THE
NATIONAL LAW REVIEW

WannaCry Ransomware Cyberattack Raises Legal Issues

Monday, May 22, 2017

The recent cyberattack highlights the need for firms to engage in proactive prevention and protection.

Ransomware (malware that encrypts data pending an extortion payment) is a recurring cyber threat that is growing more pervasive and profitable for criminals. The most recent attack this month by the WannaCry virus highlights the potential global impact, speed and acceleration, and scope of the ransomware problem.

Morgan Lewis

Article By Martin Hirschprung
Mark L. Krotoski
Morgan, Lewis & Bockius LLPLaw Flash

Communications, Media & Internet
All Federal

Ransomware as one unique form of cyberattack has been an increasing global and domestic cybersecurity problem over the last several years. Ransomware targets have included businesses, hospitals, schools, and even police departments.[1] Worryingly, some recent forms of ransomware are becoming more sophisticated and resilient.

Because of the recurring nature of this type of cyberattack, in this article we offer some steps for proactive prevention and protection and some thoughts on the legal issues that may arise following these types of cyberattacks.

Background

Ransomware like WannaCry is designed to encrypt key data on a user's computer or network. The cyberattacker then demands that victims pay a ransom to have their data or files decrypted or restored.

In the case of WannaCry specifically, the software demands that the victim pay a ransom of $300 in bitcoins at the time of infection. If the user doesn't pay the ransom within three days, the amount doubles to $600. After seven days without payment, WannaCry is designed to delete all of the encrypted files and all data will be lost.

The WannaCry virus is designed to spread quickly among computer networks and exploits a vulnerability in computers operating Microsoft Windows without a certain security "patch" that Microsoft issued in March 2017. Recent estimates are that WannaCry quickly spread to more than 150 countries and has affected over 100,000 organizations.[2]

Initial Defense: What You Can Do

Cybersecurity starts with prevention and protection. Common steps a firm and its employees can take to thwart or mitigate ransomware include the following:

Offline and Secure Backups

Ransomware demands are premised on the need to recover and restore data that has been locked up. If offline and unaffected backups exist, the ransomware demands can be disregarded and are rendered irrelevant.

The backup can be either in the form of an external physical hard drive or with a secure cloud-computing service provider. With backups, the firm can erase the data from the infected computers and restore its system from the backups after a ransomware demand.

Avoiding Links or Phishing Schemes with Attachments Containing Malware

An initial line of cyber defense is to avoid the introduction of malware or ransomware onto a network or computer to begin with. This is where the human factor comes in. Many viruses and malware spread by tricking end users to download them via email based on phishing campaigns, spear phishing, or spam. The malware could be embedded in an attachment or at a link contained in an email.

One primary defensive step the firm can take is to train and encourage its employees to practice vigilance against key cyber risks. Cyber-aware employees will avoid clicking on links or downloading attachments from suspicious emails or sources.

Here are some ways to spot a "phishy" email:

- Look at the email address of the sender and see if it looks legitimate.
- Look for obvious typos and errors in the body of the email.
- Hover over hyperlinks and read the name of the website to which they link before clicking.
- Exercise common sense and good judgment when assessing the legitimacy of an email (i.e., are they asking you to reply with personal or financial information?).

Update Operating Systems, Software, and Patches and Use Antivirus Software

Another key step is ensuring that operating systems, security software, and patches are up to date for all systems and devices. Software makers frequently issue security updates for their products. These updates will often address and "patch up" security vulnerabilities.

Employees should also be reminded to regularly update the software on their mobile and other devices. While all software should be kept up to date, updated antivirus software is especially important.

Monitoring and Intrusion Detection

The firm can take steps to detect and block malware through monitoring and intrusion detection. Monitoring may include analyzing basic network traffic as well as looking for any anomalous activity on the firm's network. Firewalls and intrusion detection systems can help protect against and provide alerts about unauthorized access or potential cyber threats.

Tailored Protections

Effective cybersecurity requires a tailored and risk-based approach to safeguard information and systems. There is no one-size-fits-all approach.[3] Typically, a layered security approach can protect data depending on the cyber risks, system, and information. Firms can consider whether necessary protections are in place as part of its broader cybersecurity strategy.

Incident Response Plan That Is Tested

In the event of a cyberattack, the firm can deploy its incident response plan. This plan typically includes key points of contact and a tailored response strategy to ensure that the firm can quickly implement appropriate steps to recover.

In the event of a ransomware demand, a number of technical and legal issues may arise. A technical team can isolate the infected system, assess the scope of any damage, take steps to mitigate the cyberattack, and determine whether a decryption key may exist (low probability but worth considering). The firm can screen any backups to ensure that they are malware free. The technical team can work closely with counsel, as noted in the next section, to address legal issues at all phases including a decision about contacting law enforcement. A postincident review will be useful to highlight other security measures and steps to protect the organization.

Common Legal Issues

The facts of each cyber incident must be carefully considered against a host of potential legal issues. Experienced counsel can guide firms through these issues as well as the investigation and any legal process. We have seen a number of common legal issues that may arise during a ransomware or cyberattack. Issues to consider include the following:

Initial Cyber Investigation under Attorney-Client Privilege

Initially, the firm must carefully assess the nature of the attack and its scope. There are many initial considerations:

- What networks, systems, or data were affected?
- Is the cyber incident ongoing or has it been contained?
- Has security been restored?
- What, if any, data may have been exfiltrated?
- Was any data “accessed” or “acquired” or reasonably believed to have been accessed or acquired?

The answers to these and other related questions will likely take some time to resolve. Because the answers will likely have legal consequences, it is highly recommended that any cyber investigation be conducted under attorney-client privilege. This will allow the firm to obtain frank and candid legal advice as the facts are emerging.

Determining Any Notification Requirements

Depending on the facts and nature of the data, the cyber incident may trigger a legal notification requirement. The notifications may be obligated under contractual requirements or statutes depending on the industry and jurisdiction of enforcers. Additionally, it is important to note that there may be different triggering standards for the notification requirement.

As an example, in the United States, 52 jurisdictions (including 48 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands) have enacted some version of a data breach notification law.[4] Under these laws, notification may be required for any customer whose personally identifiable information (PII) was acquired or accessed, or reasonably likely to have been acquired or accessed. While most states require some form of notice to their residents depending on applicable legal standards, some states also require notification to public agencies, such as the state attorney general. Until a uniform federal standard is adopted, the nuances and variations among these statutes must be reviewed and evaluated.[5]

Response to Government Inquiries and Enforcement Actions

Regulators may seek information regarding a cyber incident. Federal and state agencies have increased their focus on whether firms have reasonable cybersecurity protections in place even where a firm is the victim of a cyberattack.

Experienced counsel can assist in responding to these inquiries and in devising a recommended strategy with which to respond. Government inquiries may be initiated by federal and state regulators. We are seeing cases involving concurrent jurisdiction of regulators that may result in simultaneous investigations.

Anticipating Potential Civil Litigation

The firm can consider what specific steps can be taken to avoid or mitigate potential civil actions, including private rights of action or class actions regarding a cyber incident. Many states allow for a private right of action to be filed in order to recover damages. On cybersecurity matters, there has been substantial activity involving class actions. Engaging experienced counsel early after the cyber incident may help the firm recognize potential litigation, and counsel can recommend steps to anticipate and mitigate costly legal actions.

Contacting Law Enforcement

Another important question involves whether and when to contact law enforcement. Federal authorities recommend that law enforcement be contacted when ransomware occurs.[6] The facts of each case must be carefully considered by the firm. Law enforcement will likely want to obtain relevant data about the cyber incident that is properly authenticated under chain of custody protocols. The investigation and prosecution of the incident by law enforcement may result in public information and proceedings. Experienced counsel can assist in answering questions about the criminal justice process and cyber prosecutions.

Information Sharing in the Private and Public Sectors

The sharing of cyber-threat information with others may present issues that require legal consideration. A number

of industries (such as automotive, aviation, and financial services) have Information Sharing Analysis Centers (ISACs). The Cybersecurity Information Sharing Act of 2015 was enacted to establish new protections and foster information sharing by the private sector to the government to "share cyber threat indicators and defensive measures."[7] The circumstances of sharing information under this law should be carefully considered. Communications with competitors should also be evaluated to ensure antitrust protections are in place and to avoid further governmental scrutiny concerning the contact with competitors.[8]

Scope of Cyber-Insurance Coverage

While many firms have cyber insurance, whether it covers ransomware depends on the terms of the applicable policy. Experienced counsel can review and provide guidance on any coverage issues.

Conclusion

Cyberattacks such as ransomware are unfortunately becoming more pervasive. Firms can take a number of steps to prevent and protect themselves against this form of cyberattack.

When a cyber incident arises, experienced counsel can help identify issues that may arise, work closely with technical specialists, and make recommendations for how best to navigate the process. Most important to firms is the implementation of a strategy that minimizes business disruptions and permits a return to full business operations as soon as possible.

---

[1] *See, e.g.*, Press Release, Computer Virus Affects Police Department Servers, Cockrell Hill Police Department (Jan. 25, 2017); *see also* Chris Francescani, Ransomware Hackers Blackmail U.S. Police Departments, NBC News (Apr. 26 2016); Jason Trahan, Cockrell Hill police lose years worth of evidence in ransom hacking, WFAA (Jan