Cybersecurity 101

Save to myBoK

By Susan Lucci, RHIA, CHPS, CHDS, AHDI-F, and Tom Walsh, CISSP

One of the most alarming statistics in the news, which is growing with intent and severity, is the prevalence of cyber-attacks, particularly in healthcare. It is an alarming trend that has gained a good deal of attention. For example, in July 2015, UCLA reported that up to 4.5 million patients' information may have been compromised. In March 2015, the Anthem hacking event affected nearly 80 million subscribers. Later the same month hackers may have accessed 11 million patients' data in an attack against the insurer Premera.

The sophistication and deliberate targets reveal that these threats are well-planned by organized criminals (i.e., Russian mafia) and nation states (i.e., North Korea, China, Iran, etc.) and are no longer the result of a basement hacker trying to gain access randomly to various business sites. Health information management (HIM) professionals need to be aware, more than ever, of cybersecurity threats and where their organization stores its protected health information (PHI) internally, as well as where their PHI is shared externally.

Hacking is Getting Worse

The US Department of Health and Human Services (HHS) has posted on their website a list of reported breaches affecting more than 500 patients, often referred to as the "wall of shame."[1] Although the percentage of hacking events seems relatively low at just 10 percent, the number of patients impacted is soaring at 72 percent of all patients affected. Since early 2010, when HHS first started publishing breach information, hacking events have affected a whopping 96 million individuals with over 93 million patient records being hacked in just the first six months of 2015.

Unlike some of the early cyber-events that targeted credit card data like Target, Home Depot, and similar events, hackers have now realized the increased value of healthcare data. This data gives criminals the ability to file false tax returns and fraudulent medical claims, obtain new identities, and also may provide access to healthcare services and prescription medications.

There is also growing concern that hacking events may be expanding beyond covered entities because healthcare regulations and business practices require patient data to be exchanged with:

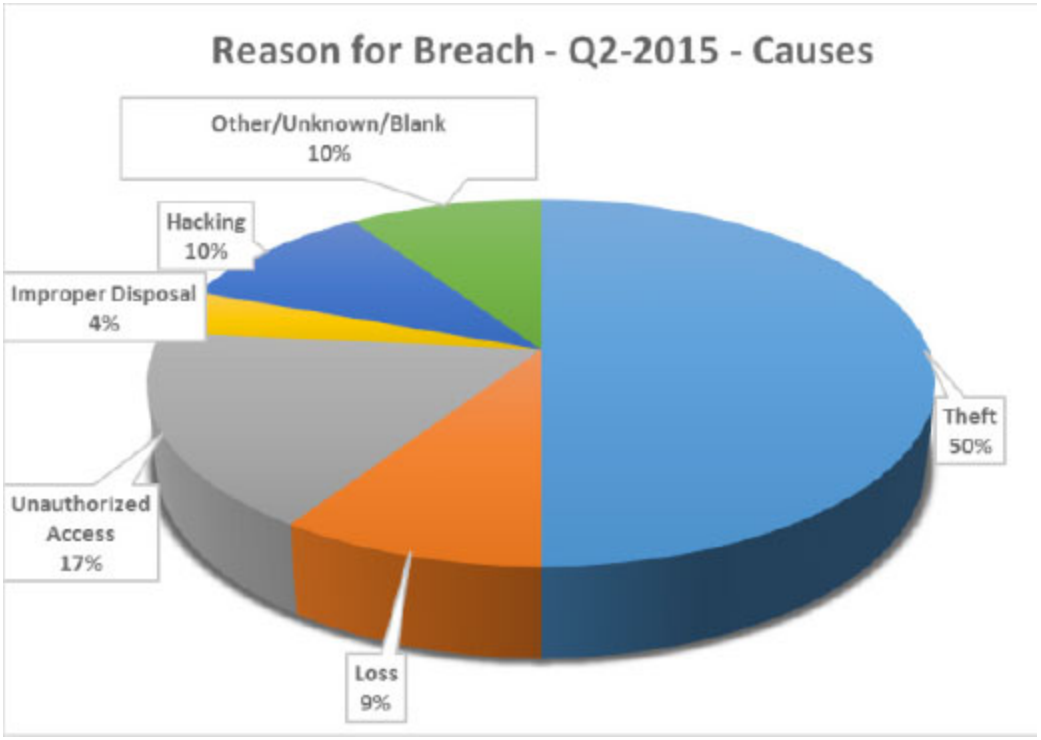
- Patients (i.e., patient portals, portable CDs, etc.)
- Other providers (i.e., e-mail, text messages, etc.)
- Clearinghouses and insurance companies for payment of claims/patient bills
- Government entities (i.e., state and federal agencies)
- Business associates to provide support services

