CORPORATE COUNSEL
An ALM Website
corpcounsel.com | October 30, 2017

Ransomware: What Every Corporate Executive Needs to Know

It's Friday afternoon before the New Year's holiday. A Fortune 500 CEO gets a call from her company's general counsel: "We've been hit by ransomware. We are locked out of our network and can't communicate with our customers. The hackers demanded $30,000 in Bitcoin in the next 24 hours."

Paul Rosen and Carlton Greene

It's Friday afternoon before the New Year's holiday. A Fortune 500 CEO gets a call from her company's general counsel: "We've been hit by ransomware. We are locked out of our network and can't communicate with our customers. The hackers demanded $30,000 in Bitcoin in the next 24 hours."

This scenario is increasingly common. "Ransomware" attacks are on the rise. The Department of Justice estimates that 4,000 ransomware attacks occur each day. But hackers are becoming more sophisticated, resourceful, and unpredictable, thereby increasing the frequency, scale, and effectiveness of attacks. The ransom request will inevitably come at a busy time, the payment demand will be immediate, and should the company decide to pay, the type of payment demanded (usually Bitcoin) will take time to acquire. Such attacks increasingly make front-page news and place significant risks on corporations large and small around the world. However, thorough preparation, and an understanding of the legal and practical realities, can inform a company's reaction to a ransomware attack and dramatically alter how the story ends.

What Is Ransomware?

Ransomware is simply malware, or harmful software, that prevents or limits your access to your own data. Ransomware commonly uses screen locks or encryption, getting its name from requiring a "ransom" payment to unlock your own data. The actors that deploy ransomware are varied, as are their motivations. Criminals use it for financial gain; nation state actors use it for political reasons or to create chaos. No matter the actor or motivation, sophisticated companies around the world are incurring significant financial and reputation costs as a result of such attacks. For example, this summer a Fortune 300 global company announced that a ransomware attack may cost it $300 million in lost revenue.

As criminal hackers become increasingly sophisticated, so must companies' defenses. Appropriate prevention and protection can substantially mitigate, if not prevent altogether, catastrophic damage. Your IT department will tell you that some fundamental measures include frequently backing up your data and systems, promptly patching your network with software updates, and guarding against phishing—one of the most commonly exploited tactics. No matter how much preparation, however, in the end nothing is fool-proof—which is why understanding the legal and practical considerations of paying a ransom is critical.

You're Locked Out: What's next?

The first step in any crisis is to activate your incident response plan, which hopefully has a section focused on ransomware and has been practiced with tabletop exercises. In doing so, companies should quickly assemble a core team and gather as many facts as possible, ideally through a rapid privileged review conducted by a law firm with the assistance of forensic specialists. After you have a reasonable understanding of what happened and hopefully a sense through forensic analysis (and perhaps law enforcement assistance) of who the perpetrators may be and whether the data is in fact locked, someone with the authority to do so needs to make the decision about whether the company will pay the ransom in the hopes of getting the data unlocked.

Legal Considerations

There are serious potential legal implications for paying a ransom and for facilitating such transactions.

As the recent global cyberattack over the summer referred to as "NotPetya" demonstrated, paying a cyberransom can expose companies to U.S. economic sanctions laws. That attack shut down company networks around the world and has been attributed by some researchers to the Russian security services, in particular the FSB and the GRU. Both entities are subject to sanctions administered by the Department of the Treasury's Office of Foreign Assets Control (OFAC). Those sanctions prohibit any transfer of funds to entities designated for sanctions, as well as the provision of services to, or receipt of services from, such entities.

OFAC also has imposed sanctions on certain governments known to commit offensive cybercrime, such as Iran and North Korea, on various transnational criminal organizations, and on a number of terrorist groups, such as ISIS, that have demonstrated increasing interest and capability in cybercrime. The penalties for sanctions violations can be severe. Civil violations can cost $289,000 per violation, or twice the amount of the violating transaction, whichever is greater. Criminal violations can result in imprisonment of up to 20 years and fines of up to $1 million. In a case where the attacker is a terrorist group, the possibility also exists that payment of a ransom would violate laws against providing material support to terrorists.

