Hospital Cyber Resiliency Initiative

Landscape Analysis

DEPARTMENT OF HEALTH & HUMAN SERVICES • USA

Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

HHS 405(d)
Aligning Health Care
Industry Security Approaches

Table of Contents

Tables

Figures

Disclaimer

This document is provided for informational purposes only. Use of this document is neither required by nor guarantees compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all healthcare providers and organizations. This document is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks.

Letter from the HHS Deputy Secretary

Cyber attacks are an increasing threat to the Health and Public Health (HPH) sector. As seen with delayed procedures, diagnostic imaging and laboratory system shutdowns, patient diversions, and more, these attacks can directly compromise patient safety. With the rising frequency and complexity of cyber attacks, the Department of Health and Human Services (HHS) is committed to supporting our sector's resiliency and ability to protect patients.

In anticipation of forthcoming policy discussions, we felt it was necessary to better understand the current state of sector cybersecurity. As a starting point, HHS partnered with the Health Sector Coordinating Council (HSCC) to conduct a Landscape Analysis of a common attack point for cyber criminals, United States (US) hospitals. In light of the acuity of the patient population, cyber attacks at hospitals can be particularly consequential to patient safety. Through this Landscape Analysis we sought to better identify the biggest threats facing hospitals and assess their cybersecurity capabilities relative to commonly accepted cybersecurity practices.

Time and again, HHS and the private sector have shown they have the ability to collaborate to address urgent, complex problems. With the rise of cybersecurity threats it is more important than ever that we come together to adopt and implement new materials, tools, best practices, and more to protect patients across the country. We see this Landscape Analysis as a core, foundational document that will serve numerous operational actions and policy considerations in the months and years to come. Thank you for partnering with us.

Andrea Palm
Deputy Secretary of Health and Human Services

Introduction

The United States (U.S.) Healthcare and Public Health (HPH) sector has faced dramatic increases in cyber-attacks, causing disruption to the care continuum. The National Security Council (NSC) considers the HPH sector to be one of the top three (3) sectors prioritized for additional cybersecurity attention. This designation is consistent with other reports, such as the 2022 Verizon Data Breach Report (healthcare listed as top vulnerable sector) and the CrowdStrike 2023 Global Threat Report, which both list healthcare as the third most frequently targeted sector.

The actors conducting advanced attacks against the HPH sector generally have a few known motivations influencing their actions, including:

1. Financially motivated crime (eCrime); deploying extortion attacks like ransomware
2. State-sponsored espionage; conducting destructive attacks and generating currency for their regime or group
3. Hactivism; (for a cause) or to inflict reputational impacts
4. Public trust degradation

Threat actors operating under safe harbor (provided by hostile nation states) have been responsible for launching highly visible, crippling ransomware attacks against the U.S. HPH sector. The attacks are now growing both in numbers and severity. These attacks have been responsible for the disruption and delay of care delivery at healthcare facilities across the country, resulting in an increased risk to patient care and safety. U.S. hospitals have particularly experienced significant damage from these attacks. Consequences of cyber-attacks directed at US hospitals include extended patient care disruptions caused by multi-week outages; patient diversion to other facilities; and strain on acute care provisioning and capacity, causing the cancelation of medical appointments, non-rendered services, and delayed medical procedures (particularly elective procedures). In fact, a recently updated study from the Ponemon Institute, sponsored by Censinet, stated that 53% of respondents believed that a ransomware attack has resulted in disruption to patient care[1]

The Federal Bureau of Investigation (FBI) and Department of Justice (DOJ) are now treating the patient and public safety risk that cyber-attacks are posing on hospitals as “threat to life” crimes. These attacks are not only affecting patient care and safety, they are also creating fear and confusion while eroding the public’s trust and faith in our hospital systems throughout the U.S., potentially leading to public health challenges.

The FBI and DOJ are now treating the patient and public safety risk that cyber-attacks are posing on hospitals as **“threat to life” crimes.**

New vulnerabilities from advances in technology and care delivery are broadening the cyber-attack surface. With the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Affordable Care Act, and the 21st Century Cures Act, coupled with the internet and medical device technological advancements, healthcare facilities are increasingly adopting digital tools for new care delivery services and settings. These tools enhance the ability for clinical, revenue cycle, and business workflow enhancements through technologies such as electronic medical records (EMR), digital billing, scheduling services, Human Resource (HR) information systems, and customer relationship management software. Within clinical

[1] New Ponemon Report Shows Ransomware Continues to Impact Patient Safety, Per Survey of Hospital IT/Security Leaders - Censinet

environments, network-connected medical devices, imaging, pharmacy, and laboratory equipment can be connected and interoperate with EMRs. Additionally, these care services are expanding beyond the walls of the healthcare facility. Care is being provided in patient homes, and information sharing is occurring between patient homes and these facilities. This new dynamic has not only transformed care delivery, but has also introduced significant cybersecurity risk across the HPH sector, including hospitals.

In response to this growing threat to patient safety and public health, the HHS 405(d) Program convened its public-private partnership to conduct a review to better understand the state of cybersecurity within U.S. hospitals, deemed the "Landscape Analysis". The Landscape Analysis included a review of active threats attacking hospitals and the cybersecurity capabilities of U.S. hospitals. Included within the Landscape Analysis are the results of investigations into 1) the tactics and techniques that threat actors use to compromise hospitals and 2) the current state of participating hospital cybersecurity resiliency (using the Health Industry Cybersecurity Practices (HICP) as a framework).

The partnership was co-led by the Health Sector Coordinating Council Cybersecurity Working Group (HSCC CWG), and the HHS' Centers for Medicare & Medicaid Services (CMS).

In response to this growing threat to patient safety and public health, the DHHS 405(d) Program convened its public-private partnership to conduct a review to better understand the state of cybersecurity within US hospitals, deemed the "Landscape Analysis".

Acknowledgments

The United States Department of Health and Human Services (HHS) is grateful for the collaboration across government and with the healthcare industry in making this cybersecurity resiliency assessment possible, under the under the 405(d) Program and with the assistance of the Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG). HHS is particularly appreciative of the in-kind efforts of numerous task group members who rolled up their sleeves and provided direct support in the creation of this document.

Authors

- Erik Decker (Co-Lead)
- Robert Wood (Co-Lead)
- Dr. Syed Mohiuddin
- Douglas Nock
- Akshay Venugopalan

Additional Acknowledgments

- Troy Adams
- Cindi Bassford
- Julie Chua
- Dr. Christian Dameff
- David Finn
- Greg Garneau
- Greg Garcia
- Ed Gaudet
- Ty Greenhalgh
- Carter Groome
- Nick Heesters
- Navar Holmes
- Dr. Samantha Jacques
- Theresa Meadows
- Raj Mehta
- Monroe Molesky
- Lisa Munro
- Dr. Hannah Neprash
- Mitch Parker
- Reuven Pasternak
- Lorren Pettit
- Kate Pierce
- Sanjeev Sah
- Kendra Siler
- Nick Rodriguez
- John Riggi
- Paul Russell
- Kevin Tambascio
- Dr. David Willis
- Jessica Wilkerson

This publication is the result of the leadership and the collaboration of the following groups and professionals: the HPH Joint Cybersecurity Working Group, the Health Sector Coordinating Council, the Health Information Sharing and Analysis Center (H-ISAC), the 405(d) Steering Committee, and the 405(d) Task Group. We would also like to express gratitude to CMS, DHS, and NIST for their input, collaboration, and efforts to establish and support the 405(d) Task Group and this publication.

Executive Summary

The Landscape Analysis' charge was to highlight findings and issues affecting the cybersecurity resiliency of U.S. hospitals. National Institute of Standards and Technology (NIST) defines cyber resiliency as, the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. For the purposes of this study, the scope was narrowed to those activities that protect access to patient care and safety and reduce the negative impact of cyber threats on clinical operations. Breaches of sensitive data, although equally important, are not the focus of this study - unless the breach has a direct impact on patient care and safety.

The study's two objectives were:

- To develop a clear understanding of the current cybersecurity capabilities and preparedness across participating U.S. hospitals, as well as their ability to combat cyber threats
- To share the analysis and findings with the HSCC CWG for consideration as one of several inputs for informing prioritized cybersecurity practices for U.S. hospitals, as well as other considerations the U.S. government might undertake to improve U.S hospitals' cybersecurity resiliency

This was accomplished by evaluating the current cyber threats faced by hospitals and the entire HPH sector, as well as conducting an analysis of hospital cybersecurity capabilities and resources benchmarked against theHealth Industry Cybersecurity Practices (HICP)[2] Publication. To complete these objectives, the analysis leveraged multiple sources of data within three categories:

1. Threat data from the U.S. government, cybersecurity vendors, and open-source intelligence, threat reports from CrowdStrike and Verizon, and over 30 joint reports outlining the highest impact of hacking and ransomware groups from Cybersecurity and Infrastructure Security Agency (CISA)/ FBI advisory reports, National Security Agency, Health Sector Cybersecurity Coordination Center (HC3) reports, and Health-Information Sharing and Analysis Center (Health-ISAC) threat reports
2. Quantitative analysis of two (2) major survey instruments to determine cybersecurity capabilities[3]:
   - CHIME's Most Wired Survey (n=377), sponsored by First Health Advisory, and
   - A survey conducted in partnership with Censinet, the American Hospital Association (AHA) and KLAS (n=59)
3. Twenty (20) conversations conducted with geographically and demographically diverse hospitals.

A full list of contributing sources can be found in the Data Sources section of this document. The individual key results (by study source) are located in Studies.

Key Observations

Our analysis from the two (2) quantitative studies combined with participating hospital conversations resulted in a series of key observations, highlighted below:

[2] Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

[3] These survey instruments were chosen because of their direct correlation with HICP. Further, both surveys possessed research needed for this study, the findings are time relevant, and the participants represent a wide range of hospital types.

1. ***Directly targeted ransomware attacks aimed to disrupt clinical operations are an outsized and growing cyber threat to hospitals.*** Since 2021, primary intrusions used to cause disruption and damage increased across all sectors and industries by 50%. Ransomware is currently the largest threat to this sector and deserves immediate attention – especially considering the impact the non-availability of services can have on patient care and safety.
2. ***Variable adoption of critical security features and processes, coupled with a continually evolving threat landscape can expose hospitals to more cyber-attacks***
    - ***Multi-Factor Authentication (MFA):*** Adoption of MFA is taking place in over 90% of surveyed hospitals; however, data suggests that MFA may not be utilized consistently across key systems and critical entry points, creating additional risk of exploitation. For instance, 84% of Virtual Private Networks (VPNs) are protected with MFA, and 88% of email systems protected with MFA. Given a lack of full adoption on critical assets, it can be concluded that single credential theft through phishing attacks can lead to successful compromises.

      MFA is leveraged in over 90% of surveyed hospitals; however, data suggests that **MFA may not be utilized consistently** across key systems and critical entry points, creating additional risk of exploitation.

    - ***Vulnerability Assessments:*** 89% of the hospitals surveyed indicated that they were conducting regular vulnerability scanning at least on a quarterly basis; however, they also indicated that their use of advanced forms of testing such as penetration, red team, purple team, and tabletop exercises was 20% or lower[4]. Additionally, 70% of hospitals surveyed state they are conducting vulnerability scans against websites, which are exposed to the internet. Despite this scanning activity, only 53% of surveyed hospitals stated they have a documented plan for addressing the vulnerabilities identified. Vulnerability management that is solely comprised of regular scanning is not sufficient - partly due to the typical scope of scanning and lack of corresponding processes to prioritize and address any identified issues. Through conversations with hospitals, it was understood that vulnerability results were fairly easy to acquire through existing tools, however prioritization and resource constraints were raised as challenges for mitigating the vulnerabilities identified.
    - ***Training & Outreach:*** 86% of the hospitals surveyed responded that their users are informed and trained on performing their cybersecurity-related duties and responsibilities. However, data suggests there may be considerable variability in the training provided to hospital staffs across the sector. Additionally, little data was available on the dequacy and effectiveness of training and outreach efforts. During the interviews, participating hospitals regularly raised education and training as a desired means of achieving higher levels of cyber resiliency. A few hospitals indicated that scenario-based training (where results are shared near real-time) is an effective way to improve cyber hygiene, as well as training that is targeted to high-risk groups (e.g., executives) who might be targets of cyber-attacks.

      Hospitals regularly raised **education and training** as a primary means of achieving **higher levels of resiliency.**

[4] A red team is a team of offensive security professionals, such as penetration testers, ethical hackers, and other skilled professionals who look to uncover flaws and vulnerabilities. A purple team is a team of blue (defense) and red (offense) team who exercise in coordination to promote greater understanding of how to uncover and defend against cyber-attacks. Tabletop exercises are simulated events whereby a scenario is created, and a response team tests their response playbooks.

- ***Hospital-at-Home:*** The delivery of in-home care, accelerated by COVID-19, is growing and expanding the cyber threat landscape. In-home care delivery typically requires use of medical devices and technologies in patients' homes to communicate, monitor, and report information about their care and treatment with medical professionals. These advances in care delivery are creating new cyber resiliency challenges for hospitals and patients. Challenges range from ensuring that communications and technologies are protected, standardization issues, avoiding vendor lock-in, to scaling services while maintaining the security of assets. These are all exacerbated in rural communities where communication bandwidth is often limited, frequent internet outages occur, and in-house cyber expertise is insufficient to implement adequate controls.

3. ***Hospitals report measurable success in implementing email protections, which is a key attack vector.*** Over 99% of hospitals surveyed reported having basic spam and phishing protection capabilities in place. In the same studies, 92% of hospitals stated they use URL detection, and 86% stated they leverage automated responses to malicious email removal. However, basic spam and anti-spoofing protections do not definitively thwart the current generation of social engineering and phishing attacks. In many cases, threat actors will deploy attacks that become malicious after they are delivered, thereby thwarting basic spam and anti-virus protections.

4. ***Supply chain risk is pervasive for hospitals.*** Only 49% of hospitals state they have adequate coverage in managing risks to supply chain risk management (a sub-category of the National Institute of Standards and Technology Cybersecurity Framework [NIST CSF]). In addition, third-party and supply chain risk rates as the third most important threat amongst 288 CISOs, surveyed as part of the 2023 H-ISAC Threat Report[5]. Furthermore, one study indicated that of the 47% of respondents who reported a ransomware attack, 46% stated it was caused by a third-party. A separate study indicates that 50% or less of hospitals are considering risks to patient care in their evaluations of new suppliers' products[6]. This finding suggests that hospitals may be evaluating risks based on sensitive data compromises, rather than considering the patient safety risks that products and services third-party suppliers can create. Supply chain risk management was mentioned in nearly every conversation conducted with participating hospitals as a top priority to address in the next couple of years. Many hospitals mentioned policies have been implemented so that the hospital CISO approves all acquisition requests. Even so, much more effort is needed in this area.

50% or less of hospitals are considering risks to patient care in their evaluation of new suppliers' products. Hospitals may be evaluating risks more on **sensitive data compromises** rather than the **patient safety risks that third party suppliers can create.**

5. ***Medical devices have not typically been exploited to disrupt clinical operations in hospitals.*** Despite a few isolated cases mentioned during hospitals conversations, threat intelligence and breach data suggest medical devices are not a prominent attack vector for adversaries to disrupt hospital operations. However, they continue to be an independent source of cybersecurity concern and still warrant significant attention. Device vulnerabilities can allow advanced forms of attacks to spread across the organization. Unsupported, legacy medical devices may be considered more vulnerable to cyber-attack, typically requiring additional segmentation which can limit the usefulness

[5] 2023 Health ISAC Executive Summary Annual Threat Report

[6] HCC The State of Supply Chain Risk in Healthcare

of the devices. Historically, scanning older devices for vulnerabilities has been problematic. Disruption to the medical device during the scanning process has occurred, directly impacting patient care.

6. ***There is significant variation in cybersecurity resiliency among hospitals.*** The hospitals that participated in the study instruments were able to quantitatively determine their current set of cybersecurity capabilities. In conversations with smaller hospital cybersecurity professionals (not participating in the survey), it was noted that knowledge of resiliency coverage was limited, with a minimal ability to stay current on threats, and that slim to negative financial margins inhibited cybersecurity investments. Variation in investment was witnessed even among larger sized hospitals reporting mature cybersecurity controls, where the range of investment spanned a ~166% difference, from a lowest normalized cybersecurity investment of 0.07% to the highest of 0.75% of revenue. Primary sources of investment variation include third-party risk management, medical device security, asset management, participation in Information Sharing and Analysis Centers (ISACs), and the use of governance, risk, and compliance systems. Many of the hospitals expressed a need for more benchmarking data and consumable, actionable intelligence information, but cost and poor awareness of existing resources is a strong deterrent.

Hospitals without dedicated survey staff noted less use of surveying instruments, limited knowledge of resiliency coverage, and **minimal ability to stay current against cybersecurity threats.**

7. ***The use of antiquated hardware, systems, and software by hospitals is concerning.*** 96% of small, medium, and large sized hospitals claim they were operating with end-of-life operating systems or software with known vulnerabilities, which is inclusive of medical devices. A common technique by threat actors is to exploit known vulnerabilities. In fact, a recent industry report published an estimated six (6)-fold increase in attacks (from 2 to 12 exploited vulnerabilities in past year)[7] by China-nexus threat groups exploiting known reported vulnerabilities. Antiquated technologies limit hospitals' abilities to harden (e.g., patch) and secure their systems, increasing risk. Some larger hospitals we spoke to shared concerns connecting and exchanging data with affiliates because of elevated cyber risk associated with legacy devices and systems, especially with small, rural hospitals and facilities where this pattern is more commonplace.

96% of hospitals claim they were operating with **end-of-life operating systems or software with known vulnerabilities,** which is inclusive of medical devices.