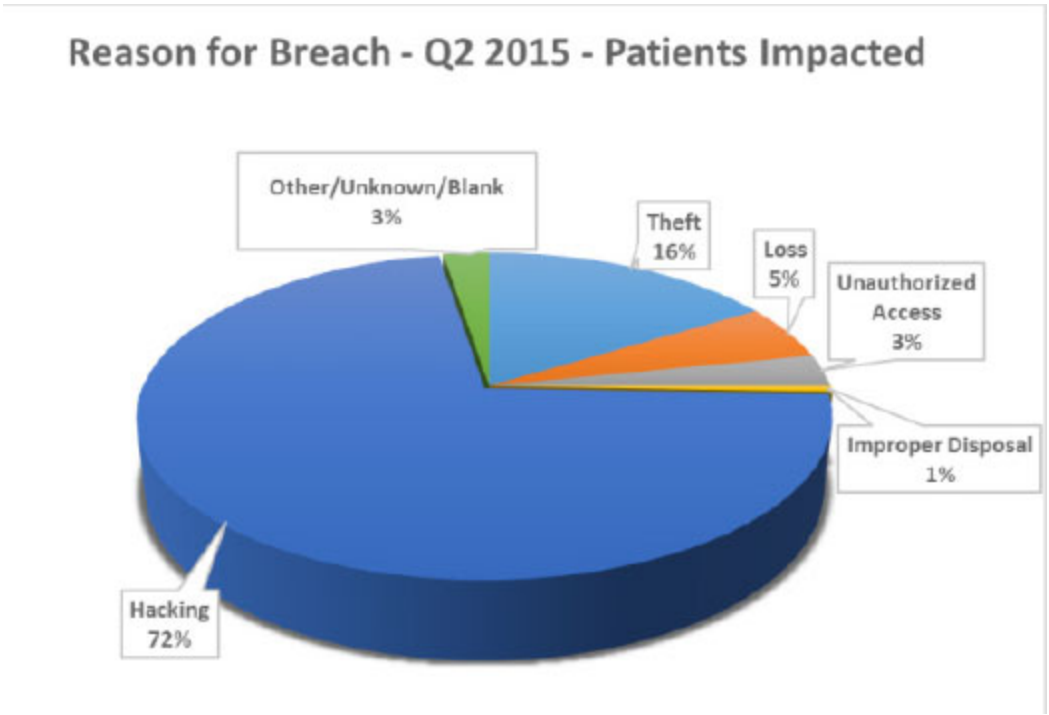
Any of these entities could experience a security breach that impacts patient data.

Business Associates On Watch

As of June 30, 2015, business associates were responsible for 277 reported breaches that affected over 500 patients, or 22 percent of all reported breaches since 2010. A total of 22,495,092 patients have been affected by those business associate breaches. Also, the HHS data shows that some business associates are not only being targeted, they are being hit again and again. For example, business Clear Point Design has had their network servers hacked four times. Blackhawk Consulting has had their network servers hacked three times. The firm E-Dreaming also has had their network servers successfully hacked twice. This should remind healthcare providers and HIM professionals that they need more than just a signature on a business associate agreement to feel confident that they have obtained "reasonable assurance" that the business associate has done their part toward securing the entity's data. Remember: compliance is not equivalent to security.