While the likelihood of a government enforcement action against a victim of a ransomware attack is generally low, especially where the same attack has affected a large number of victims and potentially the government itself, the risk exists. This is particularly true because the sanctions regime is strict liability—that is, you are potentially liable even if you did not know you were paying a sanctioned entity, which is all the more reason that preparation and prevention of a successful attack is critical.

To mitigate legal risk, a company that wants to consider paying a cyberransom should, generally in coordination with any law enforcement outreach, perform as much due diligence as possible to determine whether the entity it is paying is a state sponsor of terrorism or otherwise subject to U.S. sanctions—as should the institutions that facilitate such payments. At the most basic level, consult OFAC's list of Specially Designated Nationals (the SDN List) and review it against what is known about the attacker. Companies should also consider working with law enforcement early. Not only can that help mitigate the likelihood of enforcement action, but law enforcement also has unique tools that can help companies locate and pursue the cyber actor, and learn more about them.

Financial institutions that facilitate cyber ransom payments also face risk. Banks, virtual currency exchangers, and other financial institutions face obligations under the Bank Secrecy Act to prevent their institutions from being used to facilitate criminal activity, and must file Suspicious Activity Reports, or SARs, on suspicious activity that occurs through their institutions. Criminal money laundering laws also prohibit conducting transactions with the proceeds of criminal activity knowing that the transactions are designed to avoid reporting requirements, such as those imposed by the Bank Secrecy Act. This can be an issue where, as often happens, cybercriminals demand payment through a virtual currency or virtual currency exchanger that is designed for

anonymity or otherwise to promote crime. Recent actions by FinCEN and the Department of Justice against virtual currency providers such as Liberty Reserve and BTC-e, based on these companies' actions to facilitate anonymity and criminal activity, show that regulators and prosecutors are focused on this issue.

Beyond the government enforcement considerations involved in deciding whether to pay a ransom, there are also a number of legal issues to consider in being locked out of corporate data, including customer harm and potential breach of contract claims. Companies and their counsel will need to evaluate these issues depending on the specific nature of the cyber-attack, and hopefully the issues will have already been considered before any such attack.

Practical Consideratons

Even if a company is comfortable with the legal risks of paying a ransom, several practicalities must be addressed, ideally in advance of any attack.

First, recognize that there is no guarantee that a ransomware hacker will return the decryption key and unlock your data. And, even if you do engage with hackers, the files they return may be incomplete or corrupted. We have seen attacks clothed in "ransomware" that in reality were simply meant to wreak havoc and destroy systems and data. So, even if you pay, you may need a plan B.

Second, paying ransom can subject a company to further attacks, including incentivizing further ransomware episodes and related criminal activity. And critics may suggest that companies that pay ransom are further funding and incentivizing criminal activity.

Third, most ransomware demands seek payment in a form that helps anonymize the payee, usually with virtual currencies such as Bitcoin. While many company executives understand what Bitcoin is, the process of obtaining a Bitcoin wallet and converting currency to Bitcoin can be complicated and take time. Companies often need to be vetted and processed by a Bitcoin broker before they can open a Bitcoin wallet. Forensic vendors and law firms can assist in this process and help facilitate an appropriate payment structure.

For example, if an attack affected multiple systems or involved a large ransom request, and a company decides to pay the ransom, it may be prudent to negotiate multiple payments, after which the forensic vendor could validate that the data (or some of it) was returned or unlocked before paying the next installment.

In addition, virtual currency administrators and exchangers operating in the U.S. likely will be subject to federal laws administered by FinCEN, and perhaps also to state anti-money laundering regulations. These may prevent a virtual currency provider from processing such payments, and may result in them, or in banks involved in converting real currency to virtual currency, filing suspicious activity reports on the company making them, which would be available to state and federal law enforcement. In addition, the serious penalties banks and other financial institutions face for failing to stop suspected money laundering through their institutions also may cause them to terminate account relationships for companies that make such payments.

Some companies have considered maintaining Bitcoins on hand in case they need to access them quickly. Doing so presents the same policy and image questions outlined above, but it is a practical consideration that corporations are entertaining.

At the end of the day, businesses must weigh the legal risk and practical implications of paying $300 or even 100 times that. In scenarios where companies can lose millions of dollars each day in the form of lost revenue and productivity, the decisions are significant and the precedent for how the company interacts with hackers will be lasting.