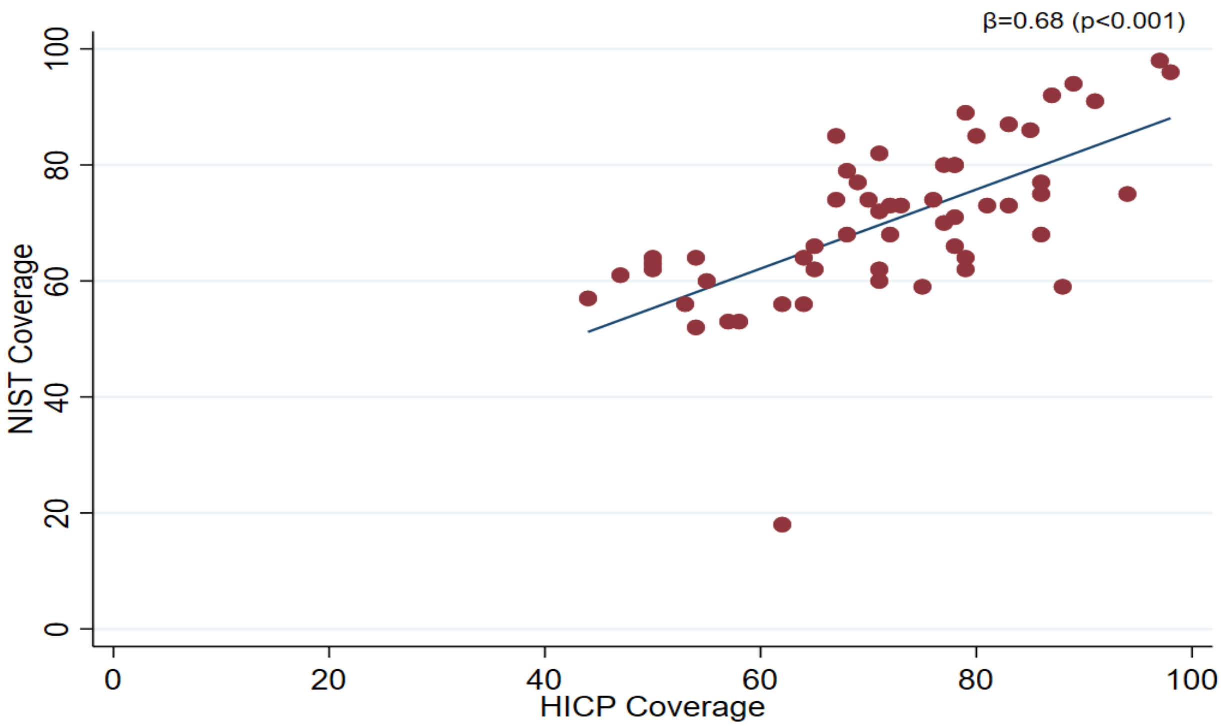
8. ***Cybersecurity insurance premiums continue to rise.*** On average, cybersecurity premiums increased by 46% in 2021. Five of fifty-six hospitals surveyed in 2022 experienced increases more than 100%, whereas 32 experienced increases just below 35%. Drastic increases in cyber insurance cost have resulted in some hospitals having to forgo insurance or self-insure to reduce risk. Coverage exclusions for not meeting minimum security standards have reduced the adequacy of coverage as well. These exclusions tend to be more problematic for small and rural hospitals, which typically have smaller budgets and fewer cyber professionals to implement better protections. Additionally, smaller sized hospitals tend to view cyber insurance as a "stop gap" to cover a major or outlying cyber event, potentially impacting their appetite to invest in better cyber controls to reduce insurance costs and improve their resiliency.

[7] 2023 CrowdStrike GSR Report

9. ***Securing cyber talent with requisite skills and experience is challenging.*** Conversations with participating hospitals uncovered they are experiencing securing cyber professionals to meet the security challenges facing this sector. The supply of trained individuals to fill cyber vacancies across the U.S. is substantially low. According to Cyberseek, as of March 2023, there are 755,743 job openings for cybersecurity professionals nationwide. Coupled with high vacancies across the U.S., individuals remarked that those applicants who have requisite skills tend to gravitate to non-healthcare industries that pay better. Attracting and securing cyber talent is especially difficult for small, rural hospitals. Their cyber teams are very small, and in some cases, are staffed by individuals who wear many hats, lack skills, and work in part-time arrangements. Furthermore, remote work is often not an HR policy that is supported by hospitals, so the pool of talent tends to be limited and locally based. Many of them would like to enhance their security posture and resiliency, but lack personnel with necessary skills in specific disciplines, and funds to attract top talent. Some small, rural hospitals we spoke with remarked on the challenges of meeting existing industry guidance and compliance standards when there are talent gaps. The standards are written the same regardless of facility size or make-up, making meeting them especially difficult for small hospitals that typically have inadequate cyber budgets and staffing.

10. ***Adopting HICP improves cyber resiliency*** An interesting correlation that was uncovered during analysis was a strong connection between those who have adopted HICP and robust NIST CSF coverage. This indicates that organizations that focus on HICP Practices will gain value and benefit towards managing implementation of the NIST CSF cybersecurity framework. Proving the investment in hygiene pays dividends in larger programmatic maturity. The relationship between HICP and NIST

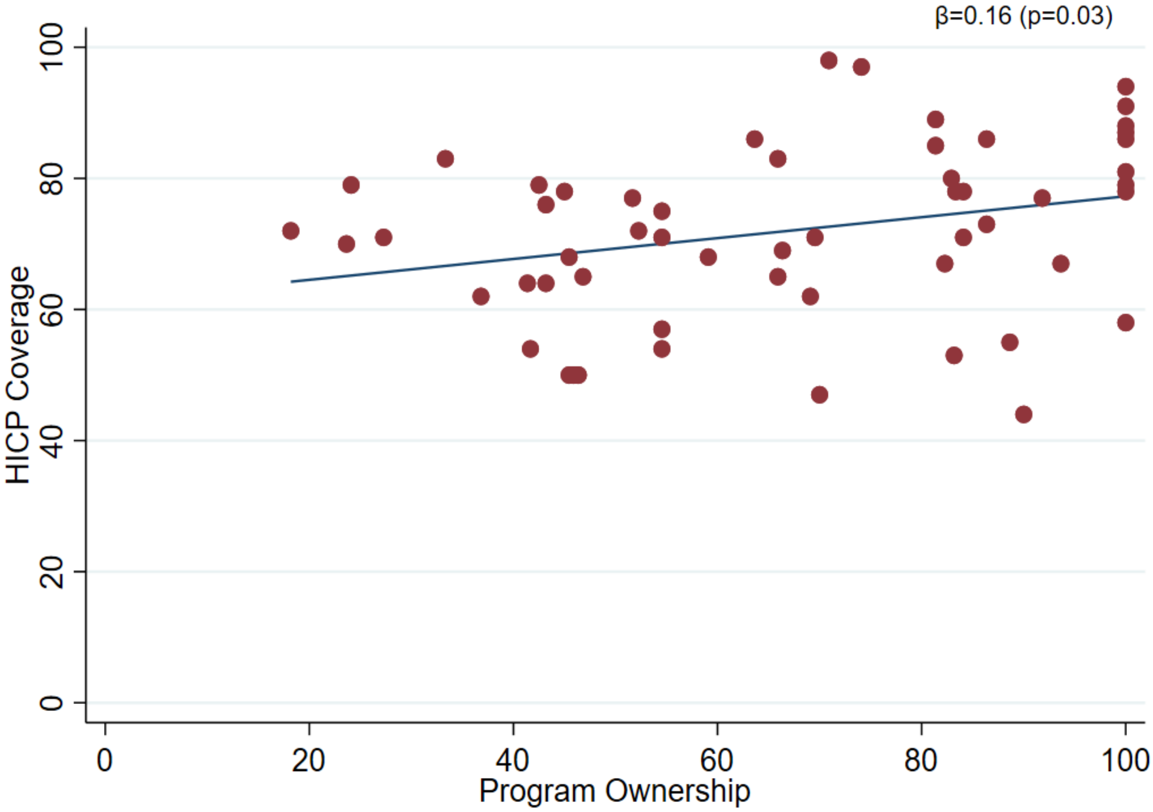
Figure 1 Correlation of HICP and NIST coverage



coverage at the organizational respondent level was quantified using bivariate linear regression. A strong positive association was found between the two. For every 1 percentage point increase in HICP coverage, an average increase of 0.68 percentage points in NIST coverage was found - suggesting a strong positive correlation between the two variables.

- ○ Quantitative studies were run through a regression analysis, HICP coverage (overall and by individual practice domain) was then quantified as a function of the following cybersecurity investments reported by Censinet respondents: number of cyber employees, cyber expense to revenue, program ownership, cost to protect patient records (nominal and normalized), cost to protect the workforce (nominal and normalized), and the increase in cybersecurity insurance costs. Only program ownership and cost to protect the workforce were strongly associated with HICP coverage. For every 1 percentage point increase in program ownership, a 0.16 percentage point increase in HICP coverage was found.

Figure 2 Quantified association of HICP coverage



HICP Practice Adoption

This Landscape Analysis leveraged the 405(d) HICP publication to determine the current state of each hospital's cybersecurity resiliency. HICP directly correlates to the threats outlined in this analysis, such as ransomware. HICP also maps to CISA's Common Performance Goals (CPGs)[8]. The analysis of the data sources mentioned on page 51 suggests that hospitals' adoption of HICP practices fall into the following four categories:

No Action Required—Significant Progress Made	Urgent Improvement Needed	Additional Research Required	Further Attention Required (Not Urgent)
• E-mail protection systems	• Endpoint Protection Systems • Identity and Access Management • Network Management • Vulnerability Management • Security Operation Center and Incident Response	• IT Asset Management • Network Connected Medical Device Security • Cybersecurity Oversight and Governance	• Data Protection and Loss Prevention

A detailed risk assessment was conducted based on the above categories and HICP practices., which are included in the remainder of this document.

Data Sources

This Landscape Analysis uses data from private and public partners to compare U.S. hospital systems' cybersecurity capabilities against the most prevalent methods cyber adversaries use to break in and cause disruptive attacks. The data for this study were chosen due to the breadth and depth of coverage of cyber practices, and specifically their connection to both the NIST CSF and HICP. These two study instruments allowed for a comparative analysis across these factors. This study did not consider impacts or implications to data-related breaches, as these breaches do not generally cause clinical disruption and risks to patient safety. The process of cross-referencing data across the selected sources and threat data provides high confidence in this analysis.

Many of the hospital-specific cybersecurity protection insights gleaned from this analysis are derived from two studies conducted by industry experts. Both studies offer analyses on cyber resiliency from a wide range of hospital types, obtained through voluntary surveying. A positive and selection bias might exist in the survey data collected, due to the voluntary and self-reported nature of the survey data.

The two primary quantitative studies are:

1. CHIME Most Wired Survey, sponsored by First Health Advisory, completed in 2022
2. Censinet/AHA/KLAS Study with normalized data collected by hospitals from 2021, completed in March 2023

288 healthcare executives said **ransomware** was their biggest cybersecurity concern.

[8]

The participants in the two surveys above represent a wide range of hospital types. (See **Table 1**). These survey instruments featured a strong focus and depth of coverage on HICP.

Additional analyses were conducted on data collected through the HSCC JCWG, inclusive of the following:

- CrowdStrike 2022 and 2023 Global Threat Report and Threat Hunting Report[9]
- Health Sector Cybersecurity Coordination Center (HC3) Ransomware Threat Impacts to HPH
- H-ISAC 2022 Annual Threat Report
- H-ISAC Monthly Threat Briefings
- Individual briefings collected from PwC, Deloitte, and Fortified Health
- Ponemon Institute's The State of Supply Chain Risk in Healthcare[10]
- 2022 Verizon Data Breach Investigations Report (DBIR)[11]

The table below includes additional statistics related to the data sources listed above.

Table 1 Data Sources – table of statistics

Data Set	Demographic Background of Data
CHIME Data	• 177 hospitals representing small (owning just 1 hospital) • 107 hospitals representing medium (owning between 2 and 5 hospitals) • 81 hospitals representing large (owning more than 5 hospitals) • Represented 49 of the 50 US States
Censinet/AHA/ KLAS Study	• 59 small, medium and large hospitals (size measured by # of beds – using HICP), evaluating on coverage to the NIST CSF and 405(d) HICP, as well as organizational benchmarking
2023 H-ISAC Threat Study	• 11 notable threat actors profiled with descriptions of their tactics, techniques and procedures • 288 healthcare executives surveyed to determine top threats
HC3 Threat Data	• 2,224 healthcare specific cybersecurity incidents • Deep analysis of 33 FBI, CISA and HC3 Threat Analysis Reports
Verizon 2022 DBIR Report	• 23,896 security incidents across a variety of sectors • 5,212 confirmed data breaches of the 23,896 incidents • 849 incidents and 571 confirmed data disclosure in the healthcare sector

[9] 2022 Global Threat Report: Insights from the Threat Landscape | CrowdStrike
[10] The State of Supply Chain Risk in Healthcare | Health Sector Council
[11] 2022 Verizon Data Breach Investigations Report (DBIR)

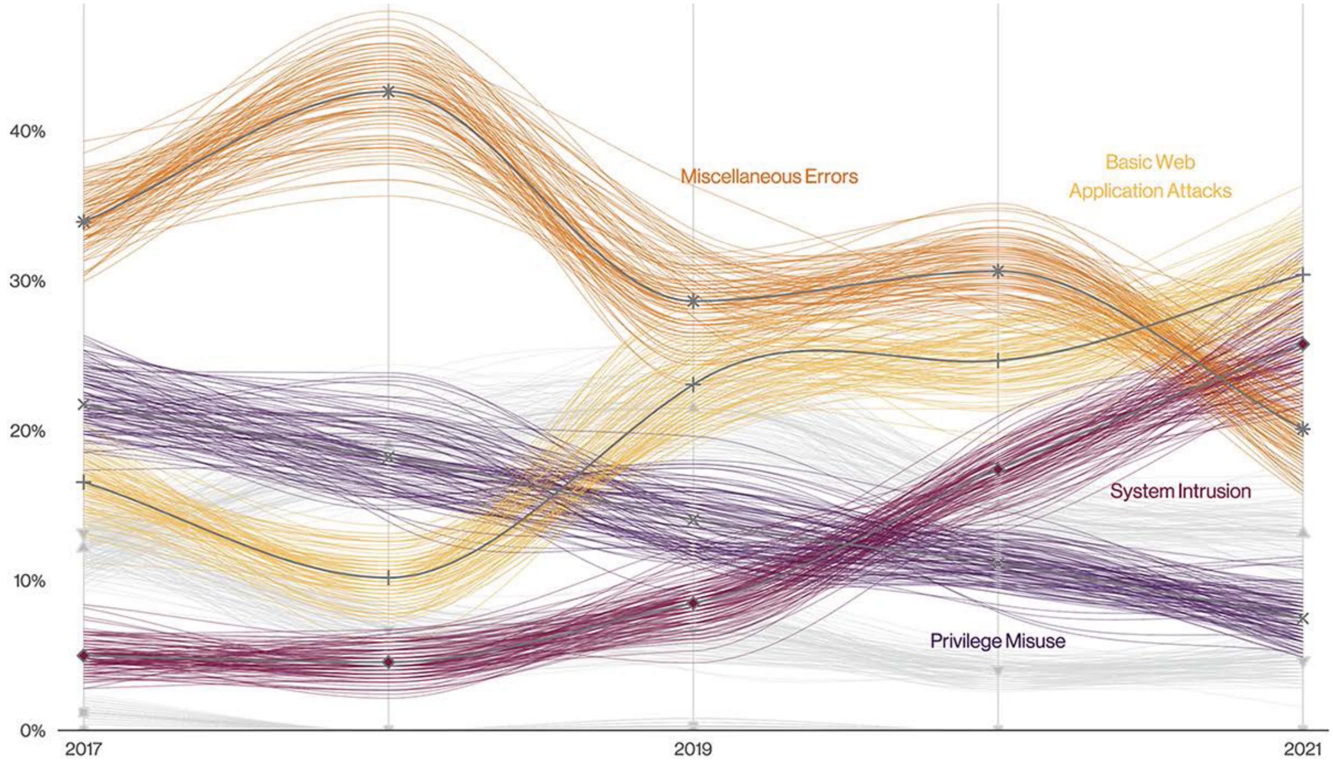
Threat Analysis

Our assessment, based on the data sources used, identified numerous cybersecurity threats to U.S. hospitals, such as

1. Ransomware and Ransomware-as-a-Service (RaaS) attacks
2. Cloud exploitations by threat actors; with data suggesting a 95% increase from 2021 in cloud exploitation cases
3. Phishing/Spear-Phishing Attacks; specifically those attacks that overcome MFA through social engineering
4. Software and zero-day vulnerabilities
5. Distributed Denial of Service attacks (DDoS)

The 2022 CrowdStrike Threat Report states that 71% of cybersecurity attacks are comprised of non-malware and 'hands-on-keyboard' activity, which implies that threat actors are moving away from malware-directed attacks. These 'hands-on-keyboard' targeted attacks require an adversary to conduct a multi-staged attack, with the goal of extorting hospitals by disrupting their business and clinical operations. This trend is further confirmed by the 2022 Verizon Data Breach Report (**Figure 3**, below) that illustrates an increase in 'system intrusion' attacks. These types of attacks which typically involve direct, non-malware, and 'hands-on-keyboard' activities.

Figure 3 2022 Verizon Data Breach Report -- demonstrating recent increase in system intrusions with corresponding decrease in miscellaneous errors and privilege misuse



Evolving Threat of Ransomware

The most common case of ‘system intrusion’ cyber-attacks tend to be extortion attacks leveraging weaponized tools such as ransomware or ransomware-as-a-service. Ransomware represents the most prolific cybersecurity threat hospitals have encountered to date. As ransomware rates rapidly increase, the result is delays or degraded operational capacity to serve patients. Within healthcare, ransomware attacks have significantly affected business and operational systems and technologies essential for clinical operations and patient services. There have been both publicly reported and anecdotal data shared that ransomware incidents have caused denial of hospital operations and services lasting from days to weeks, disruption of clinical services for weeks to months, and cost up to hundreds of millions of dollars.

According to PwC, “Ransomware operators are the largest threat to the healthcare sector. These threat actors have the capabilities to render critical healthcare services offline, as well as steal confidential and sensitive information of both patients and staff, all while expanding their operations and complexity. Due to their large network of affiliate programs, ransomware operators have the potential to infect numerous entities at once. The threat cannot be understated in a sector that depends on operational uptime and the availability of services.” CrowdStrike reports similar findings as well.

Ransomware attacks in the HPH sector are also evolving; adversaries are using a combination of extortion tactics to fulfill their objectives. Typically, adversaries will take the path of least resistance in the furtherance of the damage they aim to cause. They will look to apply their resources in the cheapest and easiest method possible. This could occur from vectors external to the hospital (e.g., the internet) or from inside the hospital (e.g., connections to third-party suppliers).

