Understanding Cybersecurity: A Primer for HIM Professionals - Retired

Save to myBoK

As protectors of patient health records, health information management (HIM) professionals are developing a keener understanding of the broad topic of cybersecurity and are becoming actively involved in organizational cybersecurity efforts. Information technology (IT) departments typically are charged with the responsibility of information and information system security. Today, HIM professionals are more actively engaged in working with IT and security operations because of their understanding of workflows and user behavioral patterns involving protected health information, including user availability and access.

The purpose of this Practice Brief is to provide insight on the surge in cybercriminal activity and to serve as a reference for how to increase awareness as well as strategies that may be employed to assist in reducing the risk of cyber attacks in healthcare.

According to Techopedia.com, “Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management and incident management.”

The Department of Health and Human Services (HHS) has required the reporting of privacy and security breach activity on their website since 2009. Between 2009 and 2014, theft, loss, unauthorized access, and inappropriate disposal were the most common reasons for data breaches that affected over 500 individuals.

Cybercriminal activities have escalated in recent years, making data breaches a daily news item. In 2015 hacking, the most pervasive and effective method that cybercriminals chose to access protected health information (PHI), swiftly soared to the top of the list of the breach category affecting the largest number of patients. The number of patients affected by hacking incidents reported between January 1, 2010 and December 31, 2015 is well over 115 million. In 2015 alone, over 111 million patient records have been accessed as a result of these types of cybercriminal activities.[1]

Year Hacking Events Reported to HHS	Number of Hacking Events Reported	Number of Patients Affected in Hacking Events for the Year
2010	10	568,358
2011	16	297,269
2012	16	900,684
2013	19	206,998
2014	31	1,786,630
2015	59	111,833,241

Top Healthcare Breaches - Caused by Hacking

(Affecting more than 1 million people)

The information below includes the name of the organization, number of individuals affected, and date disclosed to the public, and the date the attack started-if known or generally assumed to be correct.

Anthem: 78.8 Million affected (Reported in February 2015)

Premera Blue Cross: 11 Million affected (Disclosed in January 2015; attack started in May 2014)

Excellus BlueCross Blue Shield: 10 Million affected (Disclosed in August 2015; attack started in December 2013)

UCLA Health: 4.5 Million affected (Disclosed in July 2015; attack started in September 2014)

Medical Informatics Engineering: 3.9 Million affected (Disclosed in May 2015; attack started in May 2015)

CareFirst BlueCross BlueShield: 1.1 Million affected (Disclosed in May 2015; attack started in June 2014)

Source: US Department of Health and Human Services' Office for Civil Rights. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. December 31, 2015.

Types of Attacks

The nine basic patterns or types of attacks found in the Verizon Data Breach Investigation Report (DBIR) for both 2014 and 2015 are listed in the sidebar below. According to the reports, these account for over 90 percent of the 100,000 incidents that their researchers have analyzed.[2]

Verizon Data Breach Investigation Report

2015 DBIR Report Ranked by Number of Attacks	2014 DBIR Report Ranked by Number of Attacks
Miscellaneous errors	Point of sale intrusions
Crimeware	Web application attacks
Insider and privilege misuse	Insider and privilege misuse
Physical theft and loss	Physical theft and loss
Web application attacks	Miscellaneous errors
Denial of service	Crimeware
Cyber-espionage	Payment card skimmers
Point of sale intrusion	Cyber-espionage
Payment card skimmers	Denial of service

In their 2015 DBIR, Verizon states that the estimated financial loss from 700 million compromised financial, healthcare, and other business records is approximately $400 million. This reflects the importance of managing data breach risks. Unfortunately, healthcare breaches are some of the most visible, leading this trend.[3]

Why the sudden rise in hacking, in healthcare in particular? For one thing, the black market value of an electronic health record has risen sharply over other information such as credit cards.[4] The financial industry has implemented security safeguards and controls to detect and prevent fraud. In comparison, the healthcare industry struggles with the resources needed to monitor audit logs and does not have the technical tools to detect and prevent identity theft. Unfortunately, many (if not most) healthcare organizations may not be properly prepared to address the rise in hacking and new cyber-threats. As an industry, healthcare allocates fewer resources to IT security relative to its peers in other industries. Information obtained in the fourth annual Healthcare Information and Management Systems Society (HIMSS) Security Survey suggests that security spending in healthcare is about three percent of the IT budget for the majority of respondents.[5] In other industries, the budget is closer to eight percent.[6]

Threat Agents Have Evolved Over Time

Initially hacking was something that was done as an individual activity. Today, hacking is organized. There are organized groups of criminals that understand how cybercrimes have the potential to acquire money with fewer risks as compared to traditional crimes. Cyber-attacks could even be used as a weapon for waging war.[7]

Human threat factors for hacking may include:

