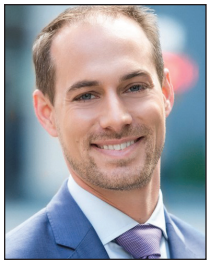
By Christopher Karambelas

Health Care Technology: Ransomware Risk and Protection



Christopher Karambelas
ToneyKorf Partners
New York

Chris Karambelas, CIRA, CHFP is a director with ToneyKorf Partners in New York. His practice includes restructuring advising, finance and health care, and he has more than 10 years of experience in project management and data analytics.

Advances in technology, especially information technology (IT), have improved and critically accelerated the delivery of health care. However, great innovation has also opened new avenues for fast, frightening and broad-scale criminal activity. Rigorous, proactive, state-of-the-art protection is available and absolutely necessary.

The rapid advance of health care technology is helping to reduce inpatient visits, lowering the length of patient stays, and improving information-sharing among an array of user groups with multiple data points. As more digital data points are gathered and stored to create a thorough and complete patient record, the more that physicians and other caregivers rely on the information to make clinical decisions in treatment planning and to understand the full scope of the patient's treatment history.

While the electronic record has improved the standard level of care by providing access to real-time information, not having the health record readily available could put patient care in jeopardy. This dependency on the medical record sets the stage for hackers to hold the information hostage for a hefty reward. The software created to do this is commonly known as "ransomware."

Malware, specifically ransomware, is becoming more common across all industries. Hackers gain access to business networks or personal devices when users click on infected links, open attachments from unknown sources or view at-risk websites. Once access is obtained, hackers then have the ability to take over and lock the user's technology systems or view and encrypt critical files. They then demand that funds be transferred before the businesses or individuals are allowed to regain control of their digital environment.

The stakes can be life or death for patients. These cyberthreats can have catastrophic implications, directly impacting patient care delivery especially when access to protected health information (PHI) becomes compromised or inaccessible. Integrated systems and cloud-based solutions add to the complexity of the issue. Hackers making demands on compromised networks and systems can require health care organizations to pay millions of dollars to regain access to patient records.

Government Actions and Requirements

Advances in technology, and the accessibility of information, are thought to be so important that the federal government implemented the Health Information Technology for Economic and Clinical Health (HITECH) Act in early 2009. Led by the Centers for Medicare and Medicaid Services (CMS), the HITECH Act incentivizes caregivers to implement electronic health record (EHR) systems that meet various metrics within multiple stages under the Meaningful Use program.

Since 2009, nearly all delivery networks have complied with the Meaningful Use program. Paper records have been moved to electronic formats, allowing patient data to be accessed in real time across the patient care continuum (including providers, payers and applicable government agencies).

Ransomware Attacks on the Rise

Recent statistics show that in 2019, more than 950 ransomware attacks were reported, with an estimated total cost of more than $7.5 billion.[1] *Of the reported cases, nearly 80 percent are specific to the health care industry.* In December 2019, Hackensack Meridian Health, one of New Jersey's largest health systems, was hit by a ransomware attack in early December 2019.[2] The incident caused serious disruption to patient care and hospital operations, requiring the organization to reschedule non-emergent procedures and revert to documenting patient information on paper charts.

The network and systems were unavailable for two days. All impacted systems returned to normal after several additional days. Although the amount has not been disclosed, Hackensack Meridian officials stated that a ransom payment was made to release the information.

Grays Harbor Community Hospital in Washington state was hit with a similar attack in mid-2019.[3] The attack occurred after an employee clicked a malicious link in a phishing email (a fraudulent email that appears to be from a "trust-

1 "The State of Ransomware in the US: Report and Statistics 2019," Emsisoft Malware Lab (Dec. 12, 2019), *available at* blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019 (unless otherwise specified, all links in this article were last visited on Jan. 22, 2020).

2 Jessica Davis, "Ransomware Attacks Disrupt Patient Care at Hawaii, NJ Hospitals," Health IT Security (Dec. 16, 2019), *available at* healthitsecurity.com/news/ransomware-attacks-disrupt-patient-care-at-hawaii-nj-hospitals.

3 Jessica Davis, "Hackers Demand $1M in Grays Harbor Ransomware Attack," Health IT Security (Aug. 14, 2019), *available at* healthitsecurity.com/news/hackers-demand-1m-in-grays-harbor-ransomware-attack.

ed" source). The system breach spread through the hospital's network over a weekend when IT resources were low. This attack impacted off-site clinics and, like Hackensack Meridian, required operations to move to paper records.

Cash flows are often tight at community hospitals, so any impact on cash collections and billings, even for a few days, can create financial havoc. The Federal Bureau of Investigation (FBI) was contacted and, as required by law under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 85,000 patients were notified of the event.

Health systems are not the only targets for ransomware in the health care industry. In 2017, Nuance Communications, a software company that provides speech translation and imaging technology solutions, was also hit with a malware attack, costing Nuance more than $92 million in lost revenue.[4] The breach spread throughout Nuance's customer base, resulting in litigation from health systems for lost IT infrastructure. Nuance's impacted health care clients were forced to move to downtime procedures while impacted systems were unavailable.