Adversaries may choose to elevate their attack when ransom demands are not met by either conducting a DDoS attack against the victim, demanding ransoms from those most affected by the release of sensitive information (patients, hospital affiliates, etc.), or both. In fact, in recent months, the number of DDoS attacks on the healthcare sector has grown. On March 17, 2023, Microsoft published a blog indicating that the number of DDoS attacks against their healthcare sector customers, using Azure, had grown from “10-20 attacks in November to 40-60 attacks daily in February.[12]”

Data suggests there is general alignment on the need to address these disruptive attacks. The 2023 Annual H-ISAC Threat Report stated that 288 healthcare CISOs listed ransomware as their biggest cybersecurity concern. This finding is also supported by hospital conversations as part of this Landscape Analysis.

Data provided by joint cyber advisories from the FBI, CISA, NSA, and HC3, suggests that the criminals conducting these attacks tend to be organized crime, and largely based in, but not limited to, Eastern European countries. Threat actor groups are growing across Eastern Asia and Middle East countries as well. Most threat actors in the healthcare sector do not have direct intent to inflict harm on individuals but the aftermath of their actions can result in collateral damage.

Adversaries are improving their capabilities through multiple methods across all sectors, including healthcare. Their attacks are coming in with high velocity, higher quality, and more efficacy. In other

[12] KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks - Microsoft Security Blog

words, attacks are faster, smarter, and more organized. Examples of these attributes are described below:

1. ***Elapsed time to exploit is decreasing.*** The CrowdStrike study revealed adversaries were able to "… in just 1 hour and 24 minutes" move laterally from the initial compromised host, a reduction from 1 hour and 38 minutes from the prior year. These "break out" actions are executed without writing malware. Threat actors are using legitimate credentials and built-in tools that are repurposed once the adversary is in the environment. In fact, nearly 80% of cyber-attacks leverage identity-based attacks to compromise legitimate credentials and use techniques like lateral movement to quickly evade detection.

80% of cyberattacks leverage **identity-based attacks** to compromise legitimate credentials and use techniques like lateral movement to quickly **evade detection.**

2. ***Expansion of Phishing-as-a-service.*** This allows threat actors to focus on high quality attacks that can evade or "annihilate" standard security controls. A common attack vector leveraged by Phishing-as-a-Service actors is to purchase credentials from marketplaces and to bypass MFA using MFA fatigue, vishing (phone), and "one-time password smishing (text) techniques."
3. ***Increase in "Access Broker" services.*** Access Brokers grew 112% from 2021 to 2022. These services focus their efforts on compromising legitimate access to organizations, then selling that access to bad actors looking to commit further objectives, such as ransomware. This type of underground market has been on the rise over the last few years and demonstrates there is enough demand and payout for these groups to specialize. This is especially concerning as it implies the adversaries are differentiating their resources and capabilities, enabling faster action at less cost.

CASE STUDY: Ransomware's Real Impact on Patient Care

Example 1: San Diego-based non-profit healthcare provider suffered a ransomware attack in May 2021, with an estimate of it costing $112M in lost revenue, remediation and fines[13] This is in addition to the $3.5m agreed as part of its class action settlement[14]. The original attack caused the healthcare provider to suspend their IT systems, including their public facing portals. Additionally, several hospitals owned by the company had to turn away patients with specific patient needs, such as those suffering from strokes or heart attacks.

Example 2: Three regional medical centers in Alabama were impacted by an unknown ransomware variant that crippled operational capabilities of the hospital to such an extent that non-critical potential patients were directed to other hospital facilities. Due to the critical nature of the services, the owners of the hospitals, decided to pay the attackers to obtain the decryption key so that systems could be restored.[15]

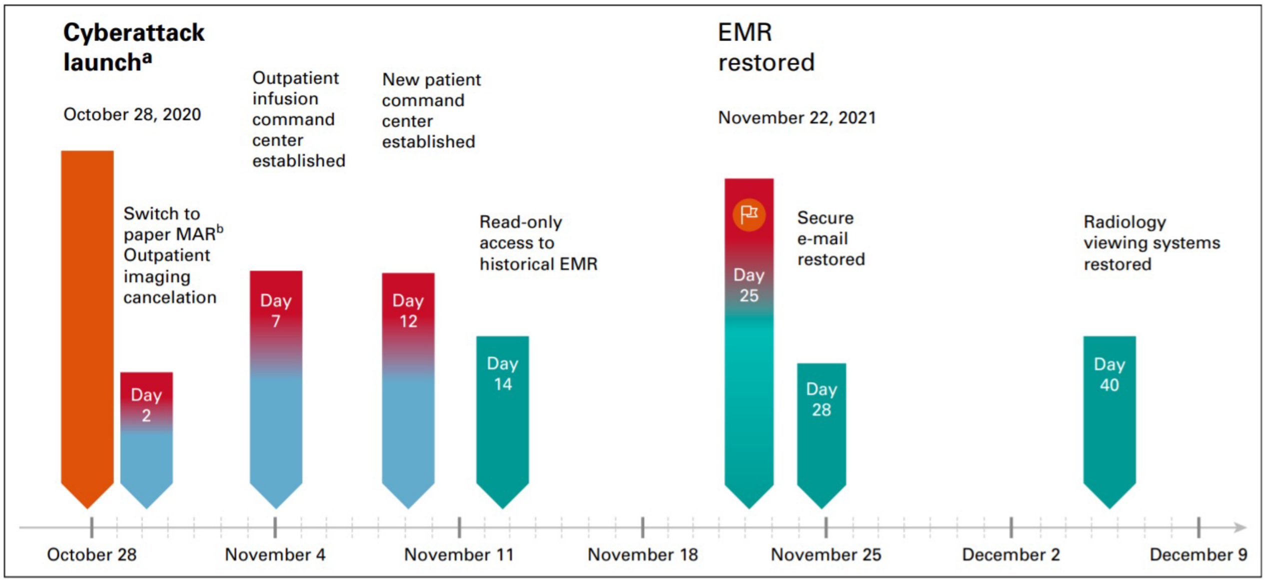
Example 3: A small medical Ear, Nose and Throat (ENT) specialty practice in Michigan shut down after cyber-attackers deleted the practice's patient records. The two physicians decided to retire early rather than paying the ransom to buy back the medical files[16].

Example 4: A University Health Network in Northeast U.S. was impacted by a ransomware attack in

[13] Scripps Health Ransomware Attack Cost Increases to Almost $113 Million | hipaajournal.com
[14] Scripps Health to pay $3.57 million after ransomware data breach | cbs8.com
[15] PWC Report, Under the Lens The Healthcare Sector, 2021
[16] All of records erased, doctor's office closes after ransomware attack | startribune.com

October of 2020 causing $21M in damages[17]. Serving as a role model to other hospitals in an effort to be transparent and aid other hospitals abilities to prevent such damage, the health system publicly disclosed the details of their attack. One thousand three hundred (1,300) of their servers were shut down, over 5,000 endpoints infected with ransomware, and hundreds of applications impacted. As the timeline below shows, they operated without email for 25 days and without imaging for 40 days.

Figure 4 Cyberattack Response Timeline



Link Between Threats and Potential Mitigation

The threat analysis provided in Table 1 below outlines the various threat actions hospitals can face, along with potential mitigation strategies. The data is informed by actual threats actions to the sector as determined by real-world breach data, threat intelligence, and industry reports.[18][19] This analysis was conducted in the context of threat actions that can lead to disruptive attacks. Generally, these attacks demonstrate the following script and characteristics that map across seven stages:

Stage 1: Conduct reconnaissance and look for weakness

Stage 2: Establish the initial foothold

Stage 3: Move laterally off the initial foothold and establish persistence

Stage 4: Discover internal targets of interest

Stage 5: Target privileged systems and elevate their access

Stage 6: Remove hospital's ability to recover through backups and restoration options

Stage 7: Weaponize malware or other administrative access to cause damage

Further details on these stages are also included in the threat analysis outlined in **Table 2**, below.

[17] UVM Health Network reports $21 million in losses - VTDigger
[18] Verizon Data Breach Investigation Report 2008-2022
[19] Technical Volumer 2: Cybersecurity Practicecs for Medium and Large Health Care Organizations

Table 2 Examples of Threat Actions, Stages, Impacts, and Potential Mitigations

Threat Actions	Stage	Potential Impact	Potential Mitigation
Vulnerability and Port Scanning	Stage 1	Evaluation of assets directly connected to the internet, looking for interesting points of entry. Commonly looking for VPN systems, web applications with common vulnerabilities, registered domain names, and remote desktop entry points.	• Log Collection from Perimeter Systems SIEM alerts 24x7 SOC • Detect typo-squatting domains used for further phishing attacks • Conduct Red Team activities to detect scanning attempts • Passive monitoring systems
Employee Recon	Stage 1	Enumeration of employees within the organization, including names, email addresses, and roles. This data is used for specific phishing targeting. Commonly attack executive leadership, procurement, HR and IT departments.	• Minimal defense options, shy of organizational policy to not participate in social media using office devices • 'Whaling' attack simulation training
Third-party Breach	Stage 1	An incident in which the third-party is compromised and can be used as an access or attack vector to launch further attacks. Hospitals can be attacked through this conduit depending on access afforded to suppliers, or they might be serving up mission-critical services to clinical operations that are the source of an attack launch.	• Implement a third-party risk assessment and management program, with focus on evaluating risk to patient safety and connectivity to the hospital • Stipulate contractual protections for mission-critical suppliers • Ensure risks are mitigated through internal controls and remediated with suppliers
Miscellaneous Errors	Stage 2	Incidents where unintentional actions directly compromised a security attribute of an information asset, such as configuration mistakes; this is not inclusive of lost devices, which would be represented in lost or stolen assets.	• Strict change management procedures to ensure secure configuration changes • Cloud Posture Management software • Vulnerability scanning – unauthenticated (looking for common issues) • Vulnerability scanning – authenticated (conform to gold standard baselines, such as CIS Benchmark) • Passive vulnerability monitoring systems • Limit privileged access to internet exposed systems, requiring specific segregation of duties for product releases; train administrators to be watchful of configuration mistakes

Threat Actions	Stage	Potential Impact	Potential Mitigation
Credential Abuse	Stage 2	Stolen credentials, whether a password or multi-factor token, are used by an unauthorized actor to authenticate to an information asset. New popular attacks to bypass MFA include cookie-harvesting attacks, whereby cookies that allow persistence are used for circumvention.	• Phish-resistant MFA on external facing systems • Implement NIST 800-63 compliant password protections. • Phish-resistant MFA for privilege escalation tools (e.g., PAM)
Phishing / Social Engineering	Stage 2	Social engineering attacks (e.g., phishing) represent a common form of malware delivery or credential-related attacks. This is typically the start of a longer attack chain.	• Email Defense: URL rewrite for click detection • Email Defense: Automated malicious email retraction • Email Defense: AV/SPAM/Denylists • Email Defense: DMARC • Conduct monthly phishing simulations; track click rates and email detection report rates by employees. • Targeted education for frequent failures to monthly phishing tests • Recurring Education: LMS training to be watchful for phishing and instruct how to report it • Policy: State intention to provide periodic security training to the hospital • MFA implementation for all external facing systems (cloud, web, remote access; consumer facing systems can be opt-in at their discretion)
Vulnerability Exploit	Stage 2	Exploitation of an unpatched or zero-day vulnerability that leverages malware and/or targeted exploitation tactics in an effort to achieve their objective (such as deploying ransomware).	• Patch assets and endpoints. • SIEM alert detection • IR Playbook for 24x7 response • Implement and monitor Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR) • Conduct static and dynamic application code scanning (SAST/DAST)
Web application attacks	Stage 2	Commonly used to deploy web shells, which is used to further conduct credential theft and lateral movement.	• Patch web applications • Web App Firewall (WAF) protections • Log management/forwarding to SIEM • IR Playbook for 24x7 response

Threat Actions	Stage	Potential Impact	Potential Mitigation
Denial of Service (DoS)	Stage 2	Attacks intended to compromise the availability of networks and systems, inclusive of both network and application-layer attacks.	• DDoS Protection systems (WAF, network layer throttling) • IR Playbook for 24x7 response • WAF for web protection
Command and Control Propagation	Stage 3	Shift off the initial endpoint or foothold and deploy access tools to gain multiple layers of persistence. Adversary switches off the initial chain of attack (under the assumption that it will be detected) and attempts to move towards a secondary infrastructure and establish persistent command and control. This could also be sourced from a third-party who has remote network access to the hospital.	• EDR tool implementation, deployed on endpoints and servers • IR Playbook for behavioral based use of built-in tools operating abnormally (such as contacting thousands of assets) • Review third-party connections and anomalous activities. • Limit third-party connections to only specific assets that they are contractually obligated to access. • Conduct Red Team exercises to determine lateral movement effectiveness. • Leverage network segmentation and firewalls to limit east-west network movement.
Internal Asset Discovery	Stage 4	Continuing with the determination of assets of interest, using the foothold that has been established common built-in tools such as ping, PowerShell, DNS, and others are used to determine other targets of interest. These targets are used both for determining maximum impact as well as determining a means for establishing persistence and moving away from the initial foothold, in anticipation of that path being discovered.	• EDR tool implementation, deployed on endpoints and servers • IR Playbook for behavioral based use of built-in tools operating abnormally (such as contacting thousands of assets)

Threat Actions	Stage	Potential Impact	Potential Mitigation
Attacks Against Connected Medical Devices/ Technologies	Stage 4	Undermined patient safety, delay or disruption in treatment that could be life threatening.	• Place medical devices/technologies on segmented networks that have stronger internal restrictions for internal access. • Establish IR Playbooks for monitoring network access probes and appropriate clinical notifications when medical devices/ technologies are affected. • Ensure default passwords are changed upon installation. • Ensure all devices are captured in configuration management database (CMDB). • Track vulnerabilities that affect medical devices/technologies and implement compensating controls until patches become available. • Patch medical equipment as patches become available. • Manage the security of legacy technologies including the core practices of governance, communications, cybersecurity risk management, future proofing, and associated recommendations (e.g., HSCC CWG's Healthcare Industry Cybersecurity Managing Legacy Technology Security document).
Credential Harvesting	Stage 5	To elevate privileges, attackers will look to harvest credentials. This can occur through malware locally deployed on endpoints/servers, as well as using Windows domain management tools like NTDSUtil to make copies of hashed credentials for offline cracking.	• Establish active directory (AD) isolation reference architecture (Red Forest/ESAE/ RAMP) to prohibit credential harvesting. • Implement MS ATA defense. • Establish IR Playbook for creation of new Domain Admin, or other high privilege accounts. • Deploy EDR to monitor for harvesting attacks from internal endpoints (and detect from servers). • Deploy Privileged Access Management tools to secure key service and administrative accounts.

Threat Actions	Stage	Potential Impact	Potential Mitigation
Privilege Escalation to Active Directory (AD)	Stage 5	A common attack path is to get the highest-level privileges within AD and maintain persistence at this stage through the creation of additional accounts or further takeover of existing Domain Admin credentials. This is used to prepare for the final attack stage.	• Establish a "Red Forest/ESAE/RAMP" design structure in AD Require MFA access to any domain controller • Require jump box, or "Privileged access workstation" access to conduct any Domain Admin level administration – isolate jump box both from a network perspective and credential perspective. • Restrict user accounts from having access to local admin credentials (exception basis only). • Implement LAPS for remote endpoint management, allowing for unique admin and password for each individual managed endpoint. • Alerts on Privilege Escalation
Destruction of Backups	Stage 6	After the discovery of backup systems, especially systems that conduct disk to disk backup, the adversary will use the privileged credentials previously gathered to wipe and destroy backup copies.	• ACLs built with strong out of band authentication to backup storage (if disk to disk) • Vaulting / air-gapping backup solutions • Immutable backup solutions (such as tape, if no other options) • Separate service accounts with strong passwords, rotated on a regular basis, for writing backup files • IR Playbooks detecting file deletion • Ransomware protection enablement on EDR tools (which prohibits large scale file access/deletion)
Weaponizing Malware or Legitimate Tools	Stage 7	Leveraging the privileged access that has been compromised, adversaries will stage and deploy the impactful attack. This could be through the deployment of malware (e.g., ransomware) or conducted by using built-in tools (e.g., PowerShell) to cause damage.	• Deploy EDR and enable ransomware prevention mechanisms to prohibit mass scale deployments. • Ensure frequent backups are occurring and have been tested (e.g., RTO, RPO) • Establish system contingency plan for recovering systems from backup (i.e., BC/DR plans). • Ensure clinical procedures are developed to maintain operations. • Tabletop exercise a large scale system down event with executives and key clinical leaders. • Conduct Red Team exercises to determine if it is possible to weaponize activities.

Capabilities and Performance Assessment

This Landscape Analysis aims to determine the current state of cybersecurity capabilities and performance of participating U.S. hospital systems. Evaluation of capabilities included mapping them back to the adversaries' methods of attack. This linkage is important, as it could help hospitals prioritize the NIST CSF and HICP.

The CHIME's Most Wired Survey data results and the Censinet/AHA/KLAS Study of 2023 were used to assess how adept hospitals' cybersecurity capabilities are, compared to the standards and practices set by the NIST CSF and HICP.

The CHIME data provided coverage of 377 hospitals and included 148 out of 994 questions specifically related to cybersecurity. The answers to these questions were either "Yes" or "No" or provided options of "periodic usage" (e.g., "How often do you conduct tabletop exercises: Every two years, annually, quarterly, never").

The Censinet/AHA/KLAS Study provided coverage of 59 organizations that operate hospitals. It included a total of 16 questions related to the demographics of the organizations, 108 questions related to the implementation of NIST CSF, and 455 questions related to the implementation of HICP. Each of the NIST and HICP questions provided a 4-point Likert scale of: 1) No Coverage (0%-34%, 2) Partial Coverage (35-69%, 3) Substantial Coverage (70%-99%), and 4) Full Coverage (100%).

Additionally, there are two key characteristics of the hospital sample in the Censinet/AHA/KLAS study worth highlighting:

1. Total number of full-time employees dedicated to cybersecurity
2. Cyber expense as a percentage of total revenue

Both data points can serve as a marker for the maturity level of a provider's cybersecurity program relative to their size.

When submitting data, hospitals selected their organization sized based on the HICP size definition, noted in Table 2, below. This tool helps organizations self-select their organization size by looking at several factors. Organizations were able to ultimately select their own size based on how they lined up amongst these factors.