1. Ex-employee or disgruntled employee
2. Angry family or patient
3. People trying to make/steal money
4. Cyber espionage
5. Terrorists[8]

Besides external attacks, organizations also have to deal with insiders whose actions, whether intentional or unintentional, may lead to data breaches. Malicious insiders may use their authorized access privileges to conduct identity theft. One such case occurred at Blue Cross Blue Shield of Michigan (BCBSM) where an employee was responsible for an identity theft scheme that affected over 5,500 BCBSM members.[9]

Without realizing it, employees may click on embedded links that release malware—including ransomware, which limits users from accessing their system until a ransom is paid to the responsible hacker—or allow external attackers access to internal applications, systems, and data. According to CNBC, some sophisticated malware now can attach itself even without a person clicking on a malicious link. For example, sites such as YouTube and other search engine sites have advertisements that may contain this malware, also called “Malvertisements.” Merely visiting these ads can introduce malware to your system that can in turn infect an entire organization. What’s worse is that because malware changes so often, sometimes thousands of times every day, even the best detection tools cannot find and eradicate the newest versions.[10]

Business associates can potentially be responsible for breaches and cyber attacks. Although business associates have been officially required to be in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule since September 2013, many may not have implemented appropriate security safeguards and controls, as evidenced by the number of breaches reported to HHS. As of December 31, 2015, 290 large breaches have been caused by business associates, resulting in the breach of over 26 million patient records.[11]

“Hacktivist” is a fairly new term used to describe an individual or a group of individuals that are motivated to carry out a cyber attack for political, religious, or other reasons with the goal to punish or inflict harm on an organization. For example, the infamous hacker network Anonymous launched a distributed denial of service (DDOS) attack against Boston Children’s Hospital and its affiliates in 2014. The attack was in protest of the Justina Pelletier case, where the State of Massachusetts had hospitalized a child against the will of the child’s mother. Once the DDOS attack began, Boston Children’s Hospital and some of its affiliates were forced to temporarily disconnect from the Internet. Fortunately, the attack stopped after about a week. There is no definitive reason as to why the attack stopped, but sources have indicated that an Anonymous member posted something that questioned the group's motives and the potential harm the attack could have on the care and treatment of children.[12]

Top Cybersecurity Concerns for Healthcare

- **Biomedical devices** – Patient lives are at stake
- **Insiders** – Workforce member – snooping or identity theft
- **Business Associates** – Responsible for approximately 20 to 30 percent of all reported breaches
- **Malicious code** – Ransomware, free mobile apps, malvertisements, etc.
- **Phishing** – In Verizon's 2014 Data Breach Investigations Report, phishing was associated with over 95 percent of incidents attributed to state sponsored actors.
- **Mobile devices** – PHI resides in places where a healthcare organization has no control and the theft or loss of personally-owned mobile devices are a growing concern
- **Webmail and unsecured cloud storage** – Like mobile devices, PHI resides in places (personally-owned computer at home or a kiosk in a hotel lobby) where there may be little or no security; Data could also be stored to the cloud (unbeknownst to the organization) through the automatic backup of smartphone data to the cloud or through file sharing services such as DropBox

Business Challenges Unique to Healthcare

As the profile of "hackers" has changed over time, so too has their target. Financial information was once a prime target of hacking. But with the sophistication of antifraud tools, the black market value of credit card data has dropped while the value of the electronic health records and user credentials have gone up.[13]

The rich demographics surrounding someone's protected health information (PHI)—such as a Social Security number, address, and date of birth—are not time-sensitive. In contrast to credit card data that has many fraud controls in place, stolen PHI has a shelf life that is much longer than credit card data and therefore has a higher black market value.

While other industries are working to lock down their data, healthcare has the added challenge of being forced to share more patient data externally. Sometimes this data sharing is required by law or regulations. For example, PHI may be shared externally to:

- Patients (patient portals, compact discs)
- Care managers (healthcare insurance companies, home health)
- Other providers (e-mail, text messages)
- Clearinghouses and insurance companies for payment of claims/patient bills
- Business associates to provide support services
- Government entities (state/federal agencies)
- Hospitals using more Internet-based business applications (cloud services) and systems
- Health information exchanges (HIEs)

The Internet of Things

The "Internet of Things" is made up of essentially any "smart" device that can connect to the Internet. While it makes some tasks easier to manage and control, it increases the risks for cyber attacks. Devices or objects that people typically do not consider "computers" are vulnerable to attack. For example, automobiles, trains, home security systems, surveillance cameras, biomedical devices, health and fitness monitors, and building control systems can now all connect to the Internet. If a smart device connects to the Internet, it can become a target of cyber-attackers if not protected.