Figure 1: Charting the Causes, Impact, and Number of Data Hack Events





Year Reported to HHS	Number of Hacking Events Reported	Number of Patients Affected by Hacking Events
2010	10	568,358

2011	16	297,269
2012	16	900,684
2013	19	206,998
2014	31	1,786,630
2015	34	93,227,349

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." June 30, 2015. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Cybersecurity vs. Information Security vs. Computer Security

Computer security (an older term) and information security tend to focus primarily on computers (workstations and servers), mobile devices (laptops, smartphones, and tablets), networks, applications, and stored data or information (stored in databases, spreadsheets, documents, or on file servers).

Cybersecurity is part of information security, although today it is at the forefront of our attention. Today the word "cyber" is frequently used as an adjective to reflect the new emphasis of risks associated with the "Internet of Things"—which refers to "smart" devices or objects we do not often associate with computers but are connected to the Internet in some way. For example, automobiles, trains, home security systems, surveillance cameras, biomedical devices, health and fitness monitors, and building control systems (air handlers and/or water chillers), to name a few, all can interface with the Internet via smartphones.

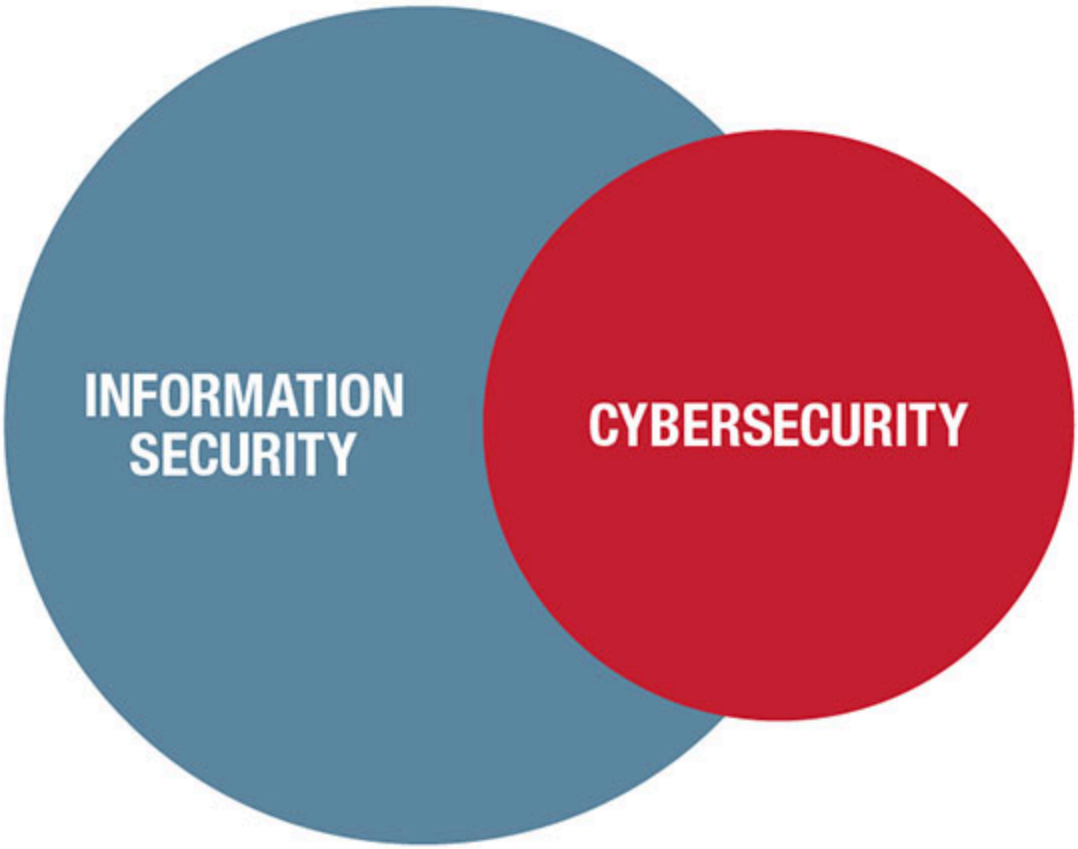
Essentially, anything that connects to the Internet is a potential target of a cyber-attack. HP Security Research reported in its 2014 "Internet of Things State of the Union Study" that besides patient data, hackers and cyber-criminals target:[2]