Table 3 Choosing Your Organization Size Based on HICP and "Best Fit"

Best Fit		Small	Medium	Large
Common Attributes	**Health information exchange partners**	One or two partners	Several exchange partners	Significant number of partners, or partners with less rigorous standards or requirements
				Global data exchange
	IT capability	No dedicated IT professionals on staff, or IT is outsourced	Dedicated IT resources are on staff, co-managed with outsourcing, or fully outsourced IT	Dedicated IT resources with dedicated budget
			IT is responsible for security	CISO or dedicated security leader with dedicated security staff
	Cybersecurity investment	Non-existent or limited funding	Funding allocated for specific initiatives (projects)	Dedicated budget with strategic roadmap specific to cybersecurity
			Potentially limited future funding allocations	
			Cybersecurity budgets are blended with IT	
Provider attributes	**Size (provider)**	1-10 physicians	11-50 physicians	Over 50 physicians
	Size (acute / post-acute)	1-25 providers	26-500 providers	Over 500 providers
	Size (hospital)	1-50 beds	51-299 beds	Over 300 beds
	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated Delivery Networks (IDNs)
				Participate in Accountable Care Organizations (ACOs) or Clinically Integrated Networks (CINs)
Other org types			Practice management organization	Health plan
			Managed service organization	Large device manufacturer
			Smaller device manufacturers	Large pharmaceutical organization
			Smaller pharmaceutical companies	
			Smaller payor organizations	

Staffing Analysis

The staffing analysis was conducted leveraging data sourced from the Censinet/AHA/KLAS Study. On average, organizations employed or contracted 50 cybersecurity full-time employees (FTEs), though the median was 38. This number varied by the size of the organization, based on HICP size analysis.

Large-sized organizations:

- First tier (bottom 25% ranking) was between 13-33 FTEs,
- Second tier (middle 50% ranking) was between 33-101 FTEs,
- Third tier (top 25% ranking) was between 101 and 148 FTEs.

For large organizations there was a single outlier of 220 FTEs.

For medium-sized organizations:

- First tier (bottom 25% ranking) was between 1-8 FTEs,
- Second tier (middle 50% ranking) was between 8-43 FTEs,
- Third tier (top 25% ranking) was between 43-80 FTEs.

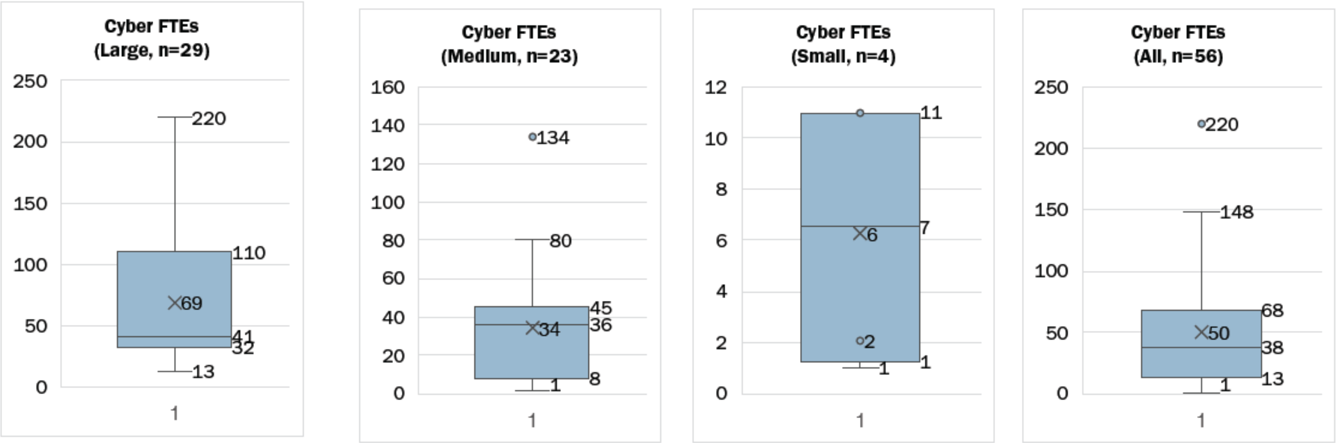
Within medium-sized organizations, an outlier of 134 FTEs invested was identified.

For small-sized organizations:

- Second tier (middle 50% ranking) was between 1-11 FTEs.

Given the small sample size of smaller sized hospitals, there was no statistically significant difference in FTE spread. Rather, the spread ranged between 1-11 FTEs; specifically with two organizations stating they had between 1-2 FTEs, and two other organizations stating they had 11.

Figure 7 Staffing Analysis of organizations by size



Cyber Expense to Revenue Analysis

The financial analysis was conducted leveraging data sourced from the Censinet/AHA/KLAS Study. The metric produced was based on self-reported financial data describing the percentage of cybersecurity investment as a component of revenue compared against the percentage of cybersecurity program ownership within the hospital. It was rare that the cybersecurity program underneath the CISO was directly responsible for, and budgeted for, all common components of the cybersecurity program. For example, in some organizations the CISO was not responsible for firewall management or identity and access management. However, these programmatic elements are still important for determining cybersecurity capability and they still introduce cost. As such, the attempt to "normalize" the financial investment by dividing "cybersecurity investment" by "percentage ownership', produced an estimated investment called "Normalized Cyber Expense to Revenue". For example, if an organization submitted a 0.25% cybersecurity expense to revenue metric and owned 60% of the cybersecurity program, the resulting normalized metric was 0.417% (.25%/60%).

On average, organizations invested 0.37% of revenue into cybersecurity budgets. This number was fairly consistent across large or medium-sized hospitals. Smaller hospitals invested higher at 0.76% on average. Through this analysis, it appears as though larger and medium-sized organizations are able to have effectively the same level of HICP coverage (69% and 74% coverage, respectively) at a lower price point due to scale. The low sample count of small hospitals (n=4) made it difficult determine a statistically significant average (80% coverage of HICP reported). The analysis did seem to indicate that the larger organizations were able to scale their expenses at a lower cost than smaller organizations.

For larger-sized hospitals:

- First tier (bottom 25% ranking) was between 0.07% and 0.20%,
- Second tier (middle 50% ranking) was between 0.20 and 0.42%,
- Third tier (top 25% ranking) was between 0.42% and 0.75% of revenue.

For medium-sized hospitals:

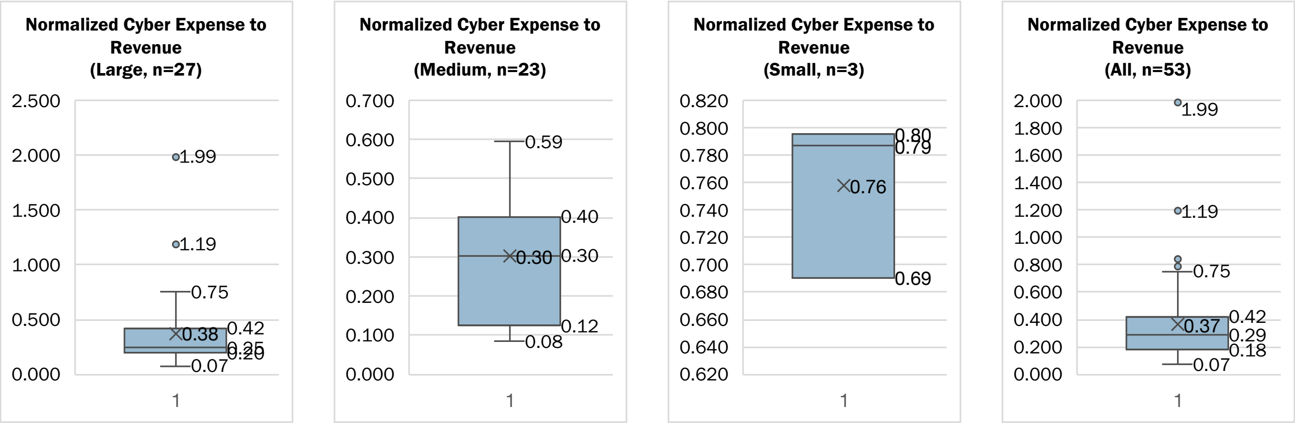
- First tier (bottom 25% ranking) was between 0.08 and 0.12%,
- Second tier (middle 50% ranking) was between 0.12 and 0.40%,
- Third tier (top 25% ranking) was between 0.40 and 0.59% of revenue.

For small-sized hospitals:

- Second tier (middle 50% ranking) was between 0.69 and 0.8040%,
- Third tier (top 25% ranking) was between 0.40 and 0.59% of revenue.

Given the small sample size of smaller sized hospitals (n=4), there was no statistically significant difference between cybersecurity investments. However, the spread ranged between 0.69% of revenue to

Figure 8 Normalized Cyber expense to revenue



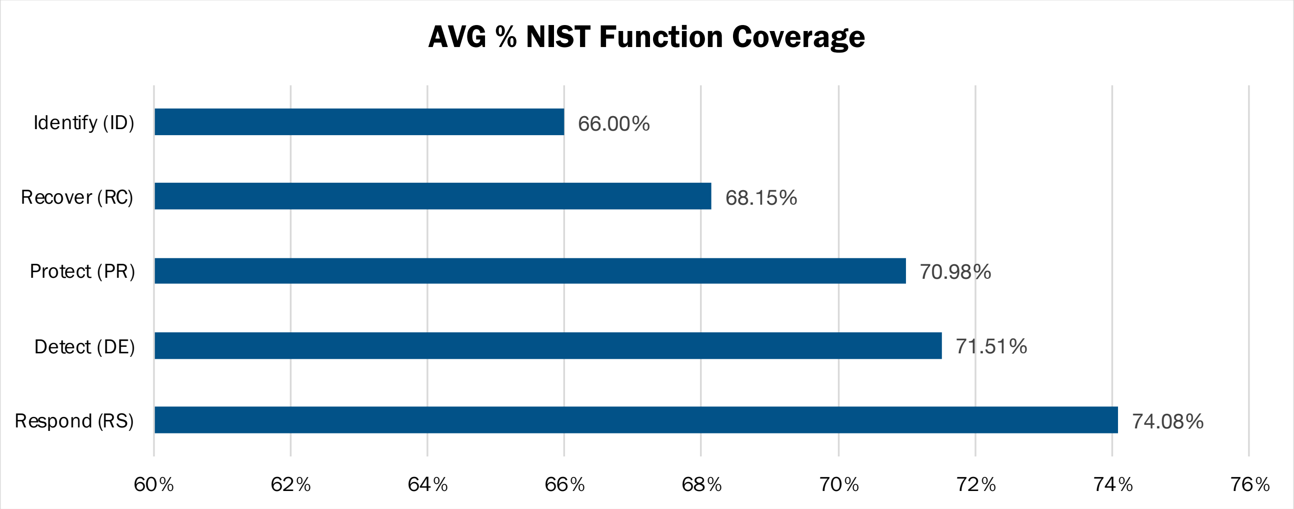
0.80% of revenue, representing a higher share of revenue than what was observed in most medium and large hospitals.

Two outliers existed for large hospitals, which included 1.19% and 1.99 % of revenue invested in cybersecurity. Other than these outliers, the spread for medium and large-sized organizations was nearly identical. This implies that, for more complex hospitals, the size of the organization does not significantly factor into how hospitals invest in cybersecurity. Other factors such as the level of sophistication and awareness of cybersecurity issues by executive leadership and its governing board may determine the level of priority and budget given to cybersecurity.

Industry Coverage to NIST CSF

Based on the Censinet/AHA/KLAS Study, the participating hospitals claim that they provided 70.7% of coverage to the NIST CSF. Based on the NIST Function level, the lowest coverage was Identify (66.0%) and the highest coverage was Respond (74.1%)

Figure 9 NIST Category level percent of coverage



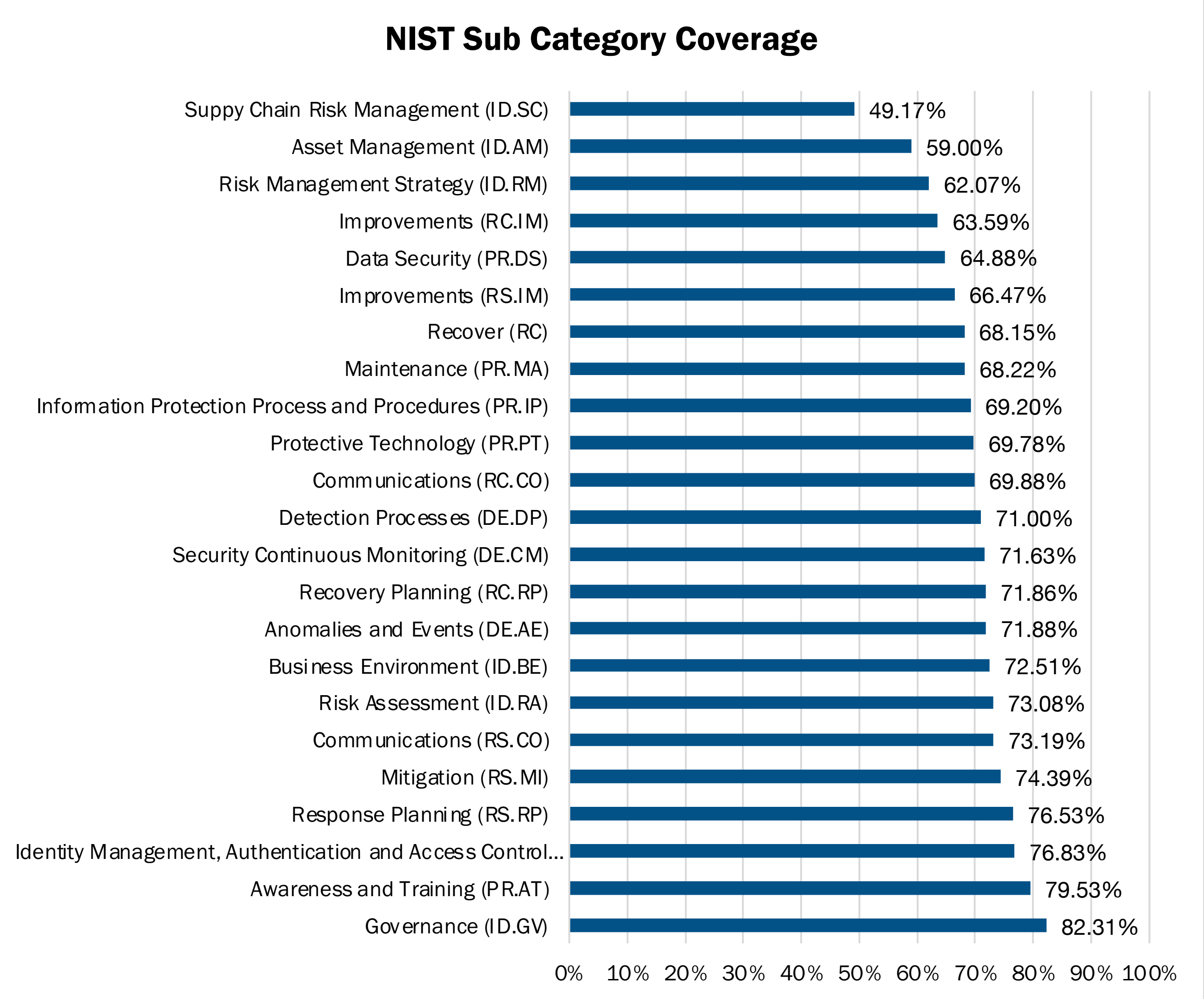
The data was further differentiated at the NIST Category level, with the lowest coverage rates relating to Supply Chain Risk Management and Asset Management, and the highest coverage rates relating to Governance, Awareness and Training, and the analysis conducted in response to incidents.

Further analysis of the Supply Chain Risk Management category shows that hospital organizations were most deficient in their ability to ensure that 1) response and recovery planning and testing was conducted with third-party suppliers (30% coverage) and 2) third-party suppliers are routinely assessed using audits, test results, and other forms of evaluations to confirm they are meeting their contractual obligations (43% coverage).

Further analysis of the Asset Management category shows that hospital organizations were most deficient in their ability to ensure 1) organizational communication and data flows are mapped (39% coverage), and 2) external systems are catalogued (53% coverage).

Hospital organizations struggle with identifying specific communication protocols between themselves and their third-party suppliers at a transactional level. These challenges may imply weakness in the

Figure 10 NIST Sub Category level percent of coverage



ability to protect against cyber-attacks sourced through third-party organizations. We have seen this as a mechanism for attack by adversaries, evidenced by the SolarWinds attack in 2020 and the Kaseya attack in 2021. The SolarWinds attack deployed malware through the software update pipeline and the Kaseya attack leveraged existing IT remote access channels to further penetrate targeted hospital organizations.

