THE GOVERNANCE INSTITUTE
A SERVICE OF nrc HEALTH
NOVEMBER 2022
Hospital Focus

Why Implement Cybersecurity Best Practices?

By **DeAnn Tucker, M.H.A.-H.I., CHPS, CHPC, RHIA, CCS**, Senior Manager, *Coker Group*

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 introduced stricter penalties for non-compliance with the Health Insurance Portability and Accountability Act (HIPAA). Twelve years later, on January 5, 2021, H.R. 7898 was signed into law, amending HITECH and requiring the secretary of the U.S. Department of Health and Human Services (HHS) to consider certain recognized security practices when determining fines and corrective action plans related to HIPAA violations.[1]

While cybersecurity professionals focus on policies and procedures that ensure the confidentiality, integrity, and availability (CIA) of information, the board typically focuses on the organization's risks, reputation, and business continuity. Senior leaders and board members need to recognize cyber threats and the risks they present. They should set the tone for cybersecurity best practices and support efforts to strengthen an organization's security posture.

Cybersecurity Act of 2015

The law defines *recognized security best practices* as "…standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity."

The Cybersecurity Act of 2015 was created partly to promote information sharing by private companies for "cybersecurity purposes."[2] Traditionally, private companies were not always comfortable sharing information for fear of civil or criminal liability. The Act authorizes private companies to share

1 U.S. Government Publishing Office, 116th Congress, 2D Session, H.R. 7898.
2 Electronic Privacy Information Center, "Cybersecurity Act of 2015," December 16, 2015.

information with the federal government, and the Department of Homeland Security acts as a clearing house, helping to increase information sharing. The Act defines a *cybersecurity purpose* as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."

Cybersecurity Oversight

It is common to have a compliance committee as a sub-committee of the full board with compliance being a regular agenda item. Depending on the complexity of the organization, a dedicated cybersecurity sub-committee should be considered. If a standalone information technology committee already exists, restructuring the reporting similar to compliance could be an alternative approach with regular reports presented to the full board. Cybersecurity can affect many areas of operations and impact business decisions. It is important that at least one member of the board has experience in technology and the ability to evaluate recommendations against industry best practices.

Examples of Bad Practices

In addition to sharing potential threats and best practices, the Cybersecurity & Infrastructure Security Agency (CISA) has created a "Bad Practices" document that organizations can use to help evaluate their security programs.[3] Below is a list of some of the practices that should be avoided.

1. Use of end-of-life software:
   - Windows 7 support ended in January 2020 and is still used in many healthcare organizations. What version of Windows is your hospital using?
   - Is there a plan for upgrading software that is nearing end-of-life support?
2. Use of known/default/fixed passwords:
   - Default system passwords are often shared among bad actors and can be used to compromise a hospital's systems. Is your organization changing default system administrator passwords?
   - Is the hospital blocking the use of commonly used and easy-to-guess passwords?
3. Use of single-factor authentication for remote or administrative access:
   - Two-factor authentication is considered a best practice for securing remote access. Has your organization evaluated two-factor authentication?

3 Cybersecurity & Infrastructure Security Agency, "Bad Practices."

4. Poor patching:
   - Patch management is the process of distributing and applying updates to software. Are your hospital's security patches up to date?

➜ Key Board Takeaways

- Ensure that an annual security risk analysis is conducted and the report is presented during a full board meeting.
- Review the risk remediation plan and provide input.
- Request regular updates to progress addressing risks.
- Support and approve implementation of *recognized security best practices.*

405(d) Program

In response to H.R. 7898, HHS launched a Web site titled "405(d) Aligning Health Care Industry Security Approaches Program," through the Office of Chief Information Officer (OCIO) and Office of Information Security (OIS).[4]

The 405(d) program is a "collaborative effort between industry and the federal government to align healthcare industry security practices in an effort to develop consensus-based guidelines, practices, and methodologies to strengthen the healthcare and public health (HPH) sector's cybersecurity posture against cyber threats." It aims to raise awareness, provide vetted cybersecurity practices, and move organizations toward consistency in mitigating the sector's current, most pertinent cybersecurity threats. It is in response to the Cybersecurity Information Sharing Act of 2015, which calls for "the timely sharing [of information by the government] with relevant federal entities and non-federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats."[5]

The 405(d) Web site also provides resources, products, videos, and tools that help raise awareness and provide cybersecurity best practices. Erik Decker, 405(d) Task Group Industry Co-Leader, stated, "This Web site is the first of its kind! It's a unique space where the healthcare industry can access vetted

4 See https://405d.hhs.gov.
5 See CISA, "Cybersecurity Information Sharing Act of 2015."

cybersecurity practices specific to the [healthcare and public health] sector on a federal government Web site."[6]

HHS also published *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*, which provides vetted cybersecurity practices for healthcare organizations of all sizes.[7] There is one volume that focuses on small healthcare organizations,[8] and another for medium to large[9] healthcare organizations. There are many valuable tools and resources and a long list of publications and other materials the group has produced that hospitals and health systems can utilize to ensure they are effectively protecting their organizations from cyber-attacks.

Five Main Threats:

1. Email phishing
2. Ransomware
3. Loss of or theft of equipment
4. Insider, accidental, or intentional data loss
5. Attacks against connected medical devices

10 Best Practices:

1. Email protection systems
2. Access management
3. Asset management
4. Vulnerability management
5. Medical device security
6. Endpoint protection systems
7. Data protection and loss prevention
8. Network management
9. Incident response
10. Cybersecurity policies

6 "HHS Launches Web site for the 405(d) Aligning Health Care Industry Security Approaches Program" (press release), December 1, 2021.
7 HHS, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, Resources and Templates.
8 See *Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations*.
9 See *Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations*.

Where to Start

The best place to start is to identify the organization's risks and vulnerabilities by conducting a security risk analysis (SRA). If your hospital or health system has not completed your initial SRA, start today.[10] The board should ensure that an annual SRA is conducted, a remediation plan is created, and risks are prioritized according to importance and cost. The first step is to identify where your electronic protected health information (ePHI) is stored, received, maintained, or transmitted. Your asset inventory should include (but is not limited to) applications, laptops, desktops, external memory devices, multi-function machines with hard drives, and medical devices. When identifying the organization's assets, don't forget to include any personally owned devices with access to ePHI. Access could include email, Web-based file sharing, and cloud-based systems.

After finding your ePHI, identify the hospital or health system's risk factors, including threats and vulnerabilities. The National Institute of Standards and Technology defines a threat as the potential for a person or thing to exercise a specific vulnerability. Threats can be human (hacker) or nature (flood). A vulnerability is a flaw or weakness in your security program. Vulnerabilities are using an operating system that is no longer supported and receiving updates, lack of virus protection or encryption, a sprinkler head in the server room, or an error in the setup of access to ePHI. Identifying risks before someone else identifies them can help you prevent a breach, and ultimately save the organization from the severe impact an attack could have on its finances, reputation, and patients.

For a deeper dive on the board's role in cybersecurity, read *Enterprise Cyber Risk Management*.

The Governance Institute thanks DeAnn Tucker, M.H.A., RHIA, CHPS, CCS, Senior Manager, Coker Group, for contributing this article. She can be reached at dtucker@cokergroup.com.

10 For helpful SRA resources see HHS, "Guidance on Risk Analysis."