Strengthening Cyber Posture in the Health Sector

June 16, 2022

TLP: WHITE, ID# *202206161300*

Agenda

- What is Cyber Posture?
- Steps to Strengthen Cyber Posture
- Benefits of Strengthening Your Cyber Posture
- Cybersecurity Risks and Best Practices
- Security Risk Assessment
- The Impact of Cyber Incidents
- Importance of Strengthening Cyber Posture

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

What Is Cyber Posture?

Cybersecurity posture refers to the overall strength of an organization's cybersecurity, protocols for predicting and preventing cyber threats, and the ability to act as well as respond during and after an attack.

Source: Security Tech

Steps to Strengthen Your Cyber Posture

- Conduct regular security posture assessments
- Consistently monitor networks and software for vulnerabilities
- Define which department owns what risks and assign managers to specific risks
- Regularly analyze gaps in your security controls
- Define a few key security metrics
- Create an incident response plan and a disaster recovery plan

Benefits of Strengthening Your Cyber Posture

- Data protection from unauthorized access, loss or deletion
- Improves customer confidence
- Protection of intellectual property
- Prevention of cyber espionage
- Prevention of fraud

Source: Billion/Lloyd's List

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Cyber Threats and Best Practices

Cyber Threats and Best Practices

As cyber incidents continue to impact the Health Sector, it is recommended that all organizations follow the best practices outlined in CISA Insights to protect against cyber threats.

Some recommended steps are:

- Reduce the likelihood of a damaging cyber intrusion
- Take steps to quickly detect a potential intrusion
- Ensure your organization is prepared to respond if an intrusion occurs
- Maximize your organization's resilience to a destructive cyber incident

Reduce the Likelihood of a Cyber Intrusion

- Validate that all remote access to the organization's network, as well as privileged or administrative access, requires multi-factor authentication.
- Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA.
- Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.
- If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls outlined in CISA's guidance.
- Sign up for CISA's free cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats.

Take Steps to Quickly Detect a Potential Intrusion

- Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging, in order to better investigate issues or events.

- Confirm that the organization's entire network is protected by antivirus/antimalware software, and that signatures in these tools are updated.

- If working with international organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; and closely review access controls for that traffic.

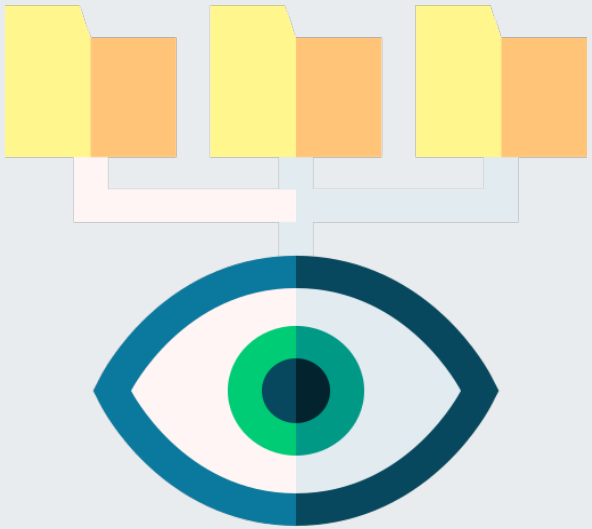
Be Prepared To Respond

- Designate a crisis-response team with main points of contact for a suspected cybersecurity incident and roles/responsibilities within the organization, including technology, communications, legal and business continuity.
- Assure availability of key personnel; identify means to provide surge support for responding to an incident.
- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

Maximize the Organization's Resilience

- Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.

- If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.



Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Security Risk Assessment

Security Risk Assessment

According to the NIST Special Publication 800-39, a security risk assessment is the process of identifying risks to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Six characteristics of an effective security risk assessment are:

- Identify Threat Sources
- Identify Threat Events
- Identity Vulnerabilities
- Determine the Likelihood of Exploitation
- Determine Probable Impact
- Calculate Risk as a Combination of Likelihood and Impact

Source: MyTechMag

Security Risk Assessment (Part 2)

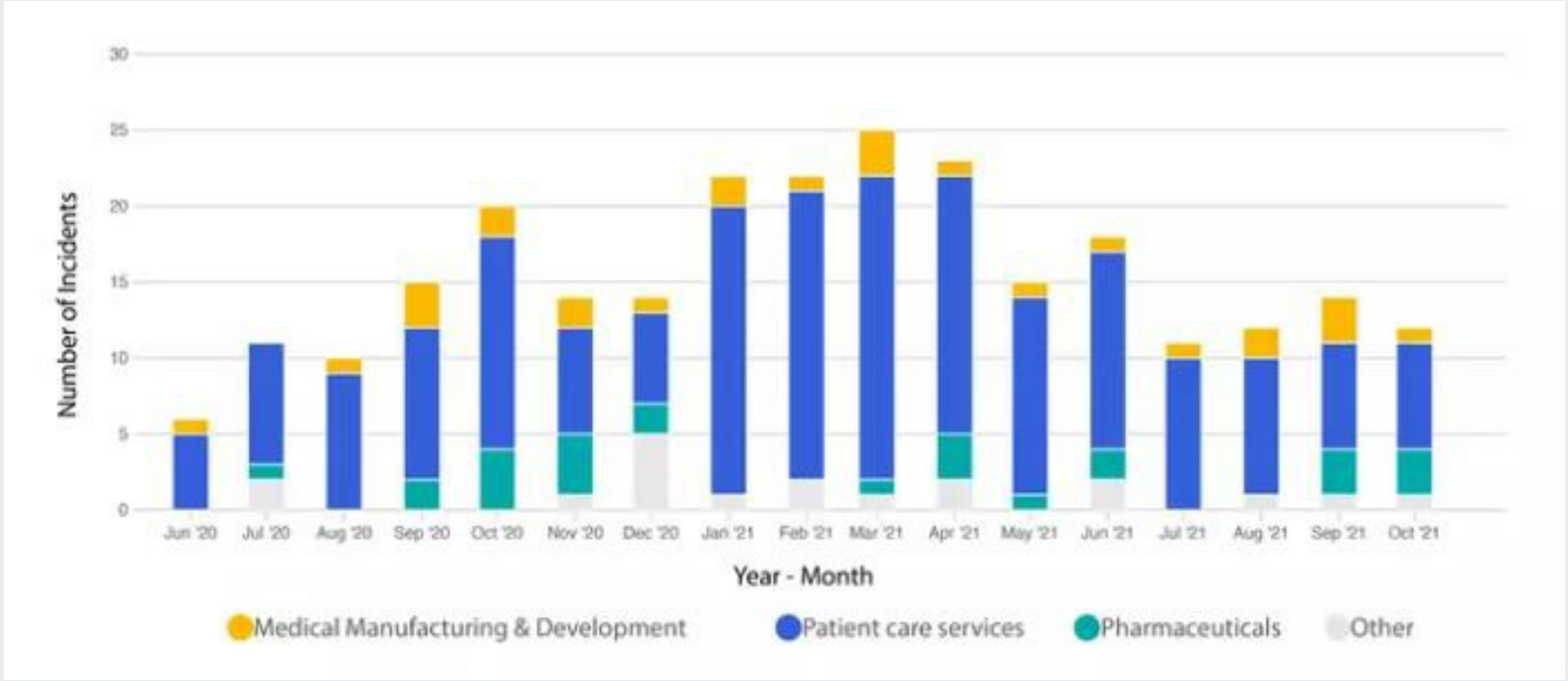
HIPAA has a Security Risk Assessment Tool available for health organizations of any size to use. It can be accessed and downloaded by visiting HealthIT.gov.

Source: HealthIT.gov

Impact of Cyber Incidents

Impact of Cyber Incidents

The healthcare sector is a popular target for cybercriminals. The CyberPeace Institute analyzed data from health sector cyber attacks in 33 countries, which showed a sharp increase at the start of the COVID-19 pandemic.



