Is Your Company Prepared for a Ransomware Attack?

Kim Peretti, Lou Dennig and Jason R. Wool, Corporate Counsel

July 11, 2016

This year already appears to be the Year of Ransomware, with the healthcare industry most acutely feeling the pain inflicted by this malware species. April saw a record number of ransomware attacks in the United States.

Until recently, a layperson might understandably believe ransomware affects only individuals, not corporations, with stories circulating for several years of encrypted desktop computers being unlocked only after the unsuspecting consumer pays anonymous hackers several hundred dollars. Recent news stories indicate, however, that ransomware is now a corporate problem, too. While this might ordinarily be viewed merely as a nuisance for some entities, those that rely on the availability of data or electronic systems to perform key functions (and who doesn't?) are faced with a grave reality: Ransomware can grind operations to a halt.

Ransomware is a type of malware that locks a device or renders its data unusable until the victim pays the attacker a ransom, often in an alternative currency known as bitcoin. According to Symantec, there are two primary categories of the malware: locker ransomware (which locks the device until the ransom is paid) and crypto ransomware (which generally encrypts individual files without locking the user out of the device entirely). Both types of ransomware ultimately deny the victim access to the data stored on the device.

Ransomware can be delivered as a malicious payload in a manner similar to any other malware, including through phishing, social engineering, malicious advertising or an existing remote-access Trojan. Once downloaded on a device, the malware generally either locks the device or quietly begins encrypting data stored on it. Many types of ransomware also seek to traverse the victim's network in an effort to move to other systems, including storage devices and critical servers. Only once the ransom is paid does the attacker unlock the device or provide the key to decrypt data, although in some cases attackers have reportedly not carried out their end of the bargain even after being paid.

The risks posed by ransomware extend well beyond the encryption of data or locking of a device. As more and more businesses embrace data-driven processes and increase their reliance on Big Data, a ransomware infection means not only that data or systems become unavailable – it means that the business may not be able to function. Entities in nearly all sectors, including financial services, e-commerce, cloud services, and more, depend on the availability of data and systems to function and provide core services. Critical infrastructure, which is often required to provide essential services (e.g., electricity, telecommunications), also depends heavily on data and system availability. As we have seen this year, hospitals appear to be particularly vulnerable.

Indeed, 2016 kicked off with a string of ransomware attacks targeting the health care industry. In early February, Hollywood Presbyterian Medical Center in Los Angeles had to operate using paper and fax machines after a ransomware attack prevented personnel from accessing patient records and communicating electronically. Reports indicated that patients bound for the emergency room had to be diverted to other hospitals. After 10 days of functioning largely in the pre-Internet era, the hospital elected to pay a $17,000 ransom, with its president and CEO noting that paying the hackers was the "quickest and most efficient way to restore our systems and administrative functions."

Over the next several weeks similar attacks were perpetrated against a separate California hospital group, Kentucky's Methodist Hospital, and most recently MedStar, which operates 10 Maryland hospitals. In those attacks, the requested ransoms ranged from $1,600 to $18,500, but all entities reported that they were able to resolve the attacks without paying the hackers. Health care ransomware attacks were not limited to the United States, as the U.S. Computer Emergency Readiness Team (US-CERT) noted in an alert that healthcare entities in Germany and New Zealand faced similar attacks in early 2016.

While health care has been hit particularly hard this year, the issue pervades a broad range of industries. The U.S. House of Representatives was the target of ransomware attacks in May that required the House to lockdown parts of its network and restrict access to certain email and cloud services programs. The Federal Financial Institutions Examination Council (FFIEC) recently issued a statement warning of an "increasing frequency and severity of cyber attacks involving extortion," including the use of ransomware. In March, security experts notified Apple that they had discovered a ransomware program embedded in an app related to BitTorrent (the peer-to-peer data sharing system) that encrypted certain files and demanded that users send one bitcoin (valued at ~$400) to unlock the data. Before Apple was able to implement a fix, an estimated 6,500 systems were infected.

Ransomware has hit less likely targets as well, such as the Horry County school system in South Carolina, which paid an $8,500 ransom to unlock its computers. Federal agencies have been the frequent target of ransomware. According to the Department of Homeland Security (DHS), between June and December 2015 alone, 321 incidents of ransomware targeted 29 different federal agencies.

