AHIMA Guidelines: The Cybersecurity Plan

The best way to defend against a cybersecurity attack is to develop a robust, tested cybersecurity plan. Below are AHIMA's suggested steps to a complete cybersecurity plan.

Steps to a complete cybersecurity plan

1. **Conduct a risk analysis of all applications and systems**

   Information governance programs do not focus solely on clinical information but a broader view of all information stored by the organization. So, in risk analysis we recommend you include all applications and systems even if protected health information (PHI) is not stored, processed, or transmitted; any application and system could be compromised and later used to launch an attack against other systems on the same network must be addressed in the risk analysis and assessment. You should also create an information asset inventory as a base for risk analysis that defines where all data and information are stored across the entire organization (again not just PHI). This should include biomedical devices, mobile devices and legacy systems.

2. **Recognize record retention as a cybersecurity issue**

   Healthcare organizations have been storing and maintaining records and information well beyond record retention requirements. This creates significant additional security risks as systems and records must be maintained, patched, backed up, and provisioned (access) for longer than necessary or required by law.

   Destroy records, emails, and documents per policy in compliance with state and federal law. In the era of big data the idea of keeping "everything forever" must end. It simply is not feasible, practical or economical to secure legacy and older systems forever.

3. **Patch vulnerable systems**

   When patches (updates) are released by the manufacturer of a system or software, they should be implemented immediately.

4. **Deploy advanced security endpoint solutions that provide more effective protections than standard antivirus tools**

   Pattern files alone are not effective. Endpoint security should include device and user ID behavior monitoring, called User Behavior Analytics (UBA)

5. **Encrypt the following:**

- Workstations (high-risk) and laptops
- Smartphones and tablets
- Portable media and backup tapes (if tapes are still being used)

6. **Improve identity and access management**

   Strengthen password requirements. You can also apply password standards consistently in applications and systems, including biomedical devices. You might also choose to lock users out of an application or systems after a predetermined number of failed log-in attempts. Implement two-factor authentication where feasible, especially for remote access by system administrators. Restrict concurrent log-ins, as many workers only need to log in once. Disabling additional log-ins for the same user or ID can prevent that ID from being used inappropriately.

   Implement time-of-day restrictions. If a worker only uses a computer on their one work shift and doesn't have remote access privileges, for example, applying time-of-day restrictions eliminates the possibility of that ID being used by someone else during a time when it should not be in use.
   Finally, educate users, as part of the information governance program, about their responsibilities for information creation, access, use, disclosure and destruction.

7. **Refine web filtering (blocking bad traffic)**

   Block traffic to/from foreign countries you are not actively doing business with. Quarantine or block inbound e-mail traffic that comes from a newly created domain; most phishing attacks come from domains that have only been in existence for a few days. Force employees to use their personally owned mobile device through a "guest" wireless network for accessing their personal accounts; block employees from accessing personal sites.

8. **Implement Mobile Device Management (MDM)**

   This strategy can help enforce security controls for tablets and smartphones (personally-owned or organization-owned devices).

9. **Develop incident response capability**

   Think to yourself: "It's not a matter of 'if'—it's a matter of 'when.'" By creating incident response playbooks, educating a response team and conducting a tabletop drill that includes common cyberattacks and/or system compromises can appropriately prepare your team.

10. **Monitor audit logs to selected systems**

Consider outsourcing this task to a Managed Security Service Provider (MMSP), an organization that specializes in monitoring key systems for possible attacks.

11. **Leverage existing security tools like Intrusion Prevention System/Intrusion Detection System (IPS/IDS) to detect unauthorized activities**

    Many organizations already have security tools available to them, but the tools have not been implemented or turned on (security flexibility within systems may not be activated).

12. **Evaluate business associates**

    Obtain reasonable assurances of compliance with the HIPAA Security Rule from current business associates; start with companies that represent a high risk such as smaller organizations. Also, evaluate the risks associated with any potential (new) business associate and prior to purchasing a product or service.

