Minimizing Your Company's Exposure to a Ransomware Attack

Sunil Shenoi, Erica Williams, Brian P. Kavanaugh, Gianni Cutri, and Lauren O. Casazza*

This article provides companies with key issues to consider before, during, and after a ransomware attack.

Recently, there have been a number of ransomware attacks against our clients. Ransomware typically encrypts one or more IT systems, causing them to become inoperable unless a company pays a ransom (usually in Bitcoin or another cryptocurrency). In many instances, ransomware effectively shuts down all or a substantial portion of a company's business. Because of the potential harm, companies should prepare for this type of attack as they would for any other potential disaster.

This article is designed to provide companies (and their financial sponsors, if applicable) with key issues to consider before, during, and after a ransomware attack.

BEFORE A RANSOMWARE ATTACK

Insurance

Companies should consider obtaining cyber liability insurance, which can cover the cost of responding to a ransomware attack (e.g., counsel, forensics IT firms) and remediating the IT environment, as well as fees or liability from lawsuits or claims resulting from an attack. Companies should also consider whether existing insurance policies (e.g., property or business interruption policies) cover cybersecurity incidents.

Incident Response Policy

Ransomware attacks often create a significant crisis for a company, which can face pressure from customers, business partners, investors, and employees to resume business operations as soon as possible. Establishing an incident response policy ahead of time can help companies respond to such attacks in a more expeditious and orderly manner, which can help minimize potential business disruption and damages from a ransomware attack. An incident response policy should consider:

- The minimal IT infrastructure required to run the business. For example, a company might be able to take orders on paper but might not be able to function without certain systems.

* Sunil Shenoi (sunil.shenoi@kirkland.com), Erica Williams (erica.williams@kirkland.com), Brian P. Kavanaugh (brian.kavanaugh@kirkland.com), Gianni Cutri (gianni.cutri@kirkland.com), and Lauren O. Casazza (lauren.casazza@kirkland.com) are partners at Kirkland & Ellis LLP.

- How company personnel can communicate if email is unavailable. Consider establishing an emergency phone tree or other alternative forms of communication.
- The role and selection of potential external "first responders." Consider including legal counsel, a forensic IT specialist, a crisis communications firm, a company's insurance carrier, and a consultant that can acquire cryptocurrency and arrange to make a ransom payment if necessary.

Backups

Companies should consider making regular backups of their IT systems, key assets, and critical configurations. Once backups are made, they should be stored in a location that is not accessible from the company's operating or production environment. Taking these actions might enable a company to avoid or minimize potential damage from a ransomware attack.

Emotet and Trickbot

Malware is constantly evolving, but two types that have been used in a number of recent ransomware attacks are called Emotet and Trickbot. The attacks often begin one to three weeks before systems become encrypted, so corporate IT teams should consider periodically checking for indications of whether these types of malware are operating on a company's systems. If such activity is detected, *even if quarantined by anti-virus or anti-malware software*, then a potential ransomware attack could be forthcoming. Contact your legal counsel and a forensic IT specialist for more information about addressing these types of malware.

DURING A RANSOMWARE ATTACK

Whether to Pay the Ransom

Several factors should be considered in determining whether to pay the ransom demand. Although law enforcement discourages victim companies from paying a ransom, some companies have paid the ransom when the affected systems are not backed up or cannot be restored from backups, or when a company cannot afford the disruption from restoring or rebuilding its IT environment. Some studies indicate that in 50 to 70 percent of ransomware cases, companies pay the ransom. Even then, the decryption key is not guaranteed to work.

Before making a payment, companies need to consider whether doing so would violate U.S. law prohibiting payments to individuals or entities that are subject to U.S. economic sanctions or that are designated as terrorist organizations. While the odds of conclusively determining an attacker's identity are low, companies and their counsel should nevertheless seek to conduct diligence on the attacker's identity (usually based on the attacker's Bitcoin wallet) to determine whether such a payment would violate U.S. law.

Forensic IT Specialist

A forensic IT specialist can assist with investigating the ransomware attack, including determining the root cause and advising on potential remediation options. Determining the root cause is important to properly eradicate the ransomware and prevent reinfection. To facilitate a rapid response, companies should consider establishing a relationship with a forensic IT specialist in advance of a cybersecurity incident.

Counsel

In addition to the issues described above, counsel can advise on potential legal issues arising from a ransomware attack, including whether public disclosures or notifications to investors, individuals, customers, business partners, lenders, and regulators are required. Securities and Exchange Commission guidance requires disclosure of material cybersecurity risks and incidents, and while the monetary impact is certainly not the only factor in determining materiality, it can be an important factor in disclosures related to ransomware attacks. In 2017 alone, Merck, FedEx, and Maersk disclosed estimated losses from ransomware attacks totaling $310 million, $300 million, and $200 million to 300 million, respectively.

Crisis Communications

If public disclosure is required per the above guidance, or to the extent that the issue is otherwise leaked, it can be helpful to engage crisis communications experts that can assist in mitigating any potential reputational effects as well as enhance the company's legal strategy.

Insurance

Companies that are victims of a ransomware attack should notify their cyber liability carriers, which can provide options for legal counsel, forensic IT specialists, and other consultants that can assist in responding to a data breach. Failure to follow procedures in the policy can preclude coverage for certain expenses, such as fees for legal counsel or forensic IT specialists.

AFTER A RANSOMWARE ATTACK

Monitoring

Many forms of ransomware embed themselves deep in a company's systems in order to launch future attacks. Even after paying a ransom and applying a decryption key, or after restoring the systems from backups, companies should consider monitoring their systems and network for potential reinfection attempts by the ransomware.

Review IT Security

To help prevent future attacks, companies should consider reviewing their IT security environment for other potential active threats, while also reviewing their security controls for potential enhancements. Many consultants can assist companies with performing an IT security assessment, which can include threat hunting and benchmarking a company's security practices against those of its peers.

Notifications

Legal counsel can advise on whether companies are required to notify employees, customers, investors, regulators, or others of the ransomware attack. Even if such notification is not legally required, companies should consider whether notification is nevertheless appropriate as a business matter.

Litigation and Enforcement

Companies that are victims of ransomware attacks typically have not been the subject of follow-on civil litigation or government enforcement actions. However, in 2018, a class action complaint was filed against Allscripts following a ransomware attack that crippled its operations for about a week. While that case is still pending, it is likely that, with ransomware attacks becoming more common, shareholders and other stakeholders will demand greater protection from companies if and when an incident occurs. As such, we anticipate that litigation and enforcement actions related to ransomware are likely to rise in the coming months and years.