Biomedical Devices

According to PricewaterhouseCoopers (PwC), "As security breaches become more common and costly, medical device cybersecurity will emerge as a major issue in 2016, requiring device companies and healthcare providers to take pre-emptive action to maintain trust in medical equipment and to prevent breaches that could cripple the industry."[14] The Federal Bureau of Investigation (FBI) has issued several warnings regarding the security of biomedical devices, including a warning in 2015 that an infusion pump was vulnerable to hacking.[15]

After conducting a comprehensive risk analysis for many healthcare systems, the most frequently identified vulnerabilities for biomedical devices include:

- Default manufacturers' system administration (generic) accounts and weak password rules
- No antivirus software
- No intrusion prevention system (IPS) to detect unauthorized activity
- Ability to be remotely accessed (vendor support)
    - The risk is that these devices may interface through a Health Level Seven gateway with an electronic health record system
- Many wireless devices still using Wired Equivalent Privacy (WEP)
- Outdated/unpatched operating systems

Importance of a Cybersecurity Plan

The best way to defend against an attack is to develop a cybersecurity plan. The cybersecurity plan should fall under the oversight of the chief information security officer (CISO). The plan needs to address, in the following order:

1. People
2. Processes
3. Technology

For example, organizations may take proactive steps to block phishing e-mails before they get through the e-mail gateway. But no technology defense is perfect. With estimates as high as 100 million phishing e-mails being sent every day, all it takes is one to get through the e-mail gateway to cause a great deal of harm to an organization.

That is why an educated workforce is the first line of defense against cyber attacks. According to estimates, the median time from when the phishing e-mail arrives until a recipient clicks on an embedded link is one minute and twenty-two seconds.[16,17] That does not leave much time to launch a countermeasure or send out a security awareness message warning the users.

Once created, a cybersecurity plan should be reviewed at least quarterly to ensure the organization is doing everything possible to prevent or detect an attack. Some suggested items to include in a cybersecurity plan include:

- Conduct a risk analysis of all applications and systems
    - Include biomedical devices
    - Include all other applications and systems even if 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
- Patch vulnerable systems; when patches (updates) are released by the manufacturer of a system or software, they should be implemented immediately
- 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))
- Encrypt the following:
    - Workstations (high-risk) and laptops
    - Smartphones and tablets
    - Portable media and backup tapes (if tapes are still being used)

- Improve identity and access management
    - Strengthen password requirements
    - Apply password standards consistently in applications and systems, including biomedical devices
    - 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. Many (if not most) 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.
- 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
- Implement Mobile Device Management (MDM) for enforcing security controls for tablets and smartphones (personally-owned or organization-owned devices)
- Develop incident response capability (*Think "It's not a matter of 'if'—it's a matter of 'when'"*)
    - Create incident response playbooks
    - Educate response team
    - Conduct a tabletop drill that includes common cyber attacks and/or system compromises
- 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
- 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)
- 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
    - Evaluate the risks associated with any potential (new) business associate and prior to purchasing a product or service
- Improve tools and conduct an internal phishing campaign
    - Stop users from clicking on embedded links
    - Teach users what to look for (see the sidebar below)
- Hire an outside security firm to conduct technical and non-technical evaluations
    - Conduct a vulnerability scan of external-facing systems
    - Run a penetration test of key applications and systems
    - Evaluate policies, procedures, and organizational practices pertaining to the IT environment

- Prepare a “State of the Union” type presentation for an organization’s Board of Directors 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?

Some Clues of a Phishing E-mail

What are the signs that you may have received a phishing e-mail? Here are a few clues that an e-mail may be part of a targeted phishing scheme:

- Suspicious e-mail URL
- 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

Source: Posey, Brien. “10 Tips for Spotting a Phishing Email.” TechRepublic. October 15, 2015. www.techrepublic.com/blog/10-things/10-tips-for-spotting-a-phishing-email/.

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 now 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.

Detecting and Preventing Intrusion

When IT staff is asked by executives “Have we ever been hacked?” the response often provided by the IT staff is “No.” Unfortunately, they may not even be aware of the fact that their systems may have already been compromised. In 60 percent of cases, attackers are able to compromise an organization in minutes.[18]

Likewise, IT staff and HIM professionals should learn that when it comes to cybersecurity, the phrase “Not that I am aware of” should be tacked on to the end of their response. For example, when asked, “Have we ever been hacked?” the appropriate answer should probably be “Not that I am aware of.” Why? One survey found that, on average, a hacker can be inside of an organization for 229 days before being detected.[19]

Therefore, if an organization has a good security program in place, it may actually have more reported incidents and breaches than organizations with a less than stellar security program. Better security controls such as intrusion detection and prevention systems and mature log monitoring can more readily detect attacks than organizations that lack those controls.

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) allows 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 Terms

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.

Notes

[1] Department of Health and Human Services' Office for Civil Rights. "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information." December 31, 2015.

[2] Verizon. "2014 Data Breach Investigations Report."

