Published on *The National Law Review* https://natlawreview.com

Is Your Business Prepared for the Ransomware Epidemic?

Article By:

Matthew R. Baker

Doron S. Goldstein

Megan Hardiman

Earlier this month, the Federal Trade Commission (FTC) kicked off its fall technology series with a workshop on the growing threat of ransomware. Ransomware is an increasingly common and insidious form of malware that locks away data, holding it hostage in an attempt to extort money from system owners.

According to some experts, ransomware is the most profitable form of malware in history. While not a new phenomenon, the threat presented by ransomware has reached epidemic status in 2016:

- 54 percent of 540 businesses surveyed were attacked by ransomware in the past 12 months, with health care and financial services the most common targets.[1] Banks have begun to prepare for ransomware infection by stocking tens of thousands of dollars in Bitcoin so that they can pay a ransom if necessary.[2]
- The FBI reported that an average of more than 4,000 ransomware attacks were recorded each day in 2016, up from approximately 1,000 ransomware attacks each day in 2015.[3]
- One survey showed that 72 percent of companies could not access their data for at least two days after a ransomware infection and 32 percent were locked out for five or more days, resulting in significant losses due to downtime.[4]
- Almost 1.2 million new variants of ransomware were detected in Q1 2016 alone.[5]
- Many organizations, including hospitals[6] and police departments,[7] have paid significant sums to hackers to unlock encrypted data,[8] with an estimated $375 million in ransoms paid out so far this year.[9]
- Paying a ransom does not guarantee data recovery.[10] One cybersecurity firm found that 7 percent of businesses who paid a ransom did not have their data restored.[11]

Given the increasing prevalence and sophistication of a ransomware attacks, organizations should take steps now to reduce the risk of infection and minimize the impact of an attack. Basic steps include: 1) incorporating the risks of ransomware and other malware into the organization's security risk analysis and risk management program; 2) implementing technical, access, and other procedures to guard against, detect, and limit the effects of malware, including ransomware; 3) training personnel on how to recognize, avoid, and report cybersecurity threats; and 4) maintaining and regularly testing the effectiveness of the organization's data incident response and business continuity programs, including the scope and frequency of data backup and recovery processes.

Health Care as a Case Study

Nowhere are the dangers presented by ransomware more evident than in the health care industry, which has become an increasingly common target for ransomware attacks. Ransomware disruptions to health care systems can have particularly severe and even life-threatening consequences, increasing the chance that affected organizations will pay a ransom.

Indeed, hospitals faced several highly publicized attacks in 2016:

- Hollywood Presbyterian Medical Center in Los Angeles paid hackers $17,000 in Bitcoins after Locky, a ransomware variant, took its computers offline for more than a week in February.[19]
- Methodist Hospital in Henderson, Kentucky was also struck by Locky in March, although it was able to bring its systems back online within a few days by restoring from backups.[20]
- When ransomware took down MedStar's systems in March, it delayed lab results, interfered with treatments, and prevented access to electronic medical records in ten hospitals and more than 250 outpatient centers in Maryland and the Washington, DC area.[21]
- Kansas Heart Hospital was attacked in March and elected to pay a ransom. The hackers, however, only unlocked some of the encrypted data and demanded a second payment to unlock the rest, which the hospital declined.[22]

Health care organizations also face heightened regulatory consequences from ransomware infection. The Department of Health and Human Services (HHS) considers the mere *presence* of ransomware (or any malware) on covered organizations' systems to be a "security incident," which triggers incident response and reporting mechanisms.[23]

Further, if electronically stored protected health information (PHI) is *encrypted* by ransomware, a breach of PHI is presumed to have occurred.[24] This potentially triggers breach notification requirements to the Secretary of HHS, the affected individuals, and—in some cases—the news media.[25]

What is Ransomware?

Ransomware is a devastating form of malware that encrypts or otherwise "locks up" computer systems and data, preventing use or access. After data is encrypted, ransomware typically informs the user of the infection and threatens to delete the commandeered data if a monetary ransom is not paid within a short time. Particularly dangerous strains of ransomware transfer copies of encrypted data back to the deploying hacker, while others pretend to be ransomware but destroy data outright

rather than encrypting it.[12]

Ransomware typically enters a system due to an end-user clicking a link in an email, visiting an infected website, or opening an infected email attachment.[13] However, emerging strains of ransomware can also spread *without user interaction* through server or software vulnerabilities or be distributed automatically by malvertising.[14] Once inside a system, ransomware will often attempt to spread to other connected systems, making early detection and response critical to preventing a widespread infection.