- User credentials (user IDs and passwords)
- Protected health information (PHI)
- Social Security numbers
- Credit card data and bank account numbers
- Research data and proprietary data
- Smartphones
- Biomedical devices

The fact that Sony Pictures was targeted in a cyber-attack through an e-mail earlier this year should serve as a reminder that there are many access points for hackers to get into an organization's data. This is why it is crucial to provide workforce reminders often. Malware is often introduced through bogus links on e-mail or e-mail attachments (called "phishing" because the criminals try to dupe a person to "take the bait" and click on an embedded link). Hackers and cyber-criminals are really good at making these messages look genuine.

It is also important to mention that healthcare organizations have been targeted with "ransomware" attacks using programs like cryptolocker. The hackers move in and encrypt all files with their code and then notify the facility of the hack, demanding a fee in order to decrypt the files. The message also states that for each day the ransom is not paid, the price to decrypt files goes up.

Figure 2: Cybersecurity is Part of Information Security



An Ounce of Prevention

Certainly the first step to protect your organization from some of these threats is to evaluate your current state and all possible points of entry. This essentially means conducting or updating the comprehensive security risk analyses on all systems, programs, and assets. Risk analysis is required by the HIPAA Security Rule (§164.308(a)(1)(ii)(A)) and the Payment Card Industry Data Security Standard (PCI DSS) (Standards 6.1 and 12.2). A risk analysis is the best opportunity to identify threats and vulnerabilities and to take action to mitigate cyber-threats.

Common risk analysis findings include organizations using the default manufacturers' system admin (generic) accounts; weak password rules; no antivirus software; no intrusion prevention system (IPS) to detect unauthorized activity; and sites that can be remotely accessed (vendor support) (i.e., interfaced through a Health Level Seven (HL7) gateway with the electronic health record (EHR)).

Also, many wireless biomedical devices are still using WEP encryption or no encryption, which is a risk, and organizations are using outdated/unpatched operating systems.
There are a number of ways that hackers can gain access to a facility's system. Therefore, security controls should be applied in layers, in what is commonly referred to as "security in depth." For example, controls are implemented to:

1. Prevent (Examples include: Access controls, antivirus software, encryption, and training)
2. Detect (Examples include: Intrusion detection/prevention systems, auditing and monitoring)
3. Ensure (Examples include: Risk analysis and management, vulnerability scanning, penetration testing, system evaluation and patch management)
4. Recover (Examples include: Backup media, system redundancy, incident response capability, forensic and/or investigation tools, disaster recovery)

Encryption is not the only process to protect an organization against these new cyber-threats. Most of the confidential and PHI data spends its time at rest. This is the data that is most vulnerable during a hacking-type event. The time may be right to investigate encryption or data masking to safeguard this data from a cyber-attack. Data masking retains the original structure of data but uses relative symbols to protect the actual data content. This practice reduces the risk of exposure to an organization's critical data.

The main point to remember is that the work to protect an organization from internal and external threats is never done. It is an ongoing process because threats are continually evolving and protection solutions must change with them. Hackers and cyber-attackers only need to get it right once. Healthcare organizations have to get it right every day. One weak link is all it takes for a hacker to get in.

Notes

1. US Department of Health and Human Services Office for Civil Rights. "Breach Portal: Notice to the Secretary of HHS Break of Unsecured Protected Health Information." June 30, 2015. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
2. Hewlett Packard Security Research. "Internet of Things State of the Union Study." July 2014. http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

Susan M. Lucci (slucci@justassociates.com) is a consultant and chief privacy officer at Just Associates. Tom Walsh (tom.walsh@tw-Security.com) is the president and CEO of tw-Security.

Article citation:
Lucci, Susan; Walsh, Tom. "Cybersecurity 101" *Journal of AHIMA* 86, no.11 (November 2015): 42-44.