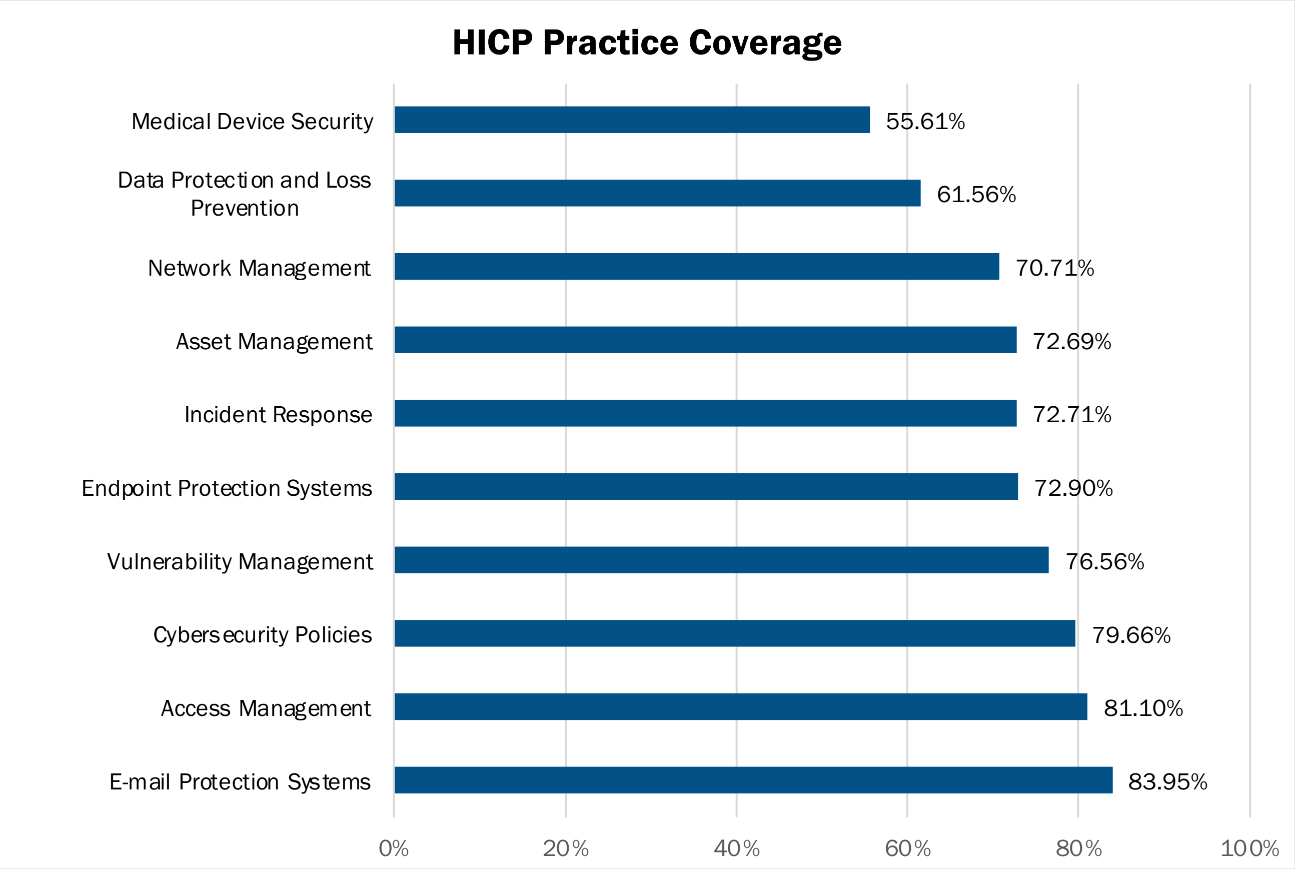
Regarding strengths, hospitals reported high adoption rates of Governance (82.31%) and Awareness and Training (79.53% coverage). Eighty-five percent (85%) of hospitals report that they regularly inform and train their workforce on their cybersecurity-related duties and responsibilities. The data also showed that only 67% of third-party stakeholders understand their cybersecurity roles. Improvement on training to make it current, relevant, and intelligence-based (inclusive of both in-house and external sources), could help improve staff's situational awareness of potential attacks – which could speed up response times. Additionally, training that discusses an attacker's mindset and what type of information they already likely have in their posession (e.g., open-source intelligence) or information they are hoping to get access to could prove useful as well. Such training may provide the requisite perspective to catalyze organizations to re-think their policies on what type of information they are sharing online, hopefully avoiding giving an attacker an added advantage.

Industry Coverage to HICP

Based on the Censinet/AHA/KLAS Study of 2023, on average, hospitals claim to have 72.05% of the HICP practices covered, with email protection being the highest amount of coverage and medical device security being the lowest.

Further analysis of each HICP practice follows within the Landscape Analysis: Practice Adoption section of this study.

Figure 11 HICP average percent coverage by practice



Adoption of HICP Practices

This section includes an in-depth review of the current state of participating hospitals based on the HHS 405(d) Program's HICP publication, established in 2019, pursuant to the Cybersecurity Act of 2015. The 405(d) Program was established by HHS in collaboration with the Department of Homeland Security (DHS), NIST, the HSCC and 200+ cybersecurity and healthcare experts. The HICP publication – a joint partnership publication (between all 405(d) Program partners, as implemented by the HSCC Joint Cyber Working Group) – defines cybersecurity best practices for hospital organizations and OCR considers it "recognized security practices" consistent with Public Law 116-321[20]. HICP is also aligned directly to the NIST Cybersecurity Framework.

This Landscape Analysis used the HICP practices to evaluate the current state of participating hospitals' cybersecurity capabilities. It should be noted that all Data Sources mentioned previously were considered in this analysis. Additionally, CISA's CPGs were mapped to HICP to provide comparative results.

HICP Components with Significant Progress

When conducting the Landscape Analysis, the study team worked to identify both areas of weakness and strengths. The following section outlines areas of strength in cybersecurity capabilities. Minor adjustments in practice deployment might still be needed for continuous improvements.

HICP Practice: Email Protection Systems

CISA Common Performance Goals Mapping: 2.M, 2.N

Overview

Email is a critical communication tool for many organizations, making it an attractive target for cyber-attackers. Implementing email protection controls is essential for ensuring the confidentiality, integrity, and availability of sensitive information. Without these controls, emails can be intercepted, and their contents altered, causing damage to the reputation and financial stability of the enterprise. Phishing attacks and malware delivery can also occur through email, leading to data breaches, loss of sensitive information, and cyber incidents (including ransomware infections) that can lead to operational disruption.

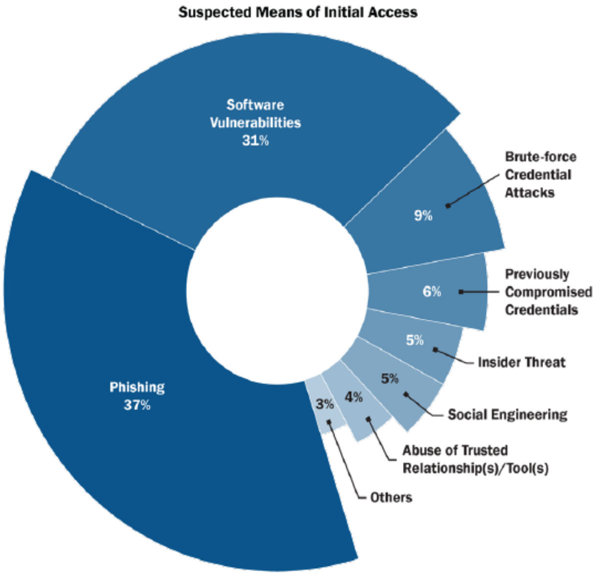
Email protection controls such as spam filters, anti-virus/anti-malware software, encryption, and MFA can prevent these security threats and protect the enterprise from data loss and other negative consequences. Implementing these controls is an important step in maintaining a strong cybersecurity posture and mitigating the risk of cyber-attacks..

Risk Assessment

In the CHIME self-assessment data, 99.2% of participating hospitals reported having some kind of basic spam and phishing protection capabilities in place. This, however, is not something that will prevent more targeted social engineering and phishing attacks from accessing targets through email. H-ISAC reports suggest that phishing and other forms of social engineering continue to make up 37% and 5%, respectively, of the initial means of access.

[20] OCR Recognized Security Practices Video Presentation

Figure 12 Unit42 research presented at H-ISAC on the suspects' means of initial access in healthcare



Based on the Censinet/AHA/KLAS Study, nearly all organizations that submitted results stated that they are 1) providing basic spam and AV protections on their email gateways, 2) applying a tag against messages received from the outside (e.g., "EXTERNAL"), and 3) provisioning every employee with a unique email address. These specific controls can be considered the minimum baseline of email protection, though, by themselves are likely not sufficient to combat the phishing and social engineering threats.

Most organizations (91.96%) have also stated they require MFA for accessing email systems. Business Email Compromise attacks continue to be a persistent problem in this space, whereby a third-party's email system is compromised, and those existing and 'legitimate' email addresses are used to further an attack against a trusted partner of the organization. Mostly used for invoice fraud, these methods can also be used to drop malware inside a hospital's networked environment as a means of bypassing perimeter protections.

91.71% of organizations stated they provide some type of 'URL Click Protection' against incoming links, which is a common defensive technique to identify malicious actions. 86.29% of organizations provide automatic response techniques when phishing or malware have been identified. One type of automatic response could be automatically removing the offending email from the email system. This implies that URL protection and automatic response are core components of email protection for medium and large-sized organizations.

90.36% of organizations also state they conduct phishing training simulations against their organizations, which has largely been considered a best practice.

One weakness uncovered is that 50% of the small hospitals (n=4) stated the use of 'free' or 'consumer' email for their email solution. These solutions might not provide the same level of robust security capability to protect against modern social engineering attacks.

50% of small hospitals reported using "free" or "consumer" email for their email solution.

Even with these defenses, phishing attacks are still successful and the primary attack vector or method into hospitals. This implies that the level of effectiveness of these tools and processes needs to mature.

HICP Components with Urgent Need for Improvement

After conducting the evaluation of threat data in comparison with the cybersecurity capabilities assessments from the CHIME and Censinet/AHA/KLAS studies, the following practices were identified as highest risk and priority.

HICP Practice: Endpoint Protection Systems

CISA Common Performance Goals Mapping: 2.K

Overview

Endpoint protection systems are essential for ensuring the security of an organization's network. An endpoint refers to any device connected to the network, such as a computer, laptop, smartphone, or tablet. These devices are often targeted by cyber-attackers as they can provide a pathway into the network and cause damage.

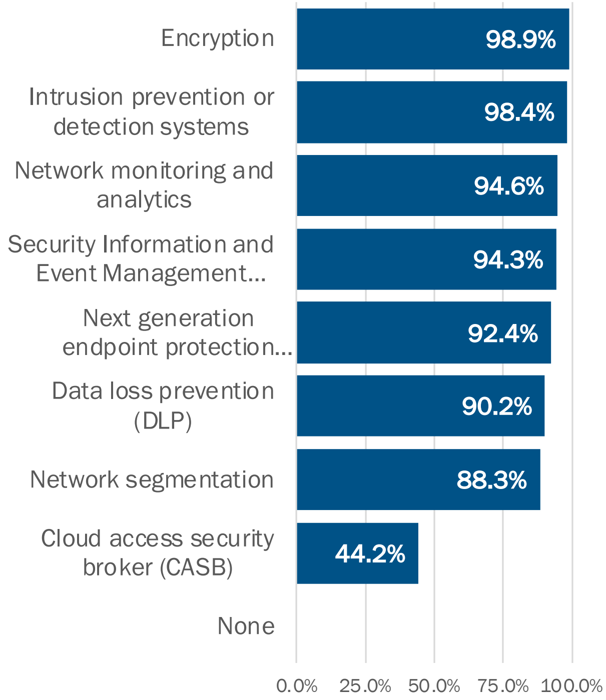
Without endpoint protection, these devices are vulnerable to malware, ransomware, and other security threats. Additionally, a highly effective way to track the inside movement of an adversary is to ensure specific detection tools exist on all endpoints that the adversary might compromise. Endpoint protection systems help prevent phishing and malware dropping related attacks and provide real-time insight to Security Operations Centers (SOCs).

Risk Assessment

CHIME's Most Wired survey suggests that most participating organizations are engaged in some type of endpoint protection tactic such as encryption or an EDR solution.

Based on the Censinet/AHA/KLAS Study, medium and large sized hospitals state that they 1) regularly dispatch field services and support workforce to remediate malware that has not automatically been mitigated (93.57% coverage), 2) regularly patch third-party applications as soon as possible (100%), and 3) dispatch patches to the operating system during regular maintenance (86.96% coverage). 86.86% of large hospitals claim to have implemented EDR tools. EDR tools are critical for identifying initial exploitation attempts and follow-on lateral movement or malicious use of built-in system utilities that may occur as part of an attacker's kill-chain pattern.

Figure 13 CHIME's Most Wired Survey: Technical Security Measures Deployed Across Participating Hospitals



The diversity of endpoint types across hospitals of all types presents a challenge for consistent deployment of endpoint protection mechanisms. Legacy devices that are mission critical are also unlikely to have any such security control deployed on them due to either compatibility issues or the threat of potential downtime. It should also be noted that many medical technologies do not permit the installation of a hospital's EDR toolset. While these studies did not explicitly delineate between legacy IT and other device types (e.g., medical, Operational Technology, Internet of Things), these are necessary to include in broader device protection practices.

HICP Practice: Identity and Access Management

CISA Common Performance Goals Mapping: 2.A, 2.B, 2.C, 2.D, 2.E, 2.H,

Overview

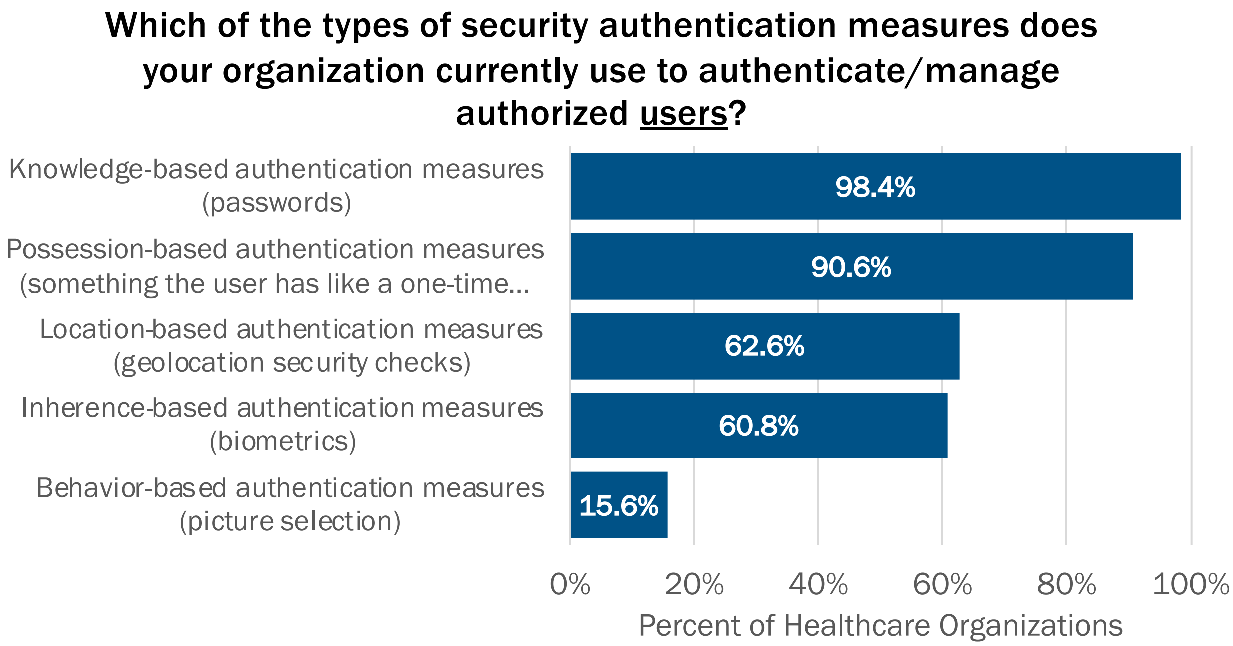
Identity and access management (IAM) is responsible for controlling and monitoring access to sensitive information and systems within an organization. IAM is essential for ensuring that only authorized individuals have access to sensitive resources and that their actions are properly monitored and audited.

Without proper IAM controls in place, organizations are vulnerable to unauthorized access, data breaches, and other security incidents. IAM solutions help prevent these incidents by providing a centralized system for managing identities, controlling access, and enforcing security policies.

Risk Assessment

Despite these claims, we continue to see a majority of successful attacks against hospitals where a single credential stolen from a phishing attack was the key vector used. This implies that although MFA might be deployed in some systems, it is not universally deployed on the most critical entry points. This could also mean that the MFA (even if deployed using an industry recommended implementation) may still be subject to replay attacks, making these threats credible. Replay attacks, according to NIST, are

Figure 14 Various Forms of authentication used by organizations



described as attacks that involve the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access. Additionally, new threat intelligence suggests that threat actors are using more sophisticated types of social engineering attacks to bypass MFA. Examples of these attacks include social engineering where users are duped into sharing one time MFA passcodes, or where users are overwhelmed with MFA notification requests until they eventually accept the request.

Furthermore, evidence suggests that attackers may use legitimate credentials or may be ‘living off the land’, which refers to the use of dual-use tools. The threat of legitimate credentials being used is concerning when only 80.63% of the hospitals have reported that they have a privileged access management program in place.

HICP Practice: Network Management

CISA Common Performance Goals Mapping: 2.F, 2.P, 2.W, 2.X

Overview

Network management helps ensure the reliability, security, and performance of the network. This could be on-premises networks, datacenters that are managed, or infrastructure-as-a-service (IaaS) environments from cloud providers like Amazon Web Services, Microsoft Azure, and Google Cloud Platform. From a cybersecurity perspective, having proper network management controls in place is essential for maintaining the confidentiality, integrity, and availability of sensitive information. In the context of a hospital, network management is inclusive of proper segmentation and resiliency planning.

Risk Assessment

The CHIME Most Wired self-assessment data on IT asset management referenced 91% of participating organizations monitoring devices on their networks, yet only 52.6% having an inventory of personal devices on the network. This disparity is suggestive of coverage gaps in network monitoring controls where they only run on specific network segments. The study cited 88.3% of organizations are implementing some form of network segmentation. Within the Censinet/AHA/KLAS Study, only 52.05% of hospitals stated they segment their vendor connections into their network. Knowing that a common attack vector is through third-party suppliers, this weakness suggests that hospitals are vulnerable via the third-party supplier link. Additionally, only 49.55% of hospitals stated they apply network segmentation strategies for their data centers. This might make it more difficult for hospitals to limit the spread of lateral movement and cyber-attacks against their key mission critical systems.

91% of participating organizations monitored devices on their way to networks yet **only 52.6% have an inventory of personal devices** on the network.

The significant impact associated with ransomware attacks in hospital networks suggest that these controls, if implemented, would address a broader mitigation strategy. Leveraging zero-trust oriented micro-segmentation strategies should be considered as well. Any segmentation would need to be coupled with authentication and authorization mechanisms to control lateral movement between segments.

Regarding cloud services and their ability to help enhance cyber resiliency, we learned from hospitals we spoke with that there is a general concern that cloud service costs are becoming unaffordable. Some hospitals are not prioritizing use of cloud services due to constrained budgets even if they have policies in place promoting its use to increase cyber resiliency. Some are choosing to use cloud services in limited capacities, and only for applications that are not frequently used as opposed to critical business functions, in order to optimize their limited IT and cyber budgets.

Many hospitals discussed networking challenges associated with providing non-acute services to patients in their home (often referred to as 'Hospital-at-Home'). Medical devices and other technologies are typically installed in the home or connected to patients to share vital telemetry data and other information with medical professionals. Some of these devices are antiquated, do not possess the latest software updates or patches, lack proper security controls, and if exploited could serve as an entry point into a hospital's secured network. More details regarding this issue are discussed under HIPC Practice 9: Network Connected Medical Device Security.

HICP Practice: Vulnerability Management

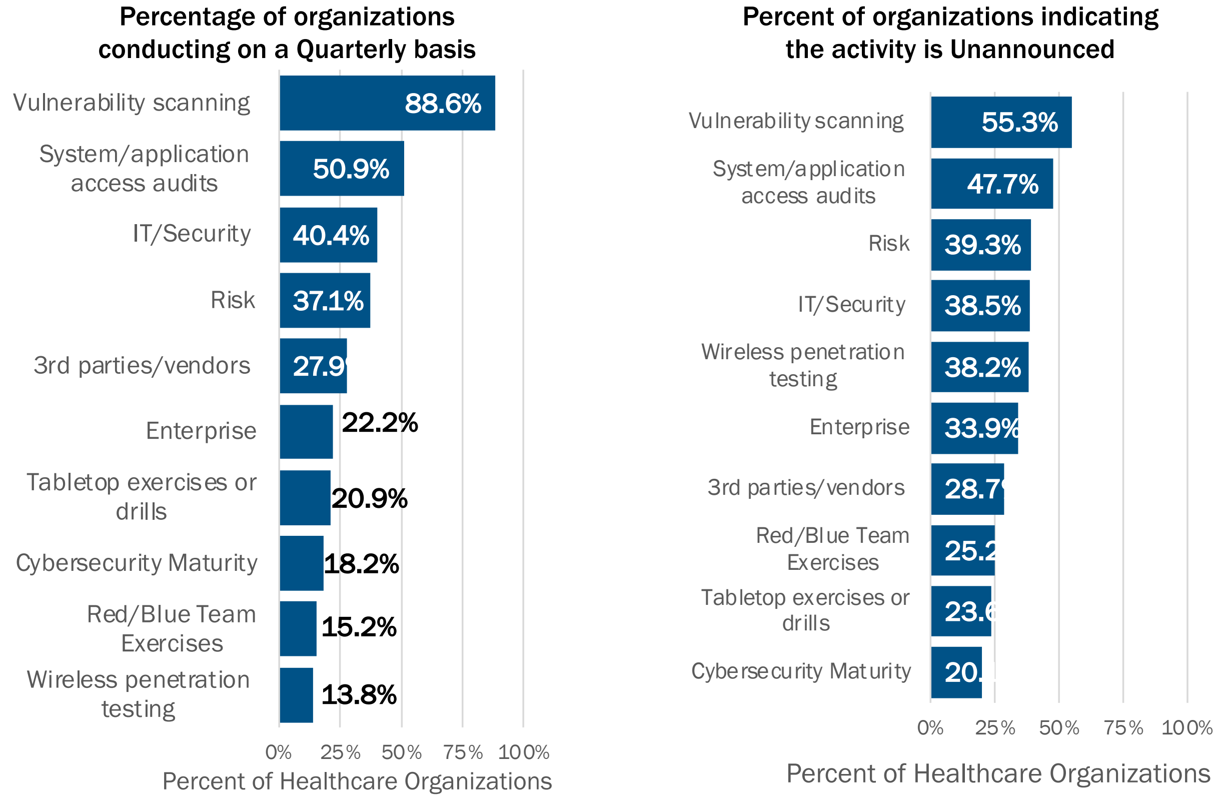
CISA Common Performance Goals Mapping: 1.E, 1.H, 4.B,

Overview

Vulnerability management is the process used by organizations to detect technology flaws that hackers could exploit. This process uses a scanning capability, often provided by an EMR or IT support vendor, to proactively scan devices and systems in an organization.

Without regular vulnerability scans on servers, applications, and third-party software, it is difficult to identify technology flaws that can be routinely patched. Typically, non-medical device patches are

Figure 15 Vulnerability Management



distributed by the vendor community on an as needed basis, but most critical vulnerabilities receive patches within 14 days.

Risk Assessment

The CHIME Most Wired data shows that there is generally a substantial number of hospitals conducting regular vulnerability scans. Typically, for organizations that may be at higher risk of exploitation (hospitals), the recommended cadence may be twice per week. The low percentage of hospitals using advanced forms of testing, like Red Team, Purple Team and Tabletop exercises to uncover technical flaws in their defenses is a major concern. To uncover advanced attacks such as ransomware, higher forms of assessment testing (those with a higher degree of effectiveness than a typical scan) are necessary. Assessment testing must complement an active vulnerability scanning regimen. Furthermore, when vulnerabilities are identified, it is just as important to have processes in place to mitigate those prioritized risks based on the threat, probability of occurrence, and organizational impact.

The IBM Cost of a Data Breach in 2022 Report provides key considerations relating to vulnerability management. These suggest that it can take 207 days to discover a breach and an additional 70 days to then contain it. According to IBM, shortening the time it takes to identify and contain a breach to 200 days or less will not only improve cyber resiliency but can save an average of $1.12M (26.5% cost reduction).

It can take **207 days to discover a breach** and an additional **70 days to contain it.**

HICP Practice: Security Operations Center and Incident Response

CISA Common Performance Goals Mapping: 1.G,2.G, 2.S, 2.T, 2.U, 3.A, 4.A, 5.A,

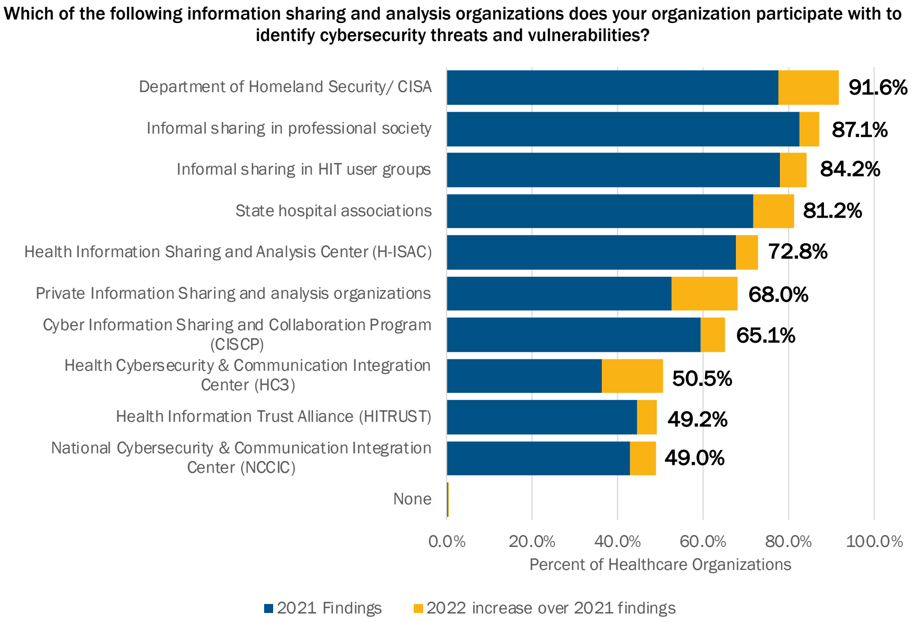
Overview

The CHIME Most Wired data suggests that the vast majority of hospitals, from small to large, are participating with DHS/CISA's threat indicator sharing programs. CISA provides two levels of access to threat intelligence sharing: 1) Automated Indicator Sharing (AIS) Program (which CHIME Most Wired indicates 91.6% of hospitals are participating), and 2) Cyber Information Sharing and Collaboration Program (CISCP) vetted community (which CHIME Most Wired indicates 65.1% of hospitals are participating). As shown below, across both sharing communities, hospitals self-report that more than 56.7% are participating in both. Additionally, CHIME Most Wired reports 72.8% are participating in H-ISAC community sharing. There is a 42% difference in H-ISAC participation between small and large-sized participating organizations.

The ability to share near real-time information about threats, threat actors, and their techniques is integral to providing an active defense. Based on hospital conversations, it appears they may tend to limit information sharing when faced with a cyber incident due to critical concern for regulatory enforcement and legal actions from customers and other affected parties. Organizations are protected under 6 U.S.C. 1505, which provides for liability protection when sharing meets certain requirements.

Congress is pursuing improved information sharing of cyber incidents through the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Rulemaking to CIRCIA is still underway, however currently it requires that a "covered entity" report a "covered cyber incident" to CISA no later than 72 hours after the covered entity "reasonably believes that the covered cyber incident has occurred. Additionally, "a covered entity that makes a ransom payment as the result of a ransomware attack

Figure 16 CHIME Survey Information and Analysis used by Organizations



Limited IT Scalability (N = 52)	Medium IT Scalability (N = 223)	Great IT Scalability (N = 95)	MAX-MIN
85%	90%	99%	14%
79%	85%	97%	18%
81%	84%	87%	7%
83%	83%	76%	7%
46%	70%	93%	46%
60%	63%	82%	22%
60%	61%	77%	17%
33%	47%	69%	37%
42%	52%	45%	10%
38%	48%	60%	22%

against the covered entity shall report the payment to the Agency [CISA] not later than 24 hours after the ransom payment has been made." Furthermore, "information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Agency [CISA]" through the obligations of CIRCIA cannot be used to "regulate, including through an enforcement action" by federal, state, local or tribal governments, "unless the government entity expressly allows entities to submit reports to the Agency to meet regulatory reporting obligations of the entity. For example, CISA must share "covered cyber incident" information with relevant federal agencies within 24 hours and federal agencies must share "cyber incident" information they receive with CISA within 24 hours.

It remains to be seen exactly how CIRCIA will impact information sharing. Regardless, an opportunity for downstream sector protection is lost if the intelligence gathered from the critical incident is not shared back through appropriate channels, such as the CISA AIS Program and H-ISAC. Outside of reporting required under CIRCIA, once it is implemented, hospitals may have other mandatory reporting obligations and voluntary reporting opportunities.

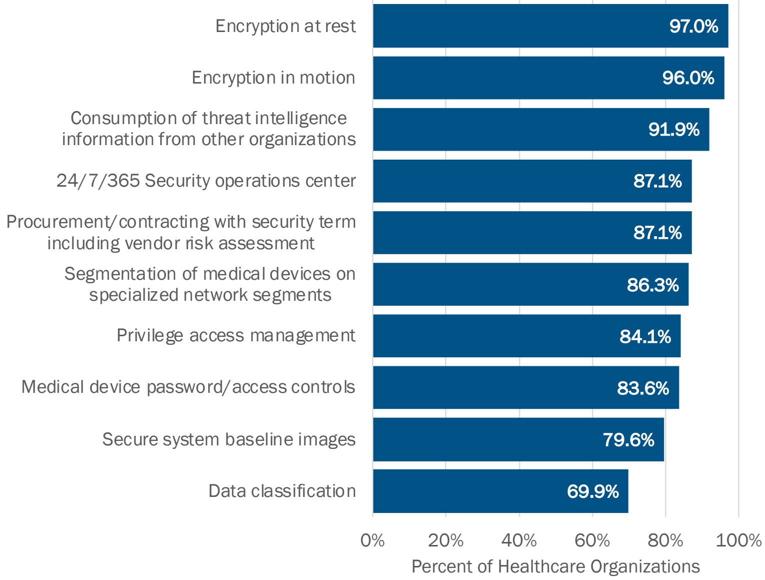
Further analyzing the CHIME Most Wired Survey, 87.1% of hospitals (and 76% of small hospitals) report they are running a 24x7x365 SOC. Furthermore, 91.9% of hospitals stated they are actively consuming threat feeds noted above, with 83% of small hospitals stating the same. It's unclear based on this data whether this is outsourced using a managed-security-services-provider (MSSP) or managed in-house.

Risk Assessment

At first glance, both the participation of information sharing and the 24x7 operations of these SOCs suggest hospitals are doing well defending against this space. However, despite these claims of full coverage, hospital conversations uncovered that these operations are not at a sufficient level of maturity due to the lack of resources, both fiscal and human. Discussions with participating hospital security personnel clarified that threat sharing programs they participate in are cumbersome, oftentimes offering largely duplicative information, with little to no unique value per feed. Ingesting this data is also separate

Figure 17 CHIME Survey Security Processes

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



	Limited IT Scalability (N = 52)	Medium IT Scalability (N = 223)	Great IT Scalability (N = 95)	MAX-MIN
Encryption at rest	96%	97%	99%	**3%**
Encryption in motion	90%	96%	99%	**9%**
Consumption of threat intelligence information from other organizations	79%	92%	99%	**20%**
24/7/365 Security operations center	77%	86%	95%	**18%**
Procurement/contracting with security term including vendor risk assessment	75%	87%	94%	**19%**
Segmentation of medical devices on specialized network segments	96%	85%	86%	**11%**
Privilege access management	85%	81%	93%	**11%**
Medical device password/access controls	77%	84%	85%	**8%**
Secure system baseline images	69%	78%	88%	**19%**
Data classification	62%	68%	79%	**17%**

from being able to act on it in a timely way. If a given hospital can't make changes to an environment, such as isolating systems, patching systems, or rotating credentials quickly, this threat data may not be adding much value in terms of risk mitigation.

When further determining incident response capabilities of organizations, the Censinet/AHA/KLAS Study indicates the use of deception technology (which aims to deceive attackers by distributing a collection of traps and decoys) has not been well adopted, with only 28.28% of coverage. Additionally, automated techniques for playbook execution, through tools like Security Orchestration, Automation and Response (SOAR), have only achieved 41.86% of coverage. 73.13% of hospitals state they participate in an ISAC or an Information Sharing and Analysis Organization (ISAO) such as H-ISAC. 88.14% of hospitals state they have 24x7x365 covered SOCs being staffed and monitored. This is consistent with the answers provided in the CHIME Most Wired Survey.

73.13% of hospitals state they participate in an ISAC or ISAO, such as H-ISAC.

Through discussions with participating hospitals, it was discovered that some crisis management processes are being utilized to deal with large scale breaches or operational disruptions caused by advanced attacks, like ransomware. In most cases, the hospitals did not have a formal crisis management plan in place to deal with large scale cyber events that affect the entire organization, other than business continuity and disaster recovery plans. However, many of them conduct after-action exercises, and have made changes to their operations as a result of prior incidents, hoping to better prepare themselves for future events should preventive controls fall short of expectations. Interestingly, a few hospitals mentioned that their insurance carrier offered consultation services to assist with breach notification, press releases, brand restoration, and other legal issues. Some mentioned having inter-departmental teams made up of officials (from HR, media relations, privacy, legal, finance and acquisitions) that are consulted on major cyber events or issues. These teams also help cyber teams by developing policies, procedures, and mechanisms to scale resources if (and when) a major cyber event occurs. Many of them welcomed more assistance and informational resources in preparing a formalized plan from both peers and the U.S. government..

HICP Components in need of additional research/follow-up

After conducting the evaluation of threat data in comparison with the cybersecurity capabilities assessments from CHIME and Censinet/AHA/KLAS, the following practices were identified as potential risks for further consideration.

HICP Practice: IT Asset Management[21]

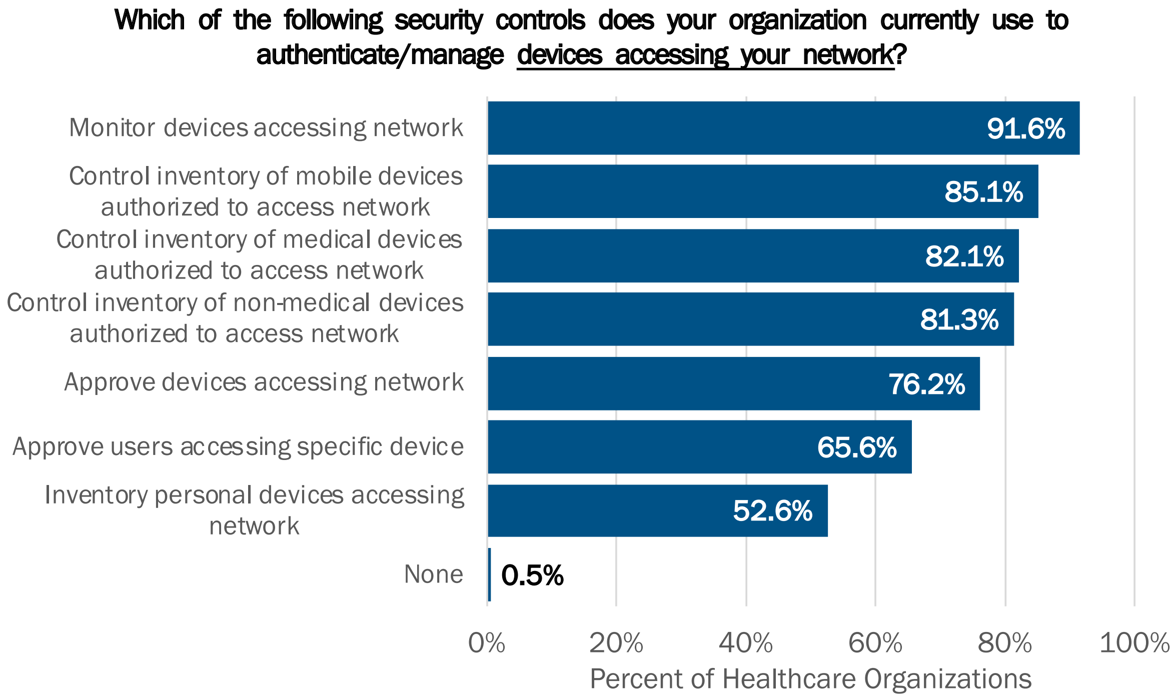
CISA Common Performance Goals Mapping: 1.A

Overview

Asset management helps ensure the proper tracking, maintenance, and utilization of physical assets. Organizations cannot protect assets that they do not know about or to which they have no means of administrative oversight. From a cybersecurity perspective, having proper asset management controls in place is essential for maintaining the confidentiality, integrity, and availability of sensitive information.

Without proper asset management controls, hospital organizations are at risk of mismanagement and waste of technology resources, as well as non-compliance with software licensing agreements and other regulations. This can result in increased costs, decreased efficiency, and increased risk of security incidents.

Figure 18 Device Monitoring on Hospital Managed Networks



[21] Cybersecurity Framework | NIST

Risk Assessment

Asset management is a foundational cybersecurity activity that feeds into other capabilities such as vulnerability management and incident response. If this activity is not in place with a certain level of maturity, there will be significant limitations incurred across the cybersecurity program.

The CHIME Most Wired data shows that there is generally some kind of device monitoring on hospital managed networks (**Figure 19**, below). The Censinet/AHA/KLAS Study indicates that 84.11% of hospitals have inventoried the endpoints and servers in their organization. Connecting this monitoring with a more structured inventory (e.g., asset management) lacks capability. It is unclear from this data set whether there are criticality ratings applied within the context of a given asset class.

HICP Practice: Cybersecurity Oversight and Governance

CISA Common Performance Goals Mapping: 1.B, 1.C, 1.F, 1.G, 1.H, 1.I,2.I, 2.J

Overview

Establishing and implementing cybersecurity policies, procedures, and processes is one of the most effective means of preventing cyber-attacks. They set expectations and foster a consistent adoption of behaviors by the workforce. With clearly articulated cybersecurity policies, employees, contractors, and third-party vendors know which data, applications, systems, and devices they are authorized to access and the consequences of unauthorized access attempts.

According to the CHIME Most Wired survey, 70.7% of hospitals are leveraging Governance, Risk, and Compliance (GRC) systems. These systems help organize both policy controls, risk assessments and registers, and controls implemented in hospital environments. Proper use of these systems can simplify risk management.

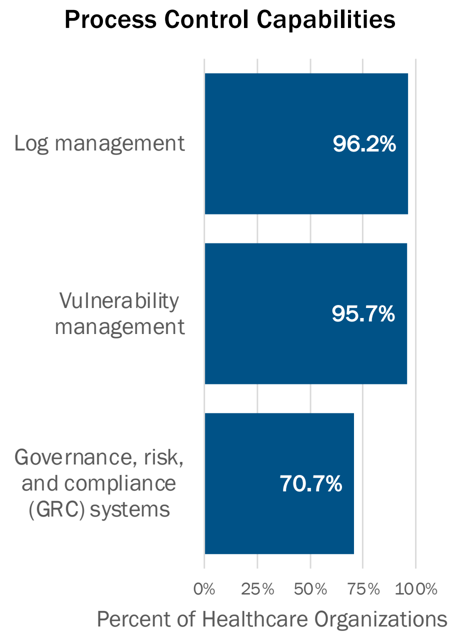
It is common for hospitals to leverage a framework to define their cybersecurity program. The NIST CSF continues to be the most popular framework (by nearly double).. The second most popular framework is SANS Top 20 critical controls.

The frequency of meetings with the board, or committees of the board, as well as management through formally charted cybersecurity committees are another measure of maturity. The majority of hospitals meet with a committee of the board on a quarterly basis. The vast majority of management meets in formally chartered cybersecurity committees.

Risk Assessment

Effective cyber security and risk programs typically flourish and are more resistant to attacks in organizations that have a strong governance and policy framework, as well as corresponding commitment from leadership. Data suggests that some hospitals may be falling short of expectations regarding established

Figure 19 Process control capabilities



GRC programs, with only 70% reporting a GRC system is currently in place today. For those reporting use of a GRC tool, most indicated the use of NIST CSF which is a common and well recognized standard in cybersecurity.

Figure 20 Security Frameworks used by organizations

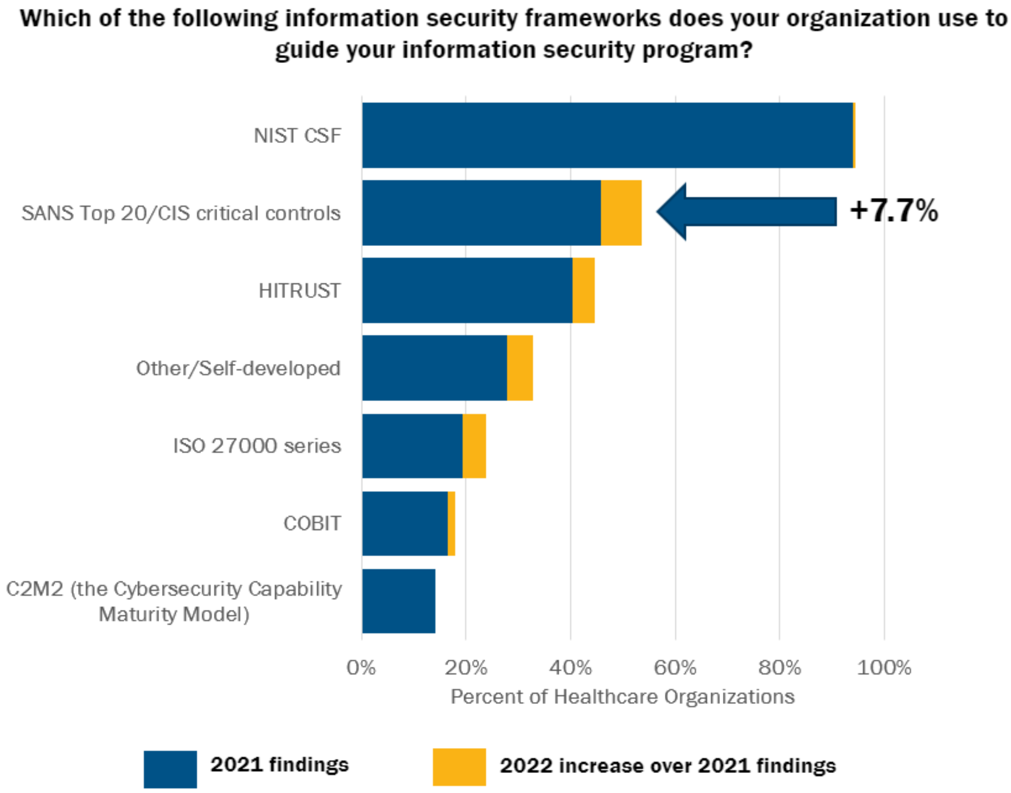
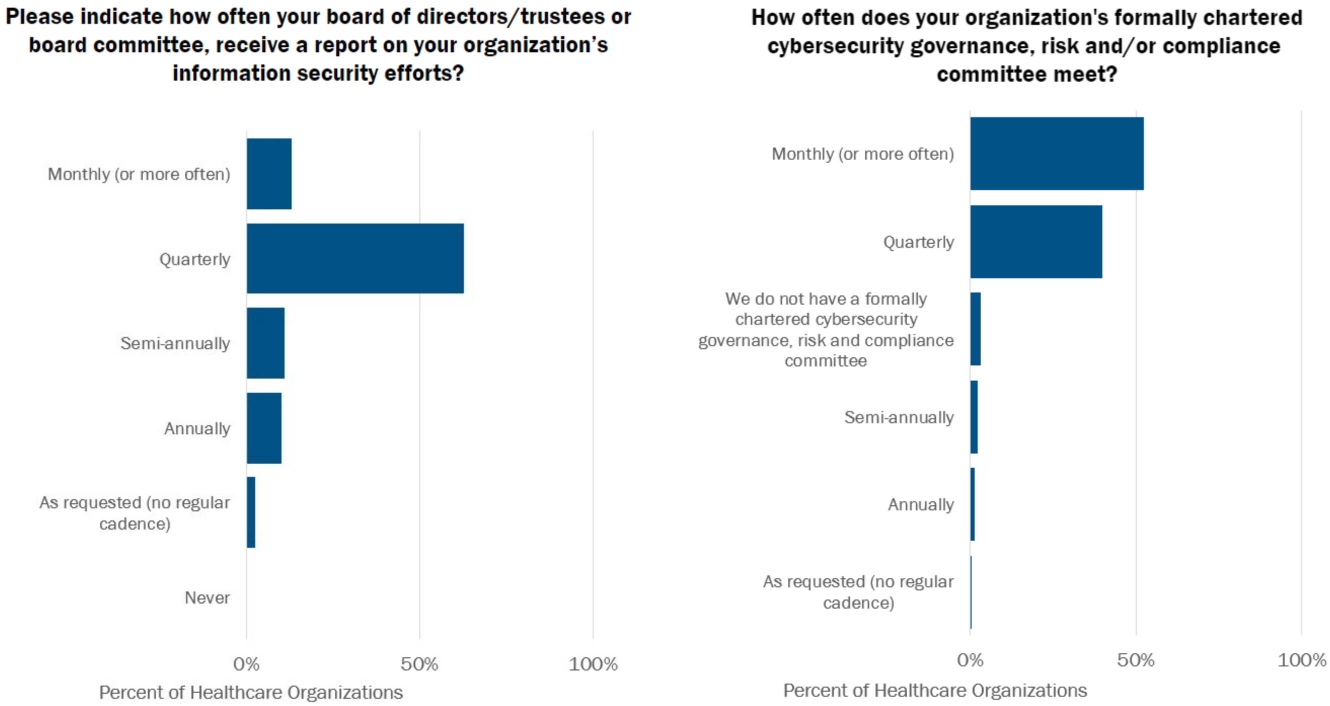


Figure 21 Cybersecurity Maturity of organizations

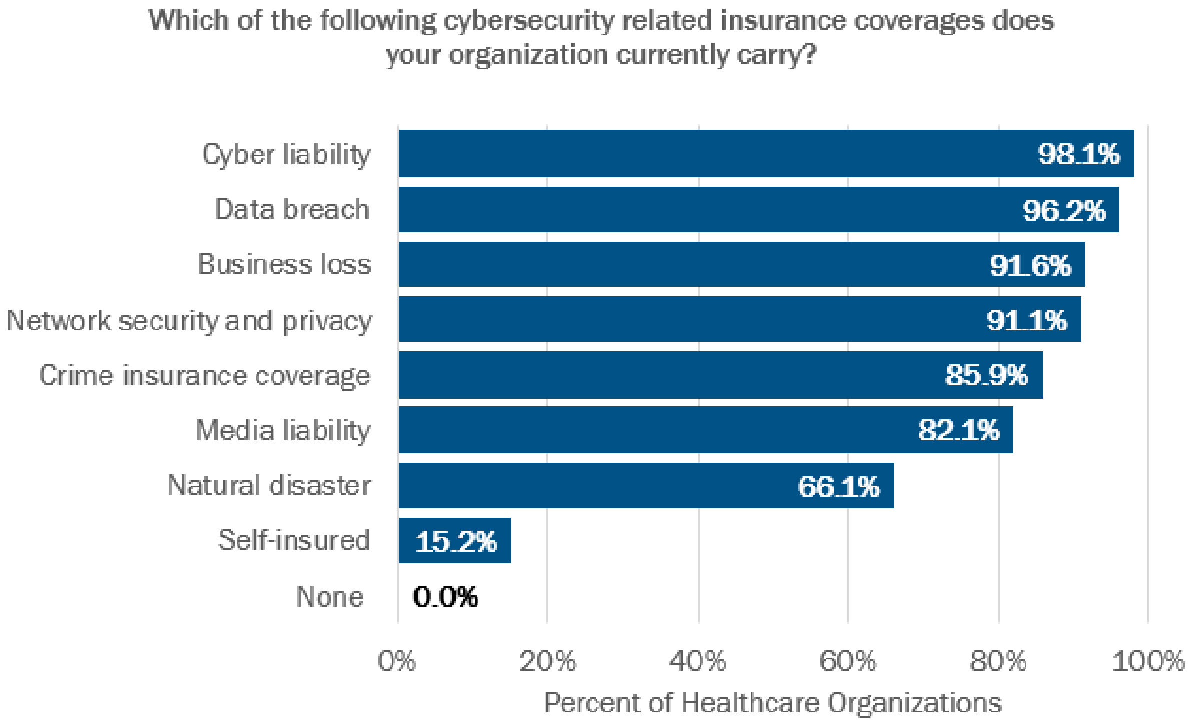


To promote faster Observe, Orient, Decide, Act[22] (OODA) loops, or a hospital's ability to respond to attacks, quarterly reporting of risks and overall compliance to leadership and executive boards may be needed. A faster cadence on reporting should be considered, especially for hospitals that have a higher risk of exploitation. This will enable corrective actions (which require funding or the re-directing of resources) to be taken in a timely manner.

Many of the hospitals mentioned improved programmatic and budgetary support from their boards in the past three (3) to– five (5) years for cybersecurity activities. As more crippling cyber-attacks impacting hospital operations are disclosed, many remarked their boards are asking good questions about resiliency and recovery activities. Many hospitals mentioned that their boards are participating in risk management activities, and treating cybersecurity as enterprise, strategic risk. Despite these improvements, several hospitals mentioned the need for better informational resources and guidance documents to aid their board's role in cyber governance. Peer-based benchmarking data was mentioned as one informational source that is useful but still lacking.

Despite **Figure 22** demonstrating a large amount of coverage, during hospital conversations challenges associated with both acquiring and retaining coverage were discovered. During these conversations it was stated the insurers expect a more mature program for underwriting a program. Based on the Censinet/AHA/KLAS Study, there has been a 46% increase in insurance premiums for large-sized hospitals and a 50% increase for medium-sized hospitals. The data on small hospitals was not statistically significant and did not correlate with what we learned through interviews (i.e., only 3 small hospitals provided cyber insurance premium increases). There is also a presence of medical service,

Figure 22 Cybersecurity related insurance coverages



[22] The Cyber OODA Loop: How Your Attacker Should Help You Design Your Defense | NIST

property damage, and exclusion of specific entities (such as hospitals) from coverage eligibility. Policies are sometimes viewed as “stop gaps” to cover major or unforeseen, rare cyber events.

Additionally, many hospitals indicated that total policy coverage amounts have significantly decreased in recent years, despite increases in policy premiums. Hospitals feel they are paying more and getting less coverage. Some hospitals that possess sufficient financial resources are electing to self-insure, as the cost of having insurance coverage have outweighed the benefits. Those hospitals that are unable to self-insure are using renewal periods as an opportunity to secure a cheaper premium with another insurance company, but fewer options are available as many insurance companies are choosing not to offer cyber liability coverage.

Hospitals we spoke with also indicated that policy exclusions tied to minimum cyber standards of practice are affecting the adequacy of coverage, with the impact being felt the most by smaller, rural hospitals that lack sufficient funds and cyber talent to meet those prescribed standards. Some small, rural hospitals mentioned that they are unable to meet some minimum standards because of the potential impact on patient care or safety. Many of these hospitals are using older devices and technologies in the delivery of care that are fully functional and acceptable, but incompatible with some of the more advanced cyber standards. Constrained budgets are preventing many of them from replacing old equipment, forcing hospitals to choose to suspend meeting a cyber standard to deliver necessary care to their patients.

Regarding claims experience, some hospitals had submitted claims in the past for cyber events. Some claims were paid, and others were not due to policy exclusions. The hospitals also had indifferent opinions about the quality of service provided by insurers. Some had great experiences filing claims and others’ experiences fell short of expectations.

HICP Practice: Network Connected Medical Device Security

CISA Common Performance Goals Mapping: 1.D, 1.E, 2.F, 4.B

Overview

Medical devices are essential to diagnostic, therapeutic and treatment practices. These devices deliver significant benefits and successfully help treat many medical disorders. As with all technologies with the ability to connect to the internet, medical devices with such connectivity may have cybersecurity vulnerabilities.

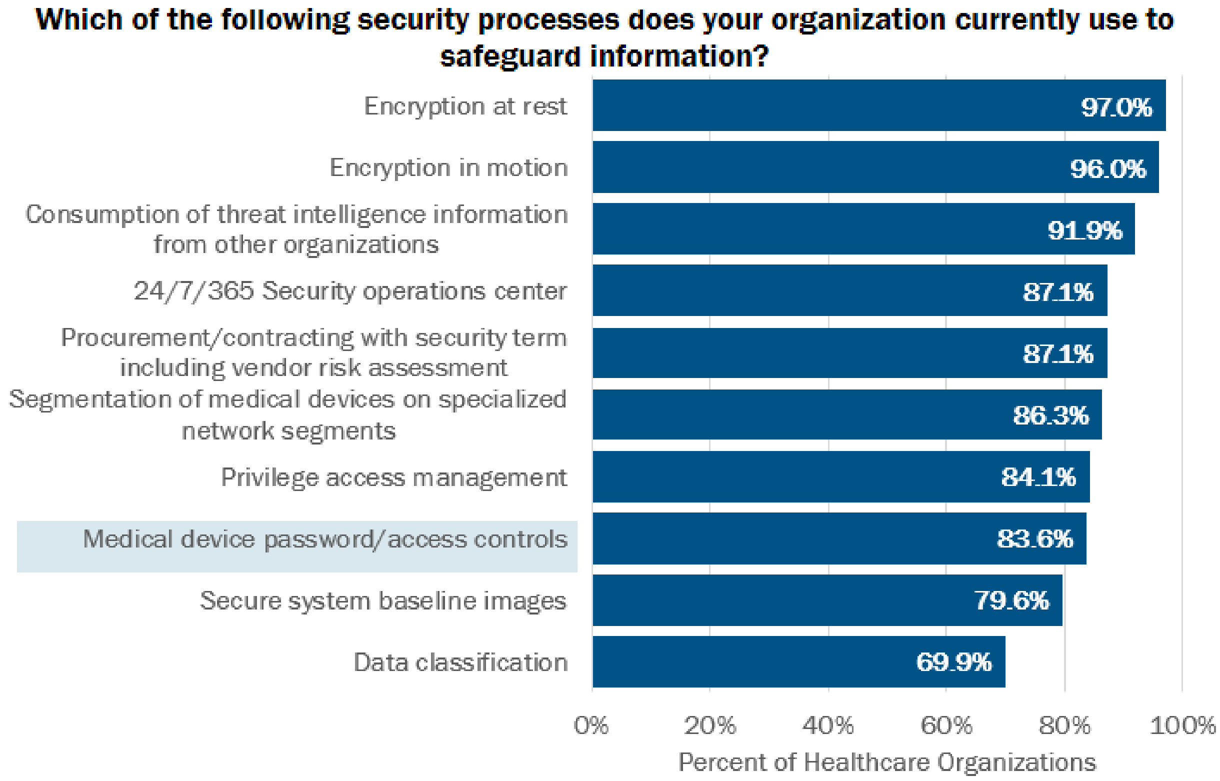
Cybersecurity vulnerabilities are introduced when medical devices and technologies are connected to a network or computer. To protect patients, it is important to protect these devices. Hospitals are encouraged to extend the relevant cybersecurity practices and implement them appropriately for medical device management

Risk Assessment

52.41% of hospitals state they **segment their medical technology** off from general access network.

In addition to **Figure 23** and **Figure 24** above, the Censinet/AHA/KLAS Study shows that 59.64% of medical technology in use in hospitals have some kind of Anti-Virus solution, or other compensating control. Additionally, 60.18% of hospitals also state they routinely patch medical technology when a patch is released by the manufacturer. Lastly, 52.41% of hospitals state they segment

Figure 23 Security Processes used by organizations



their medical technology off from general access networks. These basic hygiene controls demonstrate there are still significant challenges with medical technology security.

While available data on cybersecurity incidents do not appear to show that medical device vulnerabilities fall in the category of the most-common exploit vectors, medical devices play an essential role in the delivery of care in hospitals. Disruption to such devices have significant safety and operational impacts, and exploitation of medical device vulnerabilities have previously occurred. For public safety, it is essential that medical devices are safe, effective, and their security appropriately managed in the hospital ecosystem.

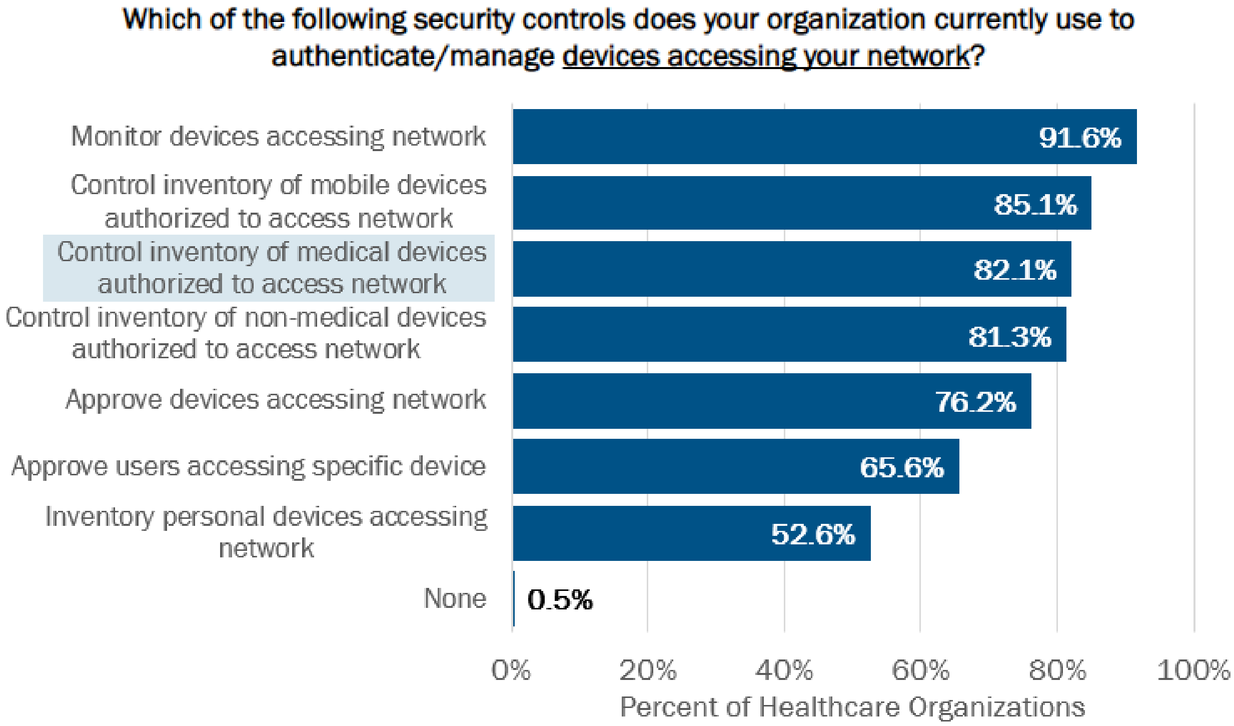
Vulnerability management tools can deploy agents on endpoints or allow for scanning against the endpoint itself. Certain endpoints, such as medical devices, cannot have standard cybersecurity tools deployed to them without violating the warranty of the endpoint. In these circumstances, the hospital might have limited visibility.

Section 524B of the FD&C Act requires the sponsor of any premarket application or submission for a "cyber device" to comply with certain cybersecurity requirements. FDA provides premarket and post-market guidance regarding the cybersecurity recommendations of medical devices for medical device manufacturers. This guidance may be useful for healthcare delivery organizations to review, along with recommendations provided by the Healthcare and Public Health Sector Coordinating Council (such as HSCC's Medical Device and Health IT Joint Security Plan) and other sector entities regarding the appropriate management of cybersecurity risks for medical devices when implemented in the healthcare and hospital settings.

Additionally, section 3305 of the Consolidated Appropriations Act, 2023 amended the Federal Food, Drug and Cosmetic Act (FD&C Act) to add section 524B and requires the sponsor of any application or submission for pre-market approval for "cyber devices" to comply with certain cybersecurity requirements. Specifically, sponsors must submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, post-market cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures. Sponsors must also design a process to make sure that their devices and related system are cybersecure, which include post-market updates and patches. Cyber devices must also have a Software Bill of Materials (SBOM)provided to the Secretary which includes off-the shelf, open source and commercial components.

Through discussions with a few hospitals, it was discovered that a significant medical device security challenge changing the cyber threat landscape is tied to Hospital-at-Home services. Hospital-at-home care delivery typically requires use of medical devices and technologies in patient's homes to communicate, monitor and report information about their care with medical professionals. Since COVID-19, and with advances in medical technology, these services are growing and expanding as more patients are requesting care delivery in their homes. Several hospitals mentioned Hospital-at-Home as their IT and cyber team's top priority for enhancing cyber resiliency. Some of the security concerns mentioned with these services included IAM with devices in the home, vendor lock-in, software costs, and being more self-reliant to manage services inhouse. These challenges are exacerbated in rural communities where communication bandwidth is often limited, frequent internet outages occur, and lack of inhouse cyber expertise to implement adequate controls[23].

Figure 24 Security Controls to manage/authenticate network access



[23] Medical Joint Device And Security Health Plan It 2019

HICP Components Where Further Attention is Recommended (Not Urgent)

After conducting the evaluation of threat data in comparison with the cybersecurity capabilities assessments from CHIME and Censinet/AHA/KLAS, the following practice was identified as a potential risk, though from the perspective of patient safety and harm, was not deemed as urgent.

HICP Practice: Data Protection and Loss Prevention

CISA Common Performance Goals Mapping: 2.R

Overview

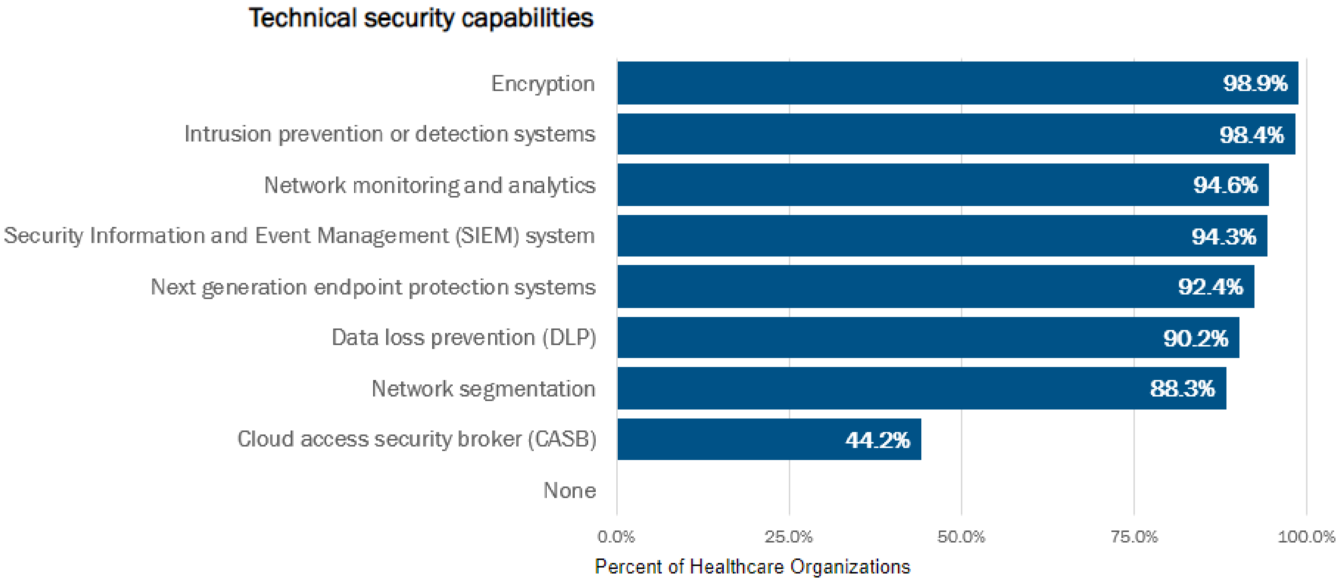
Data protection and loss prevention (DLP) is responsible for ensuring the confidentiality, integrity, and availability of sensitive information. This includes protecting sensitive data from unauthorized access, theft, and loss, as well as ensuring that critical information is available to authorized users when it is needed.

Without proper DLP controls in place, organizations are vulnerable to data breaches, theft, and loss, which can result in damage to reputation, financial losses, and loss of customer trust. DLP solutions help prevent these incidents by providing a centralized system for monitoring, controlling, and protecting sensitive information.

Risk Assessment

The data suggests that a substantial percentage of hospitals are reporting the use of DLP tooling. An attacker could use medical information that is leaked to exploit a patient or use information to change a medical record which could manifest in any number of nefarious ways, for example, a wrong prescription drug administered to a patient, or a patient receiving a wrong dosage – both could have significant impact on patient care outcomes. If the exploitation was leaked and made public, it could create fear and mistrust within the general patient population of a hospital – ultimately affecting the reputation of the facility. It is noted that this theoretical attack has not been witnessed in any conversation or study and is only considered a potential risk.

Figure 25 Technical Security Capabilities



Appendix A: 405(d) Program and History

Cybersecurity Act of 2015: Task Group Undertakes a Legislative Mandate

The CSA became law in 2015. As illustrated in **Figure 26**, within this legislation is Section 405(d): Aligning Healthcare Industry Security Approaches. In response to the CSA Section 405(d) requirement, HHS leveraged the HPH sector's Critical Infrastructure Protection Advisory Council (CIPAC) framework to establish the 405(d) Task Group. To learn more about this important partnership, please visit ASPR's Division of Critical Infrastructure Protection.

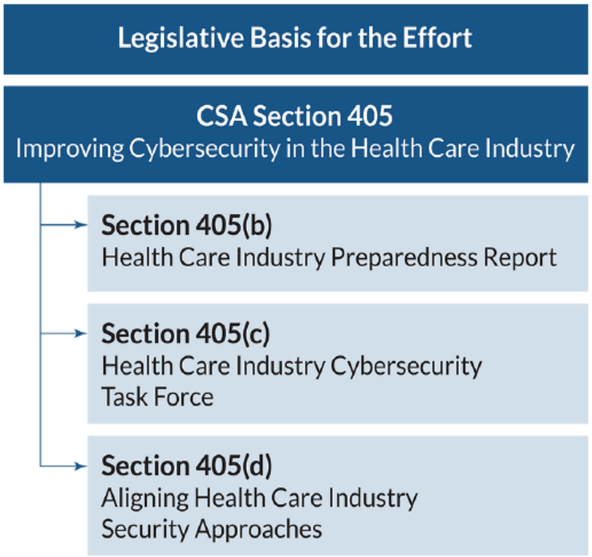
HHS convened the Task Group in May 2017 to plan, develop, and draft this guidance document. To ensure a successful outcome and a collaborative public-private development process, HHS engaged a diverse group of healthcare and cybersecurity experts from the public and private sectors. In 2023 the 405(d) Program released an update to the HICP publication.

HHS collaborated with the HPH Sector Government Coordinating Council, the HPH Sector Coordinating Council, DHS, and NIST.*

The Task Group's approach to the guidance document:

1. Examines current cybersecurity threats affecting the HPH sector;
2. Identifies specific weaknesses that make organizations more vulnerable to the threats; and
3. Provides selected practices that cybersecurity experts rank as the most effective to mitigate the threats.

Figure 26 Section 405(d) is Part of CSA Section 405, Which Focuses on the HPH Sector


Legislative Basis for the Effort
CSA Section 405
Improving Cybersecurity in the Health Care Industry
Section 405(b)
Health Care Industry Preparedness Report
Section 405(c)
Health Care Industry Cybersecurity Task Force
Section 405(d)
Aligning Health Care Industry Security Approaches

405(d) and the Health Sector Coordinating Council

The 405(d) Task Group is a standing task group within the larger HSCC Joint Cybersecurity Working Group (CWG). The HSCC is a private-sector organized and managed council created within the framework set forth in Executive Order 13636 (2013) and Presidential Policy Directive 21 (PPD-21). The 405(d) Task Group Members are by association members of the HSCC; thus membership is defined by the HSCC Charter CWG Charter. The Task Group utilizes their connection to HSCC to meet the strategic goal of industry collaboration by reviewing other HSCC products that could be turned into 405(d) products, such as the HICP publication.

* Participants included subject matter experts with backgrounds and experience in the following roles: Chief Executive Officer; Chief Information Security Officer (CISO) and/or IT security professional; chief information officer; chief risk officer or other risk manager; office of technology leader or hospital administrator; doctor, nurse, and other healthcare practitioners.

Studies

Study	Result	Year	Author
Crowdstrike 2023 Global Threat Report	Primary intrusions (used to cause disruption and damage), increased across all sectors and industries by 50% since 2021.	2023	Crowdstrike
	An estimated 6X increase in attacks (from 2 to 12 exploited vulnerabilities in past year)22 by China-nexus threat groups using known reported vulnerabilities.		
	71% of cybersecurity attacks comprise non-malware, hands-on-keyboard activity.		
	Adversaries were able to "... in just 1 hour and 24 minutes" move laterally from the initial compromised host, a reduction from 1 hour and 38 minutes from the prior year.		
	Nearly 80% of cyber-attacks leverage identity-based attacks to compromise legitimate credentials and use techniques like lateral movement to quickly evade detection.		
	Phishing-as-a-service allows threat actors to focus on high quality attacks that can evade or "annihilate" standard security controls. A common attack vector leveraged by these Phishing Service actors is to purchase credentials from marketplaces and to bypass MFA using MFA fatigue, vishing and "one-time password smishing techniques".		
CHIME Most Wired Survey	MFA is leveraged in over 90% of survey hospitals.	2022	CHIME
	88.6% of the hospitals surveyed indicated that they were conducting regular vulnerability scanning at least on a quarterly basis; however, on the same time scale hospitals surveyed indicate that their use of advanced forms of testing such as penetration, red team, purple team and tabletop exercises was 20% or below.		
Censinet/ AHA/KLAS	86% of the hospitals surveyed that their users are informed and trained on performing their cybersecurity-related duties and responsibilities.	2023	Censinet
	Further analysis of large and medium sized hospitals using MFA to a) protect their email (93%), b) protect their remote Virtual Desktop Infrastructure (92%) and, c) in combination with role-based access, protecting their VPNs (82%).		
	Over 99% of hospitals surveyed reported having basic spam and phishing protection capabilities in place.		
	Over 99% of hospitals surveyed reported having basic spam and phishing protection capabilities in place. In the same studies, 90% of hospitals stated they use URL detection, and 78% state they leverage automated responses to malicious email removal.		
	Less than 50% of hospitals surveyed indicated adoption of the NIST CSF Supply Chain Risk Management framework		

Study	Result	Year	Author
Censinet/ AHA/KLAS	Even among larger sized hospitals claiming to mature cybersecurity controls, the range of investment was ~168%, from the lowest investment of 0.03% to highest of 0.45% of revenue.	2023	Censinet
	95% of medium and large sized hospitals claim they were operating with end-of-life operating systems or software with known vulnerabilities.		
	46% of medium and large sized hospitals experienced an increase in cyber insurance premiums during 2021. Four hospitals surveyed experienced increases more than 100%, whereas 19 experienced increases just below 35%.		
	Additionally, 70.18% of hospitals surveyed state they are conducting vulnerability scans against web sites, which are exposed to the internet. Despite this scanning activity, only 52.90% of hospitals stated they have a documented plan for addressing the vulnerabilities identified.		
State of Supply Chain Risk Management in Healthcare	50% of hospitals evaluate the risks to impacting patient care by new suppliers' products.	2023	Ponemon
H-ISAC Annual Threat Report	288 healthcare executives were asked to list their biggest cybersecurity concerns and ransomware was decisively number one	2023	H-ISAC

Acronyms

Acronym	Description
ACA	Affordable Care Act
ACO	Accountable Care Organization
AD	Active Directory
AHA	American Hospital Association
AIS	Automated Indicator System
AV	Audio Video
CAC	Common Access Card
CASP	Cloud Access Security Broker
CHIME	College of Healthcare Information Management Executive
CIRCIA	Cyber Indcident Reporting for Critical Infrastructure Act
CISA	Cybersecurity and Infrastructure Security Agency
CISA CPG's	Cybersecurity and Infrastructure Security Agency Common Performance Goals
CISCP	Cybersecurity Information Sharing and Collaboration Program
CISO	Cybersecurity Information Security Officer
CMDB	Configuration Management Database
CMS	HHS' Center for Medicare & Medicaid Services
CURES Act	21st Century Cures Act
CWG	Cybersecurity Working Group
DAST	Dynamic Application Security Testing
DBIR	Data Breach Investigation Report
DDoS	Distributed Denial of Service
DHS	Department Homeland Security
DLP	Data Loss Prevention
DOJ	Department of Justice
DMARC	Domain-based Message Authentication Reporting and Conformance
DNS	Domain Name System
DoS	Denial of Service
EDR	Endpoint Detection Response
EMR	Electronic Medical Records
ENT	Ear, Nose and Throat
FBI	Federal Bureau of Investigation

Acronym	Description
FDA	Food and Drug Administration
GRC	Governance, Risk and Compliance
HC3	Health Sector Cybersecurity Coordination Center
HICP	Health Industry Cybersecurity Practices
H-ISAC	Health Information Sharing and Analysis Centers
HHS	Department of Health and Human Services
HITECH Act	Health Information Technology for Economic and Clinical Health Act
HPH	Healthcare and Public Health
HR	Human Resources
HSCC	Health Sector Coordinating Council
HSCC CWG	Health Sector Coordinating Council Cybersecurity Working Group
IAM	Identity and Access Management
IaaS	Infrastructure as a Service
IDN	Integrated Delivery Network
IR Playbook	Incident Response Playbook
ISACS	Information Sharing Analysis Centers
ISAO	Information Sharing Analysis Organization
LMS	Learning Management System
MFA	Multi-Factor Authentication
MSSP	Managed Security Service Provider
NIST	National Institute of Standards and Technology
NIST CSF	National Institute of Standards and Technology
NSA	National Security Agency
NSC	National Security Council
OODA	Observe, Orient, Decide, Act
PAM	Privileged Access Management
PwC	Price Waterhouse Cooper
RaaS	Ransomware-as-a-Service
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SIEM	Security Information and Event Management
SOAR	Security Orchestration Automation and Response
SOC's	Security Operation Centers
URL	Uniform Resource Location

Acronym	Description
VPN	Virtual Private Network
WAF	Web App Firewall
XDR	Extended Detection and Response