[3] Verizon. "2015 Data Breach Investigations Report."

[4] Humer, Caroline and Jim Finkle. "Your Medical Record is Worth More to Hackers Than Your Credit Card." *Reuters*. September 24, 2014.

[5] Sullivan, Tom. "The Surprisingly Small Percentage Health Orgs Spend on Data Security." *Government Health IT*. November 3, 2011.

[6] Nash, Kim S. "Information Technology Budgets: Which Industry Spends the Most?" *CIO*. November 2, 2007. www.cio.com/article/2437731/budget/information-technology-budgets--which-industry-spends-the-most-.html.

[7] Greenemeier, Larry. "Here's What a Cyber Warfare Arsenal Might Look Like." *Scientific American*. May 6, 2015. www.scientificamerican.com/article/here-s-what-a-cyber-warfare-arsenal-might-look-like/.

[8] Clarke, Richard. "Cybersecurity 2015: From Theft to Destruction." Presentation at HIMSS Privacy and Security Forum, December 1, 2015, in Boston, MA. http://boston.healthprivacyforum.com/cybersecurity-2015-theft-destruction.

[9] Walsh, Beth. "BCBS of Michigan Experiences ID Theft Impacting 5,500 Members." *Clinical Innovation + Technology*. March 12, 2015. www.clinical-innovation.com/topics/privacy-security/bcbs-michigan-experiences-id-theft-impacting-5500-members.

[10] Schlesinger, Jennifer. "Beware of Malicious Ads That Can Harm Computers Without a Click." CNBC. May 20, 2014. www.cnbc.com/2014/05/20/beware-of-malicious-ads-that-can-harm-computers-without-a-click.html.

[11] Department of Health and Human Services' Office for Civil Rights. "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information."

[12] Ragan, Steve. "Activism's Slippery Slope: Anonymous Targets Children's Hospital." CSO. April 24, 2014. www.csoonline.com/article/2147347/hacktivism/activisms-slippery-slope-anonymous-targets-childrens-hospital.html.

[13] Maruca, William. "Hacked Health Records Prized for their Black Market Value." *HIPAA, HITECH & HIT.* March 16, 2015. http://hipaahealthlaw.foxrothschild.com/2015/03/articles/privacy/hacked-health-records-prized-for-their-black-market-value/.

[14] PricewaterhouseCoopers. "HRI's Top Ten Health Industry Issues of 2016—Issue 4: Cybersecurity." 2016. www.pwc.com/us/en/health-industries/top-health-industry-issues/cybersecurity.html.

[15] "Hackers Directly Targeting Health Care Organizations, FBI Warns." *iHealthBeat*. August 21, 2014. www.ihealthbeat.org/articles/2014/8/21/hackers-directly-targeting-health-care-organizations-fbi-warns.

[16] 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.

[17] 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/.

[18] Anand, Priya. "How Long Does It Take To Hack a Company? Just Minutes, Report Says."

[19] Mandiant. "Beyond the Breach." 2014. https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.

Prepared By

Mark W. Dill, CISM, CRISC
Susan Lucci, RHIA, CHPS, CHDS, AHDI-F
Tom Walsh, CISSP

Acknowledgements

Barb Beckett, RHIT, CHPS
Aurae Beidler, MHA, RHIA, CHC, CHPS
Patricia Buttner, RHIA, CDIP, CHDA, CCS
Norma Chitvanni, RHIT, CHPS
Crystal Clack, MS, RHIA, CCS
Tammy Combs, RN, MSN, CCS, CCDS, CDIP
Karen Collins Gibson, MSA, RHIA, FAHIMA
Barb Glondys, RHIA

Elisa Gorton, MAHSM, RHIA, CHPS
Aviva Halpert, RHIA, CHPS
Lesley Kadlec, MA, RHIA, CHDA
Carol Maimone, RHIT, CCS
Marie Pirie-St. Pierre, RHIA
Linda Renn, RHIT, CCS, CPC, COC, CHTS-TR
Betty Rockendorf, MS, RHIA, CHTS-IM, CHPS
Angela Rose, MHA, RHIA, CHPS, FAHIMA
Joy Rose, MSA, RHIA, CCS
Donna Rugg, RHIT, CCS, CDIP
Jenny Utz, RHIT
Lou Ann Wiedemann, MS, RHIA, CDIP, CHDA, FAHIMA

Additional Practice Brief Content Available Online
www.ahima.org

There is an extended version of this Practice Brief online. For additional content, including a glossary of terms and informational sidebars, visit AHIMA's online HIM Body of Knowledge.

Article citation:
Dill, Mark W; Lucci, Susan; Walsh, Tom. "Understanding Cybersecurity: A Primer for HIM Professionals - Retired" *Journal of AHIMA* 87, no.4 (April 2016): 46-51 [extended web version].