Source: CyberPeace Institute

Impact of Cyber Incidents (Part 2)

There are also significant financial impacts of cyber incidents.

- According to the law firm Baker Hostetler's study, the healthcare industry leads with the number of lawsuits due to data breaches. The breakdown is as follows:
  - Healthcare organizations (23%)
  - Business and professional services (17%)
  - Finance and insurance (15%)
  - Education (12%)
  - Manufacturing (10%)
- Additionally, the study also showed that there were at least one or more lawsuits stemming from 23 data breaches reported. In a total of 58 lawsuits filed, healthcare organizations made up 43 of those cases.

The Importance of Strengthening Cyber Posture

The health sector is responsible for handling vital and sensitive patient data. Over the years, there has been a significant increase in cyber incidents. The alarming spike after the COVID-19 pandemic has led to numerous changes in law and policy, most recently the Strengthening Cybersecurity Act of 2022.

CISA offers free services and tools to organizations of all sizes, and HIPAA also provides a free Security Risk Assessment tool to help with monitoring risks.

In addition to being compliant with the law, organizations within the health sector should strive to do their best to stick to the mission of protecting patient data and sensitive information in our network from malicious threat actors.

Reference Materials

References

- HHS, “HHS 405(d) Aligning Health Care Industry Security Approaches,” https://405d.hhs.gov/resources
- “Impacts of Cyberattacks on Healthcare,” Currentware. https://www.currentware.com/blog/the-impact-of-cyberattacks-on-healthcare/
- Tunggal, Abi Tyas. “How to Perform a Cybersecurity Assessment.”UpGuard. 7/22. https://www.upguard.com/blog/cyber-security-risk-assessment
- “Security Risk Assessment Tool,” HealthIT. https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
- “The What is Cybersecurity Posture and How Can You Evaluate It?,” Security Scorecard. 12/2019. https://securityscorecard.com/blog/what-is-a-cybersecurity-posture
- “6 Steps to Strengthen Your Security Posture,”HyperProof. April 28, 2022. https://hyperproof.io/resource/strengthen-security-posture/

References

- The White House. “Statement by President Biden on our Nation’s Cybersecurity,”Whitehouse.gov. March 21,2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

- “New Cybersecurity Law Will Require Cyber-Incident Reporting for Critical Infrastructure,”JDSupra. March 18, 2022. https://www.jdsupra.com/legalnews/new-cybersecurity-law-will-require-7181241/

- CISA. “Capacity Enhancement Guides for Federal Agencies,” CISA.gov. https://www.cisa.gov/capacity-enhancement-guides-federal-agencies

- Senhasegura Blog Team. “Cybersecurity Health: What it is and how to comply with HIPAA,” Senhasegura. April 20,2022. https://senhasegura.com/cybersecurity-health-what-it-is-and-how-to-comply-with-hipaa/

References

- Lagasse, Jeff. “Patients increasingly suing hospitals over data breaches,” Healthcare Finance. April 13,2022. https://www.healthcarefinancenews.com/news/patients-increasingly-suing-hospitals-over-data-breaches

- “Healthcare Security Risk Assessment & HIPAA Security Risk Analysis FAQs,”MedITology. November 15,2021. https://www.meditologyservices.com/healthcare-security-risk-assessment-hipaa-security-risk-analysis-faqs/

- Duguin, Stephane. “If healthcare doesn't strengthen its cybersecurity, it could soon be in critical condition,”CyberPiece Institute/World Economic Forum. November8, 2021. https://www.weforum.org/agenda/2021/11/healthcare-cybersecurity/

- Stewart, Michael. “Common Challenges to Effective Risk Assessment,” My Tech Mag. December 9, 2020. https://www.mytechmag.com/common-challenges-to-effective-risk-assessment/

Questions

FAQ

Upcoming Briefing

- July 7 – Quantum Cryptography and Healthcare

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

HHS.GOV/HC3

HC3@HHS.GOV