RICOH
imagine. change.

Cyber Security Attacks on the Rise

Five Strategies To Arm Your Healthcare Organization

June 2016

Hackers Becoming Bolder With Healthcare

In a world where private health information (PHI) has become notably one of the most sought after and valuable assets, healthcare organizations must take a more active role in protecting their data. In fact, just this past year, healthcare skyrocketed to the top of the cyber attack list, overtaking financial institutions as the most hacked industry, according to IBM's 2016 Cyber Security Intelligence Index.[1]

Moreover, five of the eight largest healthcare security breaches since 2010 occurred in the first six months of 2015[2], compromising more than one million records. Healthcare data draws a high dollar on the black market because it is rich in personal data and valuable to identity thieves giving access to credit card information, email addresses, Social Security numbers, employment data and health history.

Unauthorized access is the number one incident category affecting healthcare, according to the IBM study, with 60% of attacks completed by insiders.[3] This is not surprising, given how difficult it is to secure health information due to multiple information touch points, a complex data string, consumer-generated data, efforts to capture paper data electronically and lack of resources to guard PHI.

Access to data is no longer the only cyber security concern. In the spring of 2016, cyber attacks appeared in a different form at several colleges, including Princeton University and the University of California, Los Angeles. These breaches saw a hacker accessing output devices, such as printers and fax machines, across the campus network to print anti-Semitic and racist flyers.[4]

The vulnerability of healthcare data security can give cyber criminals incentive to hack in growing numbers. The average number of healthcare cyber attacks rose to 3.4 per week for IBM clients participating in the survey. Meanwhile, small to medium healthcare organizations experienced one cyber attack each month, according to Ponemon Institute's State of Cybersecurity in Healthcare Organizations in a 2016 report.[5]

"Healthcare data draws a high dollar on the black market because it is rich in personal data and valuable to identity thieves giving access to credit card information, email addresses, Social Security numbers, employment data and health history."

Hackers became much bolder in the first quarter of 2016 with numerous healthcare systems experiencing attacks that shut down their entire system or disabled access to key patient information, forcing EHRs into downtime.

For example, Hollywood Presbyterian Medical Center experienced what could be considered cyber kidnapping.[6] The California hospital paid a "ransom" of $17,000 in bitcoin to a hacker who launched malware to seize control of its computer systems. Neither patient care nor patient and employee data was compromised, although the hack forced the hospital to resort to paper and pencil record keeping. The hospital CEO explained that meeting the monetary demand to obtain the decryption key was the fastest and most efficient way to restore normal operations.[7]

Meanwhile, 10 regional hospitals and 250 outpatient clinics operated by MedStar Health in the Washington, DC/Maryland area were crippled when hackers prevented the system's 30,000 employees and 6,000 affiliated physicians from logging into the computer system.[8] In another case, Methodist Hospital in Henderson, Kentucky, declared an internal state of emergency after ransomware invaded its computer system, taking control of files and compromising the internal network and other systems.[9]

[1] http://www-03.ibm.com/security/data-breach/cyber-security-index.html?platform=hootsuite
[2] http://www.healthcareitnews.com/news/five-eight-largest-healthcare-cybersecurity-breaches-2010-occurred-2015
[3] http://www-03.ibm.com/security/data-breach/cyber-security-index.html?platform=hootsuite
[4] http://www.nytimes.com/2016/03/29/nyregion/hacker-weev-says-he-printed-anti-semitic-and-racist-fliers-at-colleges-across-us.html?_r=2
[5] http://healthitsecurity.com/news/ponemon-healthcare-cyber-attack-averages-one-per-month
[6] http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#531f40a375b0
[7] http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#531f40a375b0
[8] http://www.cbsnews.com/news/fbi-probing-after-hackers-cripple-computer-systems-at-major-hospital-chain-medstar-health/
[9] http://www.healthcareitnews.com/news/methodist-hospital-recovering-five-day-ransomware-attack-claims-it-did-not-pay

Five Strategies to Help Arm Against a Cyber Attack

While these stats may be overwhelming, there are things you can do to help safeguard your organization.

