HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership

Considerations for Prioritized Recognized Cybersecurity Practices for the Health Industry

May 2023

Introduction

Cyber threats to the healthcare sector are a well-documented reality of modern healthcare delivery. Ransomware attacks against hospitals, clinics, service providers, and other healthcare delivery organizations (HDOs) routinely deny access to patient records, billing systems, and other digital technologies deployed throughout modern healthcare environments. Vulnerabilities discovered in the digital infrastructure relied upon by modern healthcare delivery organizations (HDOs) to deliver quality care pose patient safety and privacy risks that include delay or denial of treatment, data loss, manipulation or corruption of necessary treatment or other digital healthcare data, and the risk of intentionally or unintentionally tampered software, among other potential risks. And the massive and increasing complexity of today's connected healthcare ecosystem gives rise to its own risks: of unanticipated and poorly understood interdependencies; of unknown inherited security weaknesses; of overreliance on vendor solutions; of systems that fail to adequately account for human factors related to cybersecurity controls; and of inconsistencies between software and equipment lifecycles, among others. As a result, we are adopting new technologies faster than we are updating security practices, therefore creating a growing gap between slowly developing security posture and rapidly evolving security threats.

The Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) stood up a Task Group as part of its Charter to analyze which practices would provide the most significant impact towards improving cybersecurity resiliency across the nation's hospitals. The Task Group approached this charge by leveraging the following principles:

- Leveraged an adversarial mindset to determine which practices would be most impactful towards mitigating risk to patient safety due to a disruptive cyber attack. This information was sourced both from the recently produced 405(d) Hospital Resiliency Landscape Analysis, as well as HHS/HC3, H-ISAC and other adversarial Open Source intelligence.
- Used the Health Industry Cybersecurity Practices (HICP 2023) publication as the basis of core cyber hygiene. Additional practices were considered based on consensus provided by the task group.

It should be noted, that though there are specific practices outlined in this paper, the HPH sector believes this should only be taken as the "floor" or "basics" of a cyber program to be in place. All cyber programs are evolving and need to be established as such in order to stay current with modern threats. The prioritized recommendations provided in this paper take into place the *current* thinking, as of May

2023. As the adversaries change their tactics, so will our mitigations. Ultimately, it is a fully functioning cyber program that doesn't operate off a checklist of controls but rather is responsible to the business and patient needs, and considers our adversaries' progress, that makes us more resilient.

About the Health Sector Coordinating Council

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is a standing working group of the HSCC, composed of more than 400 industry and government organizations working together to develop strategies and best practices to address emerging and ongoing cybersecurity challenges to the health sector.

Healthcare Cybersecurity Prioritized Recognized Cybersecurity Practices Considerations

The HPH Sector consolidated three tranches: Tranche 1, considered the most urgent practices that will lead to the most direct and impactful mitigation to current threats; Tranche 2, important practices that either support practices in the first tranche or have direct impact on mitigations just to a lesser degree; and Tranche 3, other important practices to mitigate patient safety risk.

Designations within parenthesis are the corresponding HICP practice that is referenced. E.g. (1.M.A) refers to HICP Practice #1A for Medium Organizations, which is basic email protection.

Tranche 1: Most Impactful Practices to Mitigate Patient Safety Risk

When considering the floor of cyber hygiene with the most direct and impactful methods for mitigating current cyber threats, the HPH Sector selected the following five practices for Tranche 1. These practices are not ranked in order of priority, but rather are considered together as a package.

1. Basic Email and Endpoint Protections

Adversaries continue to leverage social engineering attacks, such as phishing, to either steal credentials (112% increase in access broker attacks) or drop malware for the initial point of compromise. After compromise the attacks will quickly shift (within 1 hour and 28 minutes, based on Crowdstrike's 2023 Annual Report) to additional assets inside the network. As such, these practices are considered to be basic practices to mitigating that initial point of intrusion.

A. Deployment of Multifactor Authentication for ALL email access, if email will ever be directly accessed from the Internet. It cannot be assumed that a single credential, even if the password associated to that credential is long and complex, will meaningfully protect against social engineering attacks. (1.M.B)
B. Deployment of key basic controls on email include using: 1) deny lists blocking known malicious sending domains; 2) leveraging antivirus to scan inbound email messages being delivered to the organization; 3) applying a label on all inbound email messages sourced from outside of the organization, such as "EXTERNAL"; 4) Implementing DMARC and DKIM policies to prevent email domain spoofing; 5) removing open relays within your email environment so emails cannot be spoofed from your authoritative domain; and 6) and email encryption (1.S.A ,1.M.A, 1.M.C)
C. Configure the most basic endpoint defensive measures, such as 1) antivirus tools, 2) limit local admin rights on the endpoint and limit provisioning the regular user account as a local administrator, 3) ensure regular cycle of patching and updates, 4) keep OS on an up to date and supported platform, 5) limiting remote access to the endpoint directly from the Internet (e.g. do not permit the direct access to remote desktop from the Internet, rather leverage a VPN connection with multi-factor authentication enabled) (2.M.A)
D. Train and deploy awareness and education to the workforce on social engineering attacks, such as providing training to the workforce through a learning management system, providing web pages and content for review, providing periodic education via staff meetings, newsletters, email or other methods to raise awareness, and conducting regular (preferably monthly) phishing simulations on the workforce to mimic a real attack. (1.M.D)

