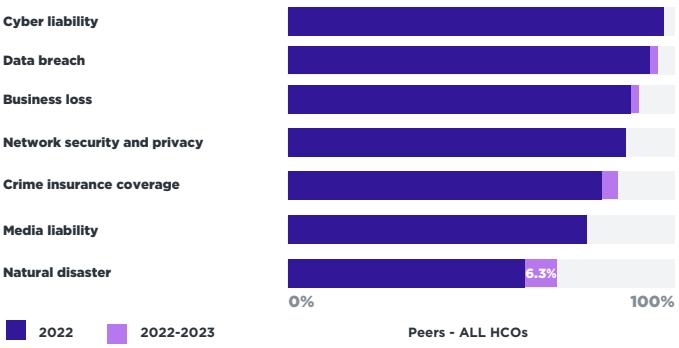
5 Security Insurance

The final area considered in the Security section of the DHMW survey concerns insurance coverage. Given the targeting of HCOs by bad actors and the costs associated with recovering from an attack, cybersecurity insurance constitutes a valuable data point to consider in assessing the digital health of an HCO.

In the 2023 DHMW survey, participants were asked to identify the varied cybersecurity related coverages of their HCO.

Question 19

Which of the following cybersecurity related insurance coverages does your organization currently carry?



Historically, organizations could purchase a blanket cybersecurity insurance policy but, over time, policies have been separated into different elements, Hickman noted. Now, policies cover the many items listed in the above DHMW graph, including *cyber liability*, *data breach*, and *business loss*.

According to the data, most HCOs (>80%) have coverage for all of these, except for natural disasters — about 70% of HCOs have this coverage, up 6.3 percentage points from the 2022 survey.

One contributing factor is that, as cybersecurity demands in healthcare become more complex, the premiums are adjusted to reflect the landscape. These costs may also go up as the number and scope of cybersecurity incidents rise in this market.

The increase in natural disaster coverage may be a direct impact from the recent pandemic, as well as environmental concerns, Petitte noted. "As we move further into climate change and see more extreme weather events that impact healthcare either regionally, nationally, or globally, we expect to see natural disaster coverage become more universal among HCOs."

Another insurance consideration related to cybersecurity is protection against class action lawsuits, Groome suggested. "We've seen a huge increase in the past two to three years of HCOs facing multiple class action suits after a ransomware incident. Research shows a mid-size hospital can expect an average of 10 class-action lawsuits following ransomware attacks, which often leads to the access and exposure of valuable information and data, including patient information."

6 Conclusion

Along the digital transformation journey, healthcare delivery has become complicated by a flood of data from a growing number of sources and the expansion of care beyond hospital walls. Likewise, cybersecurity and the cyberthreats against healthcare have become more sophisticated. HCOs need to respond in kind by baking security into digital health strategy and governance and by using all the available solutions and resources.

The data and tools are available, Groome said, and HCOs have an opportunity to act upon the resources and information to prioritize risk reduction in the environment of care. "Everybody in healthcare as the tools to implement robust cybersecurity, so why is the industry getting hit daily and weekly with cyberattacks?" he asked. "There's been a lot of acquisition of tools, but many still are not using them."

This challenge reflects the overarching theme of **"the acceleration of data usage"** found in the 2023 DHMW survey, which looked not just at HCOs' capabilities around security leadership, governance, and practices, but took a deeper dive into how often organizations are using the tools, processes, and resources to protect their networks and data from attacks.

Regardless of size, the cyberthreat landscape is growing too complex for HCOs to handle alone, and many lack the cybersecurity talent and/or resources to counter these sophisticated adversaries. The right cybersecurity partner can help HCOs plan, develop, and implement cyber strategies, while offering robust expertise and services able to provide around-the-clock monitoring, detection, and response. The right partner can support protection of valuable enterprise data and operations and free up an organization's IT staff to focus on digital health initiatives to improve patient care, experience, and outcomes.

Improving cybersecurity in any healthcare organization comes with escalating cost. However, the price of ransomware, data breaches, and other cyber incidents is exponentially higher, by millions of dollars. Particularly when considering the potential legal exposures and negative reputation impacts caused by access to protected patient data, these steep expenses should scare any HCO into accelerating their drive to, not only have the right tools, but to use them effectively and consistently.

About CHIME

The College of Healthcare Information Management Executives (CHIME) is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs), chief innovation officers (CIOs), chief digital officers (CDOs), and other senior healthcare IT leaders. With more than 5,000 members in 58 countries plus 2 US territories and over 190 healthcare IT business partners and professional services firms, CHIME and its three associations provide a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate, exchange best practices, address professional development needs, and advocate the effective use of information management to improve the health and care in the communities they serve. For more information, please visit **chimecentral.org**.

About Digital Health Analytics

Digital Health Analytics (DHA) is a global market intelligence and survey research hub for digital health technology. Provided by the College of Healthcare Information Management Executives (CHIME), DHA was created in 2022 to supercharge organizations' digital health transformation capabilities by moving from a one-snapshot-in-time, static Most Wired survey to a 365/24/7 data and analytics resource. DHA is the gateway for provider organizations and companies to better understand how digital technology supports leaders in transforming health and care and delivering data insights that help them make the greatest business impact possible. For more information, please visit **dhanalytics.org**.

About First Health Advisory

First Health is a global digital health risk assurance firm dedicated to serving the assurance, security, privacy, technology, and efficiency needs of healthcare. First Health offers managed solutions, programmatic approaches, and flexible service capabilities to help health and care organizations achieve their strategic, business, risk, and compliance goals.

Digital Health Analytics (DHA) is a global market intelligence and survey research hub for digital health technology. Provided by the College of Healthcare Information Management Executives (CHIME), DHA was created in 2022 as the gateway for provider organizations and companies to better understand how digital technology supports leaders in transforming health and care and delivering data insights that help them make the greatest business impact possible.