As cyber attacks grow in frequency, cyber security is rapidly becoming a way of life in various industries. Because many healthcare organizations likely will be affected by cyber attacks at some point, taking proactive steps now can help you better prepare and respond in the case of a breach. Consider these five strategies to help build awareness and compliance to lessen the severity of a hack — not if, but more likely when it happens.

1 Understand and monitor data access points

More than half of attacks were carried out by an insider. Keep in mind this could be an employee, business associate or other third party with access to the system.[10] At the same time, take a close look at vendors and clearinghouses that receive and send patient data to be sure information is secure on both ends. Check to confirm vendors' patient data management processes meet HIPAA guidelines and that vendors have their own cyber security program in place.

Monitor access to workstation technology and output devices such as multifunction devices, traditional printers and fax machines to avoid breaches. Identify areas of risk and employ technology and services that enable healthcare organizations to remain hyper-vigilant in identifying areas of weakness and vulnerability. Review control safeguards that help identify lapses in data and device security. Also, shared devices that are critical to patient care may require a unique set of security safeguards.

2 Lock down workstations, printers and multifunction devices to help prevent unauthorized access

Healthcare's connectivity across technology devices and systems gives hackers more places to enter the system. Some technology has built-in safeguards such as badge scanning, thumbprint recognition or other user authentication mechanisms that can help detect breaches. However, it can help to confirm that security tools are installed and fully implemented in each device.

"Only 25% of IT professionals across all industry segments are confident in employee cyber security awareness.[11]"

3 Conduct comprehensive annual risk assessments at least once a year

Identify and understand the threats to the organization based on recent cyber attacks in healthcare and other industries and by using input from technology vendors. Include actual hacking attempts based on real-life scenarios of data management systems and processes to evaluate vulnerability. Consider hiring professional hackers as security watchdogs to test the network and the cloud and to identify gaps in the system. At the same time, use mock hacks and phishing email attacks to not only test employees, but to also identify where additional staff training may be required.

It can help to include mobile devices in the assessment to verify proper use in conjunction with both cyber security and HIPAA requirements. Combine all assessment findings to create and test a cyber attack response plan, which can include well-defined downtime procedures for processing information on paper by hand until the system is back up and running securely.

[10] http://www.fiercehealthit.com/story/healthcare-no-1-target-cyberattacks-2015/2016-04-20
[11] http://business-reporter.co.uk/2016/03/21/only-quarter-it-professionals-confident-employee-cyber-security-awareness/

Five Strategies to Help Arm Against a Cyber Attack

4 Educate every end user on cyber security in addition to HIPAA requirements

Only 25% of IT professionals across all industry segments are confident in employee cyber security awareness.[11] In fact, the same group indicated the first improvement they would make to bolster cyber security is increased employee training. This starts by helping staff and physicians differentiate between cyber security and HIPAA requirements.

One approach to consider is to train staff on the appropriate procedures to follow when they suddenly can't access files on a shared server or experience some other unusual event while on the system. Include actual examples of seemingly harmless hacker techniques such as phishing emails with malicious attachments or URLs that can infect and even disable the entire system with one click.

For instance, the Methodist Hospital hack came in the form of an email about invoices and indicated the recipient needed to open the attached file, which was booby-trapped.[12] The severity of the attack may have been lessened with training, as studies report an average drop in clicks from 15.9% to 1.2% among companies that implemented security awareness training.[13]

5 Review how business systems and processes support security

A thorough analysis of all aspects of data collection, storage and use can help drive improvements and support tighter cyber security measures. Include these key business systems as part of an internal review of cyber security preparedness:

- **Business Process Optimization** — Examine current processes and operations to help identify security gaps while also looking for ways to improve efficiency.
- **Asset Management** — Monitor vulnerabilities by constantly scanning and reporting enterprise technology assets regardless of make, model or location and how those assets work together to help support the organization.
- **Content Management** — Evaluate how clinical and administrative data is captured and linked to internal systems to help improve business and clinical processes in a way that can reduce exposure.
- **Fax Server** — Confirm the secure organization and flow of internal and external information between internal and external devices.
- **Forms Management** — Review the capture, management and flow of clinical and administrative information to help guarantee that data is safely and securely handled, as well as to help reduce the chance of information mismanagement and human error.
- **Interoperability** — Look at all the ways patient data is typically shared, from an unstructured, analog method to a digital, electronic transfer method.
- **Output Management** — Monitor and audit enterprise printing to help address the need for confidentiality, misdirected or forgotten print jobs or unauthorized access.
- **Point of Service Scanning** — Assess how capturing and directly linking clinical and administrative data to internal systems at the point of service can help reduce potential exposure.
- **Hardware** — Gauge how well the organization uses hardware by examining steps such as user authentication at the printer, encryption to help safeguard documents, data, address books, passwords and more, automatically overwriting latent digital images and managing unstructured data.

[11] http://business-reporter.co.uk/2016/03/21/only-quarter-it-professionals-confident-employee-cyber-security-awareness/
[12] http://krebsonsecurity.com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/#more-34322
[13] https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

Cyber Attacks: A Trend That Cannot Be Ignored

2016 is the year "ransomware" holds America hostage, according to the Institute for Critical Infrastructure Technology (ICIF).[14] Healthcare may be among the top targets because it relies on up-to-date information and records to provide care, making healthcare organizations more likely to pay to quickly restore their data and resume normal operations.

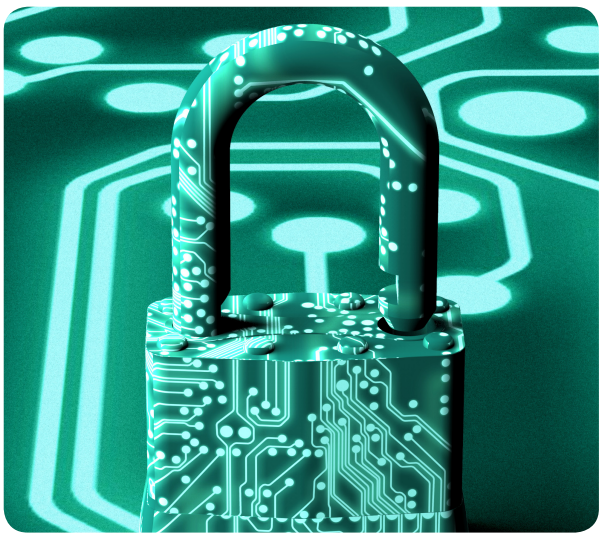
Whether a stolen laptop with PHI or a hacker that gains access to and disrupts the entire system, statistics show the threat of a cyber attack and data breach affecting a healthcare organization is higher than ever before.

While most cyber attacks this year have not disrupted clinical care or exposed private patient or employee data, the potential for these things to occur is real and growing. The weakest link in any computer system is often the user, and organizations should take advantage of technology capabilities to help identify weaknesses and prevent unauthorized access.

Beyond enabling proper data backup systems and recovery processes, it can help organizations to be able to identify and understand the initial point of exposure and close the gap to prevent future attacks. This level of proactive preparation often requires a mix of people, processes, policies and technology.

Cyber attacks are a growing trend that will likely demand new attention and strategies to proactively evade these highly dangerous and disruptive threats. If you wait until the attack has occurred, you've likely waited too long.

"Cyber attacks are a growing trend that will likely demand new attention and strategies to proactively evade these highly dangerous and disruptive threats. If you wait until the attack has occurred, you've likely waited too long."



For more information visit
ricoh-usa.com/healthcare

RICOH
imagine. change.

[14] http://icitech.org/publications/