2. Supply Chain Risk Management (which is inclusive of Third-Party Risk)

A significant number of disruptive attacks, as well as data breaches, in the last several years have occurred through supply chain processes, such as third-party organizations. These attacks might involve a data breach, attacks that have shut down clinical functions (e.g. medical oncology EMR and radiation treatment modalities[1]), distribution of malicious code inside cryptographically signed software updates[2], could be used as a method of getting access to a hospital through established network connections such as VPNs or other remote access software, or attacks occurring on vendors where the HPH sector has converged upon similar vendors whereby disruption to that service can cause disruption across multiple organizations in one attack[3].

A. Bolster supply chain and third-party risk management programs. Must move beyond just the assessment of data security and confidentiality, but also evaluating the risks the supply chain can cause to mission/life critical functions, as well as access into the organization itself. Additionally, implement mitigations to manage the risks identified down to an acceptable level of tolerance in the organization. (10.M.B)
B. Restrict access that third-party organizations have access to the HPH organization itself, be it through remote sessions such as VPN or virtual desktop infrastructure, as well as permanent network links between the third party and HPH organization. These restrictions should be set up in such a way that the third party is granted access only to the assets and resources they need, rather than providing more inclusive access to other parts of the HPH organization (6.M.B).

3. Remote Access Management

Adversaries continue to leverage remote access techniques to conduct their illicit campaigns. In some cases, credentials are purchased on the dark web and used as the sole means of achieving access, without the adversary themselves conducting a 'hack'. These credentials could be stolen from breaches elsewhere and the password is reused by the workforce between those two platforms.

A. Ensure users are provisioned and deprovisioned based on the proper triggers, such as when a new employee joins the organizations or is terminated. Access should be removed timely to ensure it cannot be exploited (3.M.B)
B. Ensure all remote access channels, such as use of VPNs, virtualized desktop environments, terminal sessions, or other 'interactive sessions' that are accessible directly from the Internet have Multifactor Authentication Protections in place (3.M.D)
C. Limit the ability for vendors directly connected to the organization to access systems that are not part of their contracts. This restriction could be conducted through network segmentation, micro-segmentation, or dynamic ACLs in VPN tunnels, or other ring-fencing techniques. This restriction is consistent with the recommendation to ensure third party access is appropriately restricted. (6.M.B, 2.L.E)

4. Critical Monitoring and Incident Response and Recovery Actions

Inevitably an adversary will be able to subvert the preventative controls put in place. As such, we must design our cyber resiliency programs in such a way that can account for mitigating intrusions as quickly

[1] Ransomware: Extortion Actors Leak Data, Vendor Attack Disrupts Services (healthitsecurity.com)
[2] SolarWinds hack explained: Everything you need to know (techtarget.com)
[3] The Kronos effect: Addressing mission-critical processes for healthcare continuity | SC Media (scmagazine.com)

and effectively as possible, before the intrusion can lead to further damage such as weaponization and deployment of ransomware. These practices are provided as a means for detecting and responding to intrusions. It should be noted this is just the first step on a larger journey for detection and response.

A. Deploy Endpoint Detection and Response (EDR) tools to all managed assets, including servers, that is capable of identifying known attack patterns, especially the malicious use of built-in tools. For medical technologies, consider EDR deployment where it will be supported by the manufacturer. (2.L.C)
B. Implement a Cyber Incident Response Plan that classifies the severity of incidents and defines the actions to take based upon those classifications. This should include the communication plan with internal and external stakeholders, such as clinicians, leadership and external entities.(8.M.B)
C. Complete an inventory of mission and life critical assets and ensure these assets have a validated backup process that meets the 3-2-1 backup methodology. Ensure the backup of these assets has been validated by testing recovery procedures periodically. (4.M.B, 5.M.A)
D. Ensure that life critical functions and departments have downtime procedures in place. This is inclusive of key clinical workflows such as imaging, lab, pharmacy, and emergency departments/trauma. Consider aligning with the HSCC's Operational Continuity – Cybersecurity Incident (OCCI) Publication, which outlines key measures to implement for the first 24 hours of a large-scale cyber event and how to partner with Emergency Operations and Incident Command.[4]

5. Vulnerability Management and Mitigation

The final key method adversaries are using to compromise HPH organizations is to leverage existing vulnerabilities that are exposed directly to the Internet. As such, understanding the vulnerability posture of these externally exposed assets is critical to ensuring a proper defense. These practices outline core methods to managing this exposure.