The Consequences of a Ransomware Infection

Ransomware presents three primary areas of risk to organizations:

- *System Downtime.* Ransomware infections can render entire systems and networks unusable. Most infected organizations suffer two or more days of system downtime that can cause disruption and significant operational losses.[15]

- *Data Loss.* An infection can result in temporary or permanent loss of data.[16] While the risks associated with such losses vary depending on the details of the organization and the affected data, the consequences can range from mild to severe harm to the organization and its affected customers or clients.

- *Legal and Regulatory Exposure.* Because ransomware can access, destroy, alter, and even transfer data to third parties, an infection can trigger security incident or data breach reporting requirements. Affected organizations may also face lawsuits and enforcement actions under privacy, data breach notification, and data protection laws.[17]

The harms associated with a ransomware infection can be significant. Victims of ransomware reported that the attacks cost them $209 million in just the first quarter of 2016.[18] As these numbers only reflect the fraction of ransomware attacks actually reported to the FBI, losses for that period are likely much larger.

How to Prepare for Ransomware Threats

Prevention and preparation are critical when it comes to ransomware protection. Organizations can reduce the risk of ransomware infection and mitigate its effects by taking several basic steps now, such as:

- *Risk Analysis.* Conducting regular risk analyses to identify vulnerabilities and threats to critical information is an integral part of any information security program. The risks associated with malware and ransomware should be incorporated into the organization's risk analyses.

- *Incident Response and Business Continuity Planning.* A swift, organized response to a ransomware infection is critical in limiting or mitigating associated harms. Having an "actionable" data incident response and business continuity plan in place, as well as a crisis communications plan, can significantly improve an organization's response to a ransomware attack. Regularly testing these plans through table top and other exercises is the key to making them actionable. A ransomware attack is a great topic for a table top exercise.

- *Regular Backups.* Ransomware's defining characteristic is denying access to data. Maintaining regular segregated backups can minimize disruption to operations in the event critical files are encrypted or deleted. Some variants of ransomware can remove or disrupt linked or live backups, so organizations should at least consider maintaining fully-segregated and/or offline backups of critical or protected data. By testing their data backup and recovery processes in advance of an attack, organizations can identify unexpected limitations in the frequency or effectiveness of these systems and take steps to shore these up in advance.

- *Workforce Training.* Employee errors are the most common infection vectors for most malware. Employees are also in a position to provide early warning of ransomware infections. As a result, employees and other workforce members should be trained and encouraged to identify, avoid, and promptly report not only suspicious emails, but suspicious computer activity in general. For example, organizations can send "test" emails to periodically assess their employees' ability to identify and properly report "phishing" campaigns and other attack vectors.

- *Technical Safeguards.* Technical safeguards, such as anti-malware programs, can be used to block suspicious emails and attachments before they are opened. Disabling macros in email attachments may prevent an incident in the event an infected document is opened. Limiting installation permissions, implementing software restriction policies and whitelists, and ensuring software and firmware are regularly updated with security patches can help prevent malware from installing itself on systems. Protecting, monitoring, and reviewing access logs for Internet-accessible devices can detect suspicious activity, such as data exfiltration attempts. Finally, organizations should implement mobile device management practices and software to address the risk of infection or data loss through employee mobile devices, such as cell phones, tablets, and laptops.

- *Access Controls.* Ransomware typically only has access to the files, permissions, and resources of the particular compromised user account. All organizations should implement access controls using the principle of "least privilege" to limit access to data so that user accounts are only able to access information and network resources necessary to carry out their duties, and so that not every compromised user infects the whole system. Additionally, firewalls, password protections, and other measures should be used to limit access to critical information and systems. These measures reduce the likelihood that an infection will reach sensitive data or spread throughout a network.

- *Vendor Management.* Vendors that have access to an organization's networks, systems, or data can introduce malware and ransomware just like any other user. Organizations should review vendors' security and compliance practices prior to engagement and periodically thereafter, and should ensure that vendor contractual obligations include security standards, incident notification requirements, and appropriate allocations of liability in the event of a breach or other security incident.

- *Insurance.* Some cyber-insurance policies now offer cyber-extortion and similar coverage that may apply to these types of incidents. Organizations should consider reviewing coverage options with their insurance provider or broker.

Note that these measures form only the foundation of a data security program. Organizations may be subject to other sector-specific legal or contractual security requirements and should take additional

steps as necessary to protect themselves and their data based on their own operations and related risk profile.

