New York Law Journal

SERVING THE BENCH AND BAR SINCE 1888

WWW.NYLJ.COM

An ALM Publication

VOLUME 262—NO. 11

TUESDAY, JULY 16, 2019

Outside Counsel

The Rising Risk of Ransomware And the Role of the Legal Team

By
David R. Owen

‘Everyone should expect to be attacked.”

Those were the chilling words of the FBI’s Mike Christman, a cybercrime expert who discussed the perils of ransomware during a recent interview with *60 Minutes*.

In a typical ransomware attack, cybercriminals penetrate an organization’s internal information systems and encrypt the company’s files, grinding regular operations to a halt until a ransom is paid to unlock everything.

IT departments are the first line of defense when it comes to such events, but unless the victimized company can quickly quarantine the infection and restore up-to-date files from backups, the discussion will almost certainly be reduced to a single, appalling question: whether or not to pay. Leadership will then turn to the legal team as they debate these unappealing choices.

To make matters worse, companies inclined to pay the ransom in the name of expediency may not fully appreciate how such payments may invite additional attacks. Hackers often sell stolen information on the Dark Web, fueling new and more effective assaults based on that material.

A Growing Threat

It is notoriously difficult to track data on ransomware and similar criminal enterprises, as victims are often hesitant to share information with authorities. Nonetheless, the U.S. Department of Homeland Security reports that since 2016, more than 4,000 ransomware attacks have taken place daily.

While FBI data released this spring suggests ransomware attacks may be leveling-off, the dollar losses from ransomware and similar attacks continues to grow, last year topping $1.3 billion. It appears that cybercriminals are becoming more efficient, shifting their assaults away from individuals and instead targeting corporations and municipalities with deeper pockets.

Unless the victimized company can quickly quarantine the infection and restore up-to-date files from backups, the discussion will almost certainly be reduced to a single, appalling question: whether or not to pay.

A successful ransomware assault will raise a variety of concerns, impacting both operations and reputation. For in-house company counsel, operational risks will typically be front and center. Companies that have not taken

DAVID R. OWEN *leads the privacy and cyber security practice Cahill Gordon & Reindel. He is qualified as a Certified Information Privacy Professional (CIPP-US) by the International Association of Privacy Professionals (IAPP), the largest and most comprehensive global information privacy community.*

appropriate measures and which are subsequently struck by ransomware will ultimately find themselves debating how long they can be out of business.

Anatomy of an Attack

To best defend against such an attack, it is essential to understand how and when cybercriminals initiate them. "Phishing" emails are crafted by hackers to exploit human failings and inattention, and are broadly disseminated in search of the easiest targets. The more refined form of the attack, known as "spear-phishing," seeks to gain specific insights from a designated victim, and hackers utilize any number of tricks to increase their success. To give their fraudulent attack the appearance of authenticity, they often employ publicly-accessible information to impersonate IT staff, organization management, vendors or customers, mimicking trusted parties in order to capture passwords, data or financial information.

With the right data in hand, the saboteurs can enter an organization's IT infrastructure, encrypting essential business data to lock-out legitimate users. Cybercriminals can also threaten to reveal an organization's sensitive data to competitors and customers. Once a basis for extortion is established, the next step is a ransom demand, often to be paid in Bitcoin.

These tactics are exceptionally effective during periods when employees are interacting with new, supposedly-trusted parties. That means companies are especially vulnerable during M&A transactions, merger integrations, or when onboarding new consultants, clients or vendors. Vulnerability increases yet again if these new relationships have been announced in the media or through public documents, such as Securities and Exchange Commission filings. Anecdotal evidence suggests at least some cybercriminals are actively tracking M&A transactions and utilizing that information to target victims. Hackers also know that during time-sensitive or high-profile events organizations may be more willing to pay to make the problem go away.

The only proven way for an organization to beat a ransomware attack is to ensure it never becomes a victim in the first place.

To Pay or Not to Pay

Perhaps surprisingly, most ransom payments do result in the release of the captured systems and data, presumably to ensure that future victims will be incentivized to pay the ransoms. Evidently the hackers' guild can appreciate their income will eventually dry up if they do not produce the paid-for result.

Yet be warned: payment may not be the complete solution it appears to be. In fact, payment can encourage additional, and even more refined attacks. As a provider of information security risk analysis and due diligence, I review security and cyber-related policies, practices, successes and failures across a great many different businesses. In that role I am frequently surprised that the victims have not considered how a breach and subsequent payment has changed their threat landscape for the worse. Within days of a successful attack, news of a company's willingness to meet the extortion demands can spread on the Dark Web. Worse, the penetration can reveal entirely new vulnerabilities that may also be shared with others, permitting a second and third wave of online bandits to descend and re-victimize the organization.

Meanwhile, a handful of companies have held themselves out as providing software solutions to ransomware, claiming they can help victims regain access to data and computer systems without paying the extortionists. *Pro Publica* recently exposed two such companies, finding they were simply paying the hackers on behalf of their corporate clients, and then charging the victims a mark-up on those illicit transfers.

Finally, the true cost of ransomware to an organizational victim extends far beyond the cost of the Bitcoin payment. Instead, it includes productivity losses, business disruption and reputational harm that may extend to the loss of client relationships. Even when systems are decrypted as promised, organizations may still suffer damage or loss of some data. Victim organizations are also likely to engage in subsequent, and costly, forensic investigation to examine both the extent of that damage and also the weaknesses that allowed the successful attack.

Defensive Strategies

Every organization must balance security against business efficiency and expediency. Nonetheless, there are a number of highly-recommended best practices endorsed by the FBI's cybercrime unit and other federal law enforcement agencies. They fall into four broad categories:

(1) Employee training. Employees are almost always the access point that opens the door to ransomware attacks. Employees are most likely to be approached by someone imitating a trusted party via email. But they may also be engaged by phone, through a webpage link or even regular snail mail, and then induced to provide information that can be used to penetrate systems. Employee training should be required, regularly updated and rigorous, for example involving interactive online role-playing that mimics methods of an attack. In addition, employees should be reminded of phishing risks at times of increased vulnerability, such as M&A activity or merger integrations.

(2) Compartmentalize system access. Compartmentalization ensures that even if an employee's credentials are stolen by a malicious third party, the damage can be limited to that employee's own access. For example, members of the accounting department are unlikely to need access to the legal team's files, directory or network to complete their daily work. Configuring these access controls and limiting the use of administrator-level access reduces the damage that can be done by any single breach. Organizations should also consider providing employees "read-only" access, instead of "write-access" for certain files and directories, reducing opportunities for files to be encrypted by hackers.

(3) Back-up/restore. Organizations should back up their data regularly, at intervals based on their risk appetite. Some corporations back-up daily, ensuring that any ransomware attack only leaves a few hours' worth of their most recent activity vulnerable to loss by malicious encryption. Having a clean back-up can eliminate the threat of business disruption. Organizations must verify the integrity of those back-ups regularly and ensure they are secured appropriately—back-ups cannot be connected to the computers and networks they are meant to protect.

(4) Software and technical solutions. Other additional solutions are relatively technical, from the legal perspective, and best suited for the experts of the IT department. Nonetheless, they are essential and include: regularly patching operating systems and software across all devices; automatically updating antivirus and anti-malware solutions; disabling macro scripts from email; and preventing programs from executing from common ransomware traps, such as zip files and temporary folders supporting internet browsers.

The only proven way for an organization to beat a ransomware attack is to ensure it never becomes a victim in the first place.