13. **Improve tools and conduct an internal phishing campaign**

    Stop employees from clicking on embedded links by teaching them what to look for, including:

    - Suspicious e-mail URLs
    - URLs that contain a misleading domain name
    - Poor spelling and grammar
    - An e-mail that asks for personal information
    - The offer seems too good to be true
    - You did not initiate the action
    - You are asked to send money to cover costs
    - Unrealistic threats
    - Message appears to be from a government agency
    - Something does not look right

14. **Hire an outside security firm to conduct technical and non-technical evaluations**

    This might include conducting a vulnerability scan of external-facing systems, running a penetration test of key applications and systems and evaluating policies, procedures, and organizational practices pertaining to the IT environment.

15. **Prepare a 'State of the Union' type presentation for an organization's leaders on cybersecurity**

    Be prepared to answer questions such as:

    - How are we doing as compared to similar organizations of our size?

- Who is in charge of our cybersecurity program?
- What are we doing to reduce our risk of an attack?
- How and when will the board be notified if there is a cyber breach?
- Do we have cyber insurance?

16. Apply a 'Defense in Depth' Strategy

In order to thwart an attempted intrusion by a cyber-attack, take a proactive stance in your cybersecurity defenses. Review current access control protocols and tighten them up, if indicated. Another proactive step you can take is to conduct an evaluation or assessment of current security policies. If they have not been updated or modified to account for risks of hacking, this is an action item that should be undertaken.

Reactive measures should also be taken to optimize your cybersecurity strategy. A review of audit logs on a regular basis is strongly recommended. Review the organization's incident response capabilities and update the incident response plan. This holds true also for an organization's disaster recovery plan and data backup plan. Conducting a desktop drill (or several) periodically will help to minimize missteps in the case of cybercriminal intrusion.

17. Detecting and Preventing Intrusion

Intrusion detection systems (IDS) are designed to detect and identify a potential intruder by monitoring network and/or system activities to spot malicious activities by signature-based or anomaly detection methods as well as other protocol-based procedures. IDS can produce reports and identify trends that could be indicative of cyber-type issues taking place.

Intrusion detection and prevention systems (IPS or IDPS) allow prevention capabilities to be set by the administrator. This feature allows the organization to determine the tuning and customization settings that are preferred so that thresholds and alerts are at the level of tolerance for the organization. Once these settings are established, they should be reviewed and adjusted to allow for appropriate detection and, ideally, blocking.

Every organization must identify their level of need for intrusion detection and prevention. Given the rise of cybercriminal activity aimed directly at healthcare, this is a subject that should be addressed for its relevancy with a sense of urgency to ensure that the entire health system's PHI, in every system, is adequately protected to the best extent possible.

Glossary of Security Terms to Know:

Breach: An incident in which sensitive, protected, or confidential information has potentially been viewed, stolen, or used by an individual unauthorized to do so.

Ransomware: A type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Some ransomware encrypts files (often called Cryptolocker).

Phishing: The attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Hacktivist: A computer hacker whose activity is aimed at promoting a social or political cause.

Malvertisements: The use of online advertising to spread malware. Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.

Cloud Storage: A model of data storage in which the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company.

References:

Anand, Priya. "How Long Does It Take To Hack a Company? Just Minutes, Report Says." *MarketWatch*. April 14, 2015. www.marketwatch.com/story/how-long-does-it-take-to-hack-a-company-just-minutes-report-says-2015-04-14.

Ferrillo, Paul A. "Wham, Bam, Thank You Spam! Don't Click on the Link!" Harvard Law School Forum on Corporate Governance and Financial Regulation. May 17, 2015. http://corpgov.law.harvard.edu/2015/05/17/wham-bam-thank-you-spam-dont-click-on-the-link/

Mandiant. "Beyond the Breach." 2014. https://www.fireeye.com/blog/executive-perspective/2014/04/annual-m-trends-report-looks-beyond-the-breach.html

This material includes excerpts from:

Dill, Mark W., Susan Lucci, and Tom Walsh. "Understanding Cybersecurity: A Primer for HIM Professionals" *Journal of AHIMA* 87, no.4 (April 2016): 46-51 [extended web version]. http://bok.ahima.org/doc?oid=301408.

US Department of Health and Human Services, Healthcare Industry Cybersecurity Taskforce. "Report on Improving Cybersecurity in the Health Care Industry." June 2017. https://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx

--Adapted from a 2017 article by Kathy Downing, MA, RHIA, CHPS, PMP, CPHI