An Ounce of Prevention

The choices companies must grapple with in the face of a ransomware attack are challenging. But many of the catastrophic outcomes of an attack can be significantly mitigated or avoided altogether. Indeed, companies can take several measures to reduce or eliminate the risk of a successful attack. By proper planning, backing up data and systems, and regularly updating policies and procedures, companies can dramatically reduce their exposure.

Have an Incident Response Plan: Working with counsel, establish an incident response plan with clear reporting structures and update the plan regularly to address lessons learned from prior incident investigations, specific threats to the organization, including ransomware and changes in law. The incident response team should consist of key stakeholders from across the organization with clear decision-making authority, and include a process by which the board is kept apprised of response efforts.

Practice Makes Perfect: Many companies have well-developed and thorough plans to address cyber incidents, but the plan is often in some basement drawer and nobody but

its author knows it even exists. Plans are only useful if the right people know about them and practice what is in them. Regular (at least annual) tabletop exercises responding to real scenarios—with participation from senior executives—are key components to preparing for a significant cyberincident.

Have a Data Backup Strategy: Your plans should include a rapid data backup and recovery procedure for catastrophic events, such as a ransomware attack. One effective method is to securely store multiple copies of recent (preferably real-time or near real-time) business critical data in two places that are not connected to the computers and networks. Bottom line: If you have good backups of your data and systems, there is less an attacker can hold hostage for ransom.

Update and Patch Software Regularly: In addition to staying on top of available threat indicators to block known bad actors and IP addresses, a patch management policy should provide for installing, testing, and deploying routine software patches on a scheduled basis, and critical patches on an expedited basis. Immediate patching can be a challenge in a large organization with complex and disparate networks and systems, but attackers will seek to exploit software vulnerabilities in your systems. Quickly deploying software provider updates to address these vulnerabilities is key. Just like executing that "critical update" on your iPhone when it pops up, make sure you have a policy and plan to do the same for your corporate systems. Failure to do so may lead to government scrutiny and potential enforcement actions by the Securities and Exchange Commission, Federal Trade Commission or related agencies.

Train Employees and Third Party Vendors: Many of the issues we see arise from human error. Employees might click on a link they shouldn't have, or a contractor may not adhere to the robust security standards you require. An appropriate risk-based training program should involve creating, enhancing, and updating key cybersecurity and privacy training materials for employees and vendors, and establishing formal tracking protocols. To maximize the effectiveness of training, companies should offer targeted, threat-specific cybersecurity training (e.g., phishing, social engineering) and routinely monitor and incorporate information about emerging threats.

For example, consider sending out an email to all employees from a suspect email address offering free tickets to the upcoming Mets game. All they have to do to claim the free tickets is to click on the link for details about picking up those tickets. Instead of tickets, they are told to report to a room for remedial online security training.

Test Your Own Network Security: Conduct a thorough assessment and penetration testing on business critical systems, at the direction of legal counsel, to identify and remediate vulnerabilities. Consider segmenting business critical data to reduce the likelihood that, if infected, ransomware would spread to other systems.

Understand and Evaluate Your Legal Risks in Advance: As part of any incident response plans, work with your counsel to understand the legal risks associated with different types of attacks, and how the company will weigh those risks and which are worth taking.

Stay on Top of Trends: Cyberattacks are evolving faster than the government and the private sector can keep up. Staying on top of new threats, trends, and best practices needs to be a core piece of any company's risk mitigation strategy. In today's world, real cybersecurity means a constant state of readiness, rather than just preparing for an incident. Such a posture will importantly promote a corporatewide culture of cyberawareness and security, rather than a more passive and reactive wait for an incident approach.

The motivations behind cyberattacks are nothing new: disruption, financial gain, and corporate embarrassment, to name a few. What is new is the sophistication and scope of such attacks, which are here to stay. Preparation and prevention for today's attacks will go a long way to preparing and preventing tomorrow's.

***Paul Rosen**, a partner in the Los Angeles office of Crowell & Moring, is the former chief of staff of the Department of Homeland Security and a former federal prosecutor. Carlton Greene is a partner in the Washington, D.C. office of the firm and is the former chief counsel at FinCEN.*