The FBI recently advised that individuals and organizations "should not pay the ransom" and highlighted that the "best way to protect yourself and your organization is to have a backup of your data, maintain it, and disconnect it from your computer." US-CERT recently issued a ransomware alert recommending that entities take several added protective measures in addition to backing up data, including the use of application whitelisting, avoiding enabling macros from email attachments and ensuring that software patches are downloaded and antivirus programs are kept up-to-date. Additionally, both the FBI and US-CERT recommend that all instances of ransomware, whether affecting individuals or businesses, should be reported to the FBI's Internet Crime Complaint Center (IC3), and victims should consider reaching out to reputable security vendors for assistance.

Responding quickly and effectively to ransomware is essential to minimize its operational impact, which can often be a highly complex undertaking if multiple systems are impacted. Unlike most security incidents involving a compromise of data, such as payment card breaches or data breaches involving personal information disclosure, ransomware attacks can leave victims with little time to decide how to respond before their operations are halted. A key reason to have a breach response plan – one that can help companies respond not only to data breaches but also to cyber incidents having an operational impact on data or systems – is the heightened stress company personnel face in responding to a breach. This is only exacerbated by ransomware attacks.

One commonality among (reported) ransomware attacks is that the monetary demands are generally not excessive, which encourages victims to pay the ransom and move on. As law enforcement guidance has noted, paying a ransom is no guarantee that the locked data or systems will be released, nor does it provide assurance that the current hackers (or, more likely, other hackers) will not come back to the well with new ransomware demanding additional payment. When facing a ransomware attack, the seemingly low cost of remediating the issue mixed with the added stress of having a suddenly nonoperational business makes it a worthy consideration to have, and test, a ransomware response plan before an attack occurs.

The operational risks associated with ransomware (as well as other types of malware that impact data and system availability, such as wiper malware) have not gone unnoticed by regulators. The European Union, for instance, will soon finalize the Network and Information Security Directive, which will require certain operators of "essential services" and "digital service providers" (e.g., online marketplaces, search engines and cloud computing services), among others, to implement "appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems," including ensuring the "continuity of those services."

This would likely include managing risks posed by attacks similar to ransomware, which often impacts continuity of services. (Germany passed a similar law last year.) In the United States, the National Institute of Standards and Technology released a voluntary Cybersecurity Framework in 2014 that encourages entities to ensure that "information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information."

By threatening the availability of core business operations, ransomware fits neatly within the set of concerns addressed through the idea of "security resilience," which is of particular importance to critical infrastructure and other entities that require highly available operations. Resilience is based on the ability to withstand or quickly recover from incidents with severe operational impacts, including malware attacks, and encompasses functions related to business continuity and disaster recovery. Traditional elements of resilience include infrastructure redundancy and robust backup and backup testing processes. These tools – particularly performing regular backups of critical data – are often recommended by security experts as a backstop measure against ransomware.

Organizations that are highly dependent on the availability of data and electronic systems should treat ransomware as a real and serious risk to their operational viability, and consider it within their enterprise and cyberrisk management processes. Ransomware and other malware with potentially severe operational impacts are becoming increasingly widespread and – as the hospital attacks show – dangerous and costly. If 2016 is the Year of Ransomware, it should also be the year that entities take steps to prepare against attacks that impact the availability of data and system operability – not only in the face of a ransomware attack, but also to face whatever 2017 has in store.

***Kim Peretti** is a partner in Alston & Bird's privacy and data security practice group and co-chair of its cybersecurity preparedness and response team. Peretti is a former senior litigator for the U.S. Department of Justice's computer crime and intellectual property section. She focuses her practice on managing complex, technical electronic investigations and responses, often resulting from cyber intrusions and data breaches. Lou Dennig is a senior associate in the firm's litigation and trial practice group and cybersecurity team. His practice focuses on assisting clients in managing cyber intrusions and data breaches as well as advising companies as they develop information security and privacy policies related to their business. Jason R. Wool is a senior associate in the firm's technology, privacy and IP transactions practice group as well as the cybersecurity group. His practice focuses on cybersecurity, privacy and critical infrastructure protection. Wool participated in all six National Institute of Standards and Technology workshops on the development of the Cybersecurity Framework.*