---

[1] Osterman Research, *Understanding the Depth of the Global Ransomware Problem 1* (2016).

[2] James Cook, *Banks are stockpiling Bitcoins in case they get hit with ransomware*, *Business Insider* (Aug. 11, 2016), available here.

[3] United States Government Interagency Guidance Document, *How to Protect Your Networks from Ransomware*, available here.

[4] John P. Mello Jr., *Ransomware's Aftermath Can Be More Costly Than Ransom*, *TechNewsWorld* (Mar. 24, 2016), available here.

[5] McAfee Labs Threats Report June 2016, 46, available here.

[6] One cautionary case involved Hollywood Presbyterian Hospital, which, after a failed attempt to circumvent the ransomware by resorting to paper and pencil, paid $17,000.00 to unlock their systems. *See* Keith Wagstaff, *Big Paydays Force Hospitals to Prepare for Ransomware Attacks*, NBC News (Apr. 23, 2016), available here.

[7] Hiawatha Bray, *When Hackers Cripple Data, Police Departments Pay Ransom*, *Boston Globe* (Apr. 6, 2015), available here.

[8] Josephine Wolff, *The New Economics of Cybercrime*, *The Atlantic* (June 7, 2016), available here.

[9] Adam Chandler, *How Ransomware Became a Billion-Dollar Nightmare for Businesses*, *The Atlantic* (Sept. 3, 2016), available here.

[10] Federal Bureau of Investigation*, Incidents of Ransomware on the Rise: Protect Yourself and Your Organization*, FBI.gov (Apr. 29, 2016), available here.

[11] Chandler, *supra* note 9.

[12] Sean Gallagher, *Posing As Ransomware, Windows Malware just Deletes Victims' Files*, *ArsTechnica* (July 12, 2016), available here.

[13] Common vectors include PDFs, image files, Microsoft Office documents, and compressed archives, such as .zip or .rar files. Unfortunately, these file types are exceptionally common email attachments; thus, it is important to train end-users to recognize and report suspicious emails.

[14] "Malvertising" is a method of distributing malware through online advertising networks and can result in infection simply by visiting a page with an infected advertisement. Even large, trusted websites such as MSN.com have suffered from malvertising campaigns, which are often used to deploy ransomware. *See* Wendy Zamora, *Truth in malvertising: How to beat bad ads*, MalwarebytesLABS (June 13, 2016), available here.

[15] Mello, *supra* note 4.

[16] Federal Bureau of Investigation*, Incidents of Ransomware on the Rise: Protect Yourself and Your Organization*, FBI.gov (Apr. 29, 2016), available here.

[17] In its September 2016 workshop, the FTC indicated that it will continue to bring enforcement actions against organizations whose cybersecurity protections it deems insufficient.

[18] Chandler, *supra* note 9.

[19] Seung Lee, *Ransomware Wreaking Havoc in American and Canadian Hospitals*, *Newsweek* (Mar. 23, 2016), available here.

[20] Kim Zetter, *Why Hospitals are the Perfect Targets for Ransomware*, *Wired* (Mar. 30, 2016), available here.

[21] John Woodrow Cox, *MedStar Health turns away patients after likely ransomware cyberattack*, *The Washington Post* (March 29, 2016), available here.

[22] Bill Siwicki, *Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money*, *Healthcare IT News* (May 23, 2016), available here.

[23] US Department of Health and Human Services., *FACT SHEET: Ransomware and HIPAA 4* (July 11, 2016), available here.

[24] HHS considers ransomware's encryption of PHI to be an "acquisition" of that data because unauthorized individuals have taken possession or control of that information. *See id.*, at 5–6. This possession or control constitutes a breach under the HIPAA Security Rule unless affected organizations can make the fact-intensive showing that there is a "low probability that the PHI has been compromised" under 45 C.F.R. § 164.402(2). *See id.*, at 6–7.

[25] *See* 45 C.F.R. §§ 164.400–414. Further, even if the affected data was encrypted in compliance with HIPAA guidance, there is still a risk of breach. For example, many types of full-disk encryption only work when a device is powered down. In these cases, if a ransomware infection occurs while the device is turned on and a user is logged in, the ransomware will generally have the same access to the system as the logged in user, rendering the full-disk encryption moot.

National Law Review, Volume VI, Number 271

Source URL:https://natlawreview.com/article/your-business-prepared-ransomware-epidemic