TIP Jar

Digital Data Security and Confidentiality: Public Agency Vulnerabilities in the Age of Ransomware

Spring 2017

In the action movie thriller *Taken,* Liam Neeson plays a former CIA operative and distraught father on a mission to rescue his daughter from kidnappers. Imagine if Neeson came upon the kidnapping of his most valuable, confidential data and it was being held for ransom. One of his most famous movie lines might read something like this:

If you are looking for ransom, I can tell you I don't have money. But what I do have is a very particular set of skills. Skills I have acquired over a very long career. Skills that make me a nightmare for people like you. If you let my data go now, that'll be the end of it … [I]f you don't, I will look for you, I will find you and I will kill you.

For any public agency administrator, school district superintendent, or IT director who has found their computer systems breached and their most confidential data "kidnapped" and held for ransom, they pray for a Liam Neeson with "special skills" to rescue it. Unfortunately, you may end up having to pay the ransom instead. And worse, you may not get the data back. Public agencies are especially vulnerable to such attacks because they maintain important, confidential information. However, there are things you can do to prevent the kidnapping of your valuable data.

The incidence of ransomware attacks in the United States alone numbered nearly 4,000 attempts each day in 2016, an estimated increase of 300 percent over the prior year, according to the U.S. Department of Justice. Government agencies are the second most likely entities to be targeted with ransomware attacks, following the education sector, according to cybersecurity experts. Moreover, according to Will Bales, a supervisory special agent in the FBI's Cyber Division, "[R]ansomware does not discriminate. Whether it's a big school district or a small school district, they have the same possibility of being hit." Experts are now saying that the likelihood of a ransomware attack is not a matter of "if" but "when."

What is Ransomware?

"Ransomware" is a type of "malware," which is software that is intended to damage or disable computers and computer systems. Imagine a kidnapping that doesn't remove the victim from the premises (i.e., the agency's computer network or servers), but hides them from you in plain sight. Once infected, ransomware begins encrypting files and folders on local drives, any attached backup drives, and potentially other computers on the same network. The hackers store a decryption key in the malware to be released when the ransom is paid. Users and organizations may not even be aware their systems are infected until they can no longer access their data or the computer displays messages advising them of the attack and demanding a ransom to restore it. The data is always there on the system; you just can't get to it.

Ransomware can be downloaded from a variety of sources. When it first


William P. Curley III
Partner and Co-Chair
Local Government Practice Group
Los Angeles Office
wcurley@lozanosmith.com


Lee Burdick
Senior Counsel
Fresno Office
lburdick@lozanosmith.com

Lozano Smith
ATTORNEYS AT LAW

appeared, ransomware was typically delivered through spam email requesting that a user click on an attachment or link which would, in turn, download the malware ("phishing"). More recently, hackers have developed targeting systems known as "spear phishing," which involves an email that appears to be from an individual or business that you know, but you actually don't. Because the email seems to come from someone you know, you may be less vigilant and decide to provide them the requested information.

Unwitting users may pick up ransomware while visiting malicious or compromised websites that exploit vulnerabilities in the user's computer software security. An insidious form of this is a "malvertisement," an online advertisement which installs malware and can sometimes search computers for bank account and other information to transmit back to the source. Ransomware can also be dropped as a payload or downloaded by other malware. A low-tech but cunning ransomware named "Locky" deployed in 2016 caused decoy image files to automatically download from social media sites like Facebook and LinkedIn and, when the user clicked on them, they infected and encrypted users' systems. Cybersecurity experts have revealed that three percent of government agencies have been exposed to Locky and four percent to another strain known as "Nymaim," the cockroach of ransomware that serves as a Trojan to allow the download of other malware. Twitter feeds and mobile applications have also been used to embed ransomware.

As the profitability of ransomware has grown, hackers have become even more sophisticated. Attackers have been directly contacting users in a variety of ways to encourage them to open access to their computers. One way is a technical support scam, where the caller claims to be a Microsoft support representative, for instance, who is checking up on reports of errors or a malware infection on the victim's computer. The caller then tells the victim to download a diagnostic tool, a connection is established to the "troubled" computer, commands are run, and dangerous-looking files and lengthy text logs are displayed on the screen, which of course indicate serious problems. Meanwhile, the scammer is infecting the victim's system with ransomware.

Once infected, ransom demands to rescue your data can vary. "Cryptocurrencies" can include payment options like Bitcoin (the most popular), and iTunes and Amazon gift cards. Paying the ransom, however, does not guarantee a user will get the key to regain access to the infected system or the hostage files. Therein lies the ultimate dilemma: Do I pay the ransom or not?

Why Should I Worry?

A public agency's data is one of its most precious and valuable assets. In February 2017, ransomware shut down the government offices of Licking County, Ohio, including the police department network. Licking is the third-largest county in Ohio, with a population of more than 166,000 residents. The attack shut down the government's online access and landline telephones for approximately a week. Although the 911 dispatch system continued to operate apart from the county's main network—as it is required to do—there is no doubt that disabling the government's online access placed the residents at risk.

School districts are also especially vulnerable. The inability to access student or operational data can be catastrophic in terms of the disruption to regular operations, financial losses to restore systems and files, lost revenues for days the schools must be closed to recover from an attack and the potential harm to a district's reputation. However, a district should also be very concerned about its legal obligations to maintain the confidentiality of all student and employee identifying information. Under both the Family Educational Rights and Privacy Act (FERPA) and the California Education Code, school districts are generally not authorized to allow access to student records to any person without written parental consent. Other federal laws further reinforce school district obligations to protect student online data privacy.

In addition, personal employee information is kept in personnel records, including Social Security numbers, salary and benefit information, addresses, education and employment history, and medical history. An employer's legal obligations with respect to maintaining the privacy of employee data are also wide-ranging and include protections under the California Constitution, the Americans with Disabilities Act, the Family and Medical Leave Act, the Health Insurance Portability and Accountability Act and the California Fair Employment and Housing Act.

Most ransomware attacks do not result in the disclosure or theft of private student or employee information that would constitute a "data breach," triggering a duty for the agency to notify affected parties. However, some ransomware can "exfiltrate" a copy of the personal data from the systems while the files are encrypted, and the IT manager might not even be aware the data is being stolen until the encryption is lifted. If data has been removed from the servers and disclosed to a third party in violation of the public agency's duty to keep it confidential, a government agency might suffer liability exposure far and above the price of the ransom to recover the encrypted files. The fact that the disclosure was the result of an external cyberattack will do little to shield the agency from liability.

What Can I Do to Prevent a Ransomware Attack?

Given that ransomware threats present a short decision-making window before the decryption key is destroyed and data is possibly lost forever, government entities must develop legal, business, ethical and tactical perspectives on these risks and issues prior to an incident. In their June 10, 2016 Law360 article, "Cyber Blackmail and Ransomware: What You Need to Know," Kristofer Swanson and Louis Scharringhausen wrote, "[D]ue to the nontrivial possibility of downstream litigation or regulatory scrutiny, many companies structure their response efforts under the leadership of external legal counsel to benefit from the protections against compulsory production that [attorney-client] privilege can provide."

Of course, there are plenty of technical resources available that outline suggestions for preventing and detecting a cyberattack. One such resource is the tech tips article in this edition of the TIP Jar.

Conclusion

In a ransomware attack, there are no action heroes who can save your data and punish the criminals for the wrong they have done. However, with proper planning and an appropriate response plan, you can at least mitigate, and potentially avoid entirely, the grave damage that a ransomware attack can do to your agency's computer systems, your students' futures and your staff's personal privacy.