In most ransomware attacks, the hacker group is typically only interested in encrypting files and holding those files hostage. In the event that PHI is accessed and released, the health system could face class action lawsuits, as well as related fines from the Office of Civil Rights (OCR). The 2016 breach and cyberattack on the Phoenix-based Banner Health system exposed the PHI of 2.9 million people, including approximately 30,000 credit card numbers stored on Banner's IT servers. A class action lawsuit alleged that the health system failed to implement adequate security protocols and infrastructure that could have alleviated the breach; the resulting settlement was $6 million.[5] An OCR investigation of Banner Health is ongoing.

Minimizing the Risk of Attacks

Although hackers are continuously finding new and creative ways to wreak havoc and chaos on an organization, there are preventive measures that institutions can promote internally to mitigate the risks of cyberattacks. The following proactive recommendations should be followed to reduce the risk of cyberthreats.

Education

Keep staff informed on current threats and common trends. This action will make staff less likely to open attachments or click links in emails from unknown sources. Conduct internal phishing tests, which can help educate staff who have clicked test links. Incorporate current security risks and past occurrences of breaches into established annual training sessions. This can be an effective medium for the continuing educating of employees.

Third-Party Software

Implement reputable protective software and keep it up to date. Block the installation of third-party software on employee computers, which can also help alleviate unnecessary security risks.

Backup and Recovery Plan

Ensure that critical data is backed up on a regular basis and stored remotely. In addition, develop a recovery plan should data become corrupt or compromised. Require authorization for installations of nonstandard software on employees' work machines.

Backup and Recovery Plan/Firewall

Ensure that critical data is backed up on a regular basis and stored remotely. Develop a detailed recovery plan should data become corrupt or compromised. In addition, ensure that a strong firewall is in place and monitored frequently.

IP Addresses

Restrict access to allow IP addresses only from known locations into your environment. Specifically, block international IP addresses other than those that are known and approved.

Patches and Updates/Email Scanning

Maintain current security server patches and updates on local devices while also implementing a robust testing program. Also, implement content scanning on exchange servers for inbound messaging.

Other Methods

Enlisting the resources of a third-party professional firm to perform a full security risk assessment will also provide an organization with insight into areas of weakness in its IT infrastructure. The third party conducting the assessment will perform a full review of all critical assets making up the IT system (*e.g.*, network, servers and applications), provide recommendations for risk mitigation, and create a framework for a standard level of security based on industry trends. Organizations can also use these assessments to meet compliance requirements for the HIPAA Security Rule as established by the Department of Health and Human Services (HHS) to ensure that patients' PHI is being protected.

Another way to bolster security is to work with a firm that performs "ethical hacking." These firms are hired to conduct penetration and vulnerability tests to find potential weaknesses in an organization's environment. Conducting both a security risk assessment and ethical hacking testing on an annual basis allows the organization to stay current with new threats and implement industry-wide best practices.

Although these preventive measures help to alleviate risks, there is always the chance that operational and financial disruption could occur from malware attacks. Internally maintaining, reviewing and training staff in downtime procedures on a routine basis will allow a health system to stay current with patient care processes should access to patient records become unavailable for an extended period of time.

continued on page 56

4 Heather Landi, "Banner Health Agrees to $6M Settlement to Resolve 2016 Data Breach Lawsuit," Fierce Healthcare (Dec. 9, 2019), *available at* fiercehealthcare.com/hospitals-health-systems/banner-health-reaches-proposed-6m-settlement-2016-data-breach.

5 Steve Ragan, "Nuance Says NotPetya Attack Led to $92 Million in Lost Revenue," CSO (Feb. 28, 2018), *available at* csoonline.com/article/3258768/nuance-says-notpetya-attack-led-to-92-million-in-lost-revenue.html.

from page 31

In the event that hackers breach security measures and hold data for ransom, it is important to notify the FBI and HHS immediately, while also working to stop the spread of the virus. Paying ransom is discouraged, as it might promote future activity and does not guarantee the release of data to its original state. However, patient care is the highest priority, and paying a ransom might be necessary. Obtaining cyberinsurance might reduce the financial burden caused by a breach. Further, reputable cyberinsurance providers will review the organization's systems and recommend or require certain IT infrastructure standards or changes in order to obtain and maintain valid coverage.

Conclusion

Breaches and cyberattacks are escalating rapidly, and hospitals and health care organizations are prime targets for being "held up" for the release of encrypted information. As IT and the reliance on technology continue to evolve, the risk of security threats on all organizations escalate. It is important to be proactive in implementing solutions that protect your data, keeping your employees aware of new threats, and staying informed of industry risks and trends. Inattention to the risks can result in significant operational and financial burdens, including patient harm, negative publicity, litigation, fines, cash-flow disruptions and the use of significant operating resources. abi