

Hospitals and Healthcare Systems Are the New Ransomware Target: How to Avoid Becoming a Hostage

By Gregory P. Silberman and
Alexandra A. McDonald



In February 2016, a Los Angeles-based hospital paid cyber criminals \$17,000, in the form of 40 Bitcoins, to restore access to its electronic medical records and e-mail systems. The hospital—Hollywood Presbyterian Medical Center—was taken offline for more than a week when a ransomware attack denied access to the hospital’s electronic records. The attack made electronic documentation of patient care, transmittal of lab work, and sharing of CT and x-ray results impossible, and doctors lost critical access to patients’ medical histories. As a result of a similar attack, Methodist Hospital in Henderson, Kentucky, declared a “state of emergency” when it lost access to patient files for a number of days. Hospitals and healthcare systems (collectively, “healthcare organizations”) are especially vulnerable to being targeted because of their dependence on information technology and the perceived public safety risks such attacks pose. For healthcare organizations, the best way to survive a ransomware attack is to understand the threat, have a plan, and be prepared.

What is ransomware?

Ransomware, more specifically, cryptoransomware, is a type of malware designed to block access to computer systems and data by encrypting files using strong encryption and threatening to destroy the decryption key and, with it,

access to the encrypted files, unless a ransom payment is made to restore access. Historically, most ransomware incidents were the result of computer users opening malicious e-mail attachments or visiting compromised websites.

Recently, more sophisticated attacks have been using ransomware to monetize targeted network intrusions. These attacks encrypt not only the initial host’s hard drive but also external and shared drives to which the infected computer has access and actively seek out backup files to encrypt in order to hinder recovery efforts. Without payment, the encryption key(s) used in a ransomware attack will typically be irrecoverable and the affected systems will remain inaccessible, potentially resulting in loss of sensitive or proprietary information, disruption of business, financial loss, and reputational harm.

Why target healthcare organizations?

Ransomware is a growing trend in cybersecurity threats, prompting warnings from the FBI,¹ as well as the U.S. Department of Homeland Security² and Canadian Cyber Incident Response Centre.³ While no business is immune, healthcare organizations appear particularly vulnerable for several reasons.

High risk, high reward. Ransomware against a hospital puts health and lives at risk, which means the cyber criminals are more likely to earn a quick and easy payout. When faced with an unprecedented loss of access to medical records, communications systems, and even connected medical devices, health organizations may feel compelled to pay a significant ransom to restore operations, ensure the safety of patients and preserve public image.

Easy targets. Healthcare organizations went digital at a later point than other industries,⁴ with the vast majority only transitioning to electronic records systems between 2008 and 2014. However, in response to a variety of incentives and benefits, they have rapidly adopted many new technologies. In many instances, security technologies and procedures have not been implemented at the same pace and take a backseat to those focused on patient care.

Vulnerable devices. In addition to network vulnerabilities, many connected medical devices, including imaging equipment, fetal monitors, and IV pumps, running outdated operating systems attract cyber criminals. The U.S. Food and Drug Administration recently published draft guidelines⁵ recommending medical device manufacturers address cybersecurity vulnerabilities, noting that all medical devices that use

“Ransomware against a hospital puts health and lives at risk, which means the cyber criminals are more likely to earn a quick and easy payout. In addition to network vulnerabilities, many connected medical devices, including imaging equipment, fetal monitors, and IV pumps, running outdated operating systems attract cyber criminals.”

software and are connected to hospital and healthcare organizations’ networks have vulnerabilities—some of which can be proactively protected against, whereas others require vigilant monitoring and timely remediation.

How to prepare for a ransomware attack

Evaluate the risk. Healthcare organizations should evaluate their security posture by performing a risk assessment of their networks and systems, and then preparing an inventory of critical assets. The results should be used to drive the development of an incident response plan.

Plan your response. It is imperative to have a plan for responding to a ransomware incident well before an attack happens. An incident-response plan should include procedures that are specific to this type of threat, including detailed roles, responsibilities, and actions that you can take as soon as the organization becomes aware of an active attack. Although law enforcement agencies advise against making ransom payments, evaluating whether there are circumstances under which an organization might pay a ransom will avoid irrational decisions in the heat of the moment.

Test your plan. While it is important to have a written incident response plan, it is equally important to test and update the plan over time.


Disaster recovery and backups. Having a comprehensive disaster recovery plan in place is the only way to ensure the safety of data in the event of an attack. Knowing what data and applications are on which servers can be critical. Important data must be backed up, and the ability to restore those backed-up files from offline sources should be regularly tested.

Security awareness. Implement security-awareness training for all users who have access to the systems, including employees, physicians, and patients, underscoring the danger of opening attachments or links in unsolicited e-mails, even if they appear to come from within your organization. While some ransomware attacks begin by exploiting system vulnerabilities, the majority still rely on social engineering to compromise users.

Retain cybersecurity and legal service providers. Retain cybersecurity and legal service providers in advance of an attack and integrate their roles and responsibilities into disaster-recovery and incident-response plans. Retaining service providers in advance will save valuable time during the critical 24 to 72 hours after an attack.

Evaluate cyber insurance coverage. Organizations should review their insurance policies to understand the coverage provided for damages associated with ransomware attacks, including business interruption, remediation, and ransom payments. How an organization plans for and responds to an attack may significantly impact its insurance recovery.

Conclusion

While there is no way for healthcare organizations to avoid being targeted by cyber criminals or completely eliminate the risk posed by ransomware, planning and preparation can reduce the risk and limit the damage. 

References

1. <https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise>
2. <https://www.us-cert.gov/ncas/alerts/TA16-091A>
3. <http://www.publicsafety.gc.ca/cnt/ntnl-scr/cbr-scr/ccirc-ccric-en.aspx>
4. <https://www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf>
5. <http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm>

Gregory P. Silberman is a partner in the Silicon Valley office, and Alexandra A. McDonald is an associate in the San Francisco office, of Jones Day.

Disclaimer

The views and opinions set forth herein are the personal views or opinions of the authors; they do not necessarily reflect views or opinions of the law firm with which they are associated.