A. Ensure an accurate inventory of assets that are *directly* accessible from the Internet, which includes ownership and patching windows. Note: this recommendation is not that 100% of all assets inside the organization should be found within the inventory, as such a process is quite complicated and challenging, but rather the assets that are most directly likely able to be exploited. (5.M.A)
B. Ensure assets that are *directly* exposed to the Internet are patched. This is inclusive of both operating system level patching as well as application layer patching. (7.M.B)
C. Conduct vulnerability scanning activities of assets that are *directly* exposed to the Internet. Upon identification of vulnerabilities, prioritize the patching or other mitigations based on the criticality of the vulnerability itself (with reference to the proposed schedules within HICP, which state critical vulnerabilities exposed to the Internet should be patched in less than 14 days). Leverage the CISA "known exploited vulnerability[5]" list when prioritizing mitigations. Prioritize mitigation of vulnerabilities based on most critical vulnerabilities. (7.M.A, 7.M.B, 7.L.B, 7.M.D)

[4] Operational Continuity – Cyber Incident (OCCI) | Health Sector Council
[5] Known Exploited Vulnerabilities Catalog | CISA

Tranche 2: Most Supportive Practices or other Material Mitigation of Patient Safety Risk

Additional practices are useful for protecting against modern adversaries. The following practices outline methods that supplement and/or provide additional protection and defense against attacks. Four additional practices were considered for Tranche 2. These practices are not ranked in order of priority, but rather the four practices outlined are considered together as a package.

6. Security Operations Center (SOC)

A full SOC will monitor multiple sources of logs, threat intelligence and other sources to determine if intrusions have occurred within the environment. This is above and beyond the monitoring that occurs with EDR (noted in Tranche 1).

A. Ensure cyber playbooks are built, deployed and monitored in a 24x7 capacity. Leverage the default playbooks outlined with in HICP Practice #8 when considering specific attack paths to protect against (which includes MFA fatigue attacks, impossible traveler scenarios, and others) (8.M.A)
B. Participate in Information Sharing and Analysis Centers/Organizations (ISAO/ISAC) which, at a minimum, involves the consumption and sharing of key Indicators of Compromise (IOCs) as well as identified Tactics, Techniques and Procedures (TTPs) (8.M.C)

7. Identity

A fully mobile and remote workforce means that Identity can be considered “the new perimeter”. As such, lifecycle management for deploying digital identities of every member of the workforce and consumer is important.

A. Ensure that all digital identities represented in your directories are allocated to a specific person, service account, or process, and that all identities are managed according to a lifecycle. (3.M.A)
B. Ensure proper provisioning and deprovisioning of accounts based upon when the lifecycle demands it, such as when a user onboards and is terminated (3.M.B)
C. Knowing that Active Directory is a key resource that adversaries attack, consider additional hardening, detection and response measures. These measures include 1) ensuring “jump boxes” for managing Domain Administrator access, 2) ensuring Multifactor Authentication for all Domain Admin access, 3) implementing Active Directory isolation designs which will prevent endpoints from directly accessing Domain Controllers, and 4) ensuring Active Directory logs are monitored by the SOC (3.M.C, 8.M.A)
D. Secure your most sensitive and privileged accounts through a formal privileged access management program (3.M.C)

8. Governance

Strategic cyber program management requires support from the highest executives and the Board. By establishing, dedicating, authorizing and empowering key personnel to own and operate the organizations cybersecurity program.

A. A. Encourage the Board, or a committee of the Board, to sponsor the cyber program for the HPH organization and designate a single leader in the organization responsible for cybersecurity. This can involve encouraging regular reporting to the Board, or a committee of the Board, on the

organization's cyber risks, program and progress. Additionally, encourage the implementation of cybersecurity governance with sponsorship and membership of executive management.

B. Establish a dedicated cybersecurity budget that is under the stewardship of the cybersecurity leader.
C. Establish a robust education program that discusses more than just social engineering attacks, but also accounts for other cyber threats, compliance obligations and other needs. (10.M.C)

Tranche 3: Other Important Practices to Mitigate Patient Safety Risk

Some additional considerations discussed and provided by the HPH HSCC Cybersecurity Working Group are as follows.

9. Miscellaneous

A. Leveraging next gen email tooling, such as URL click protection, sandboxing solutions and/or automated mitigation of malicious emails (1.L.A)
B. Limit the use of risky protocols such as Telnet, RDP, SMB, NTLM, etc....
C. Blocking personal email access from organizational devices, as well as personal file sharing sites (which can host malware), and social media sites, except for authorized sites and users who can receive and access them.
D. Consider limiting the ability for inbound email to be delivered only to designated individuals that have a need to send and receive email outside of the organization.
E. Further invest and mature asset management programs and the use of Configuration Management Databases (CMDB) (HICP Practice #5)
F. If VPN access or other "remote access" is required by a 3rd party, leverage a “third party access management tool” that can deliver “on demand” access that has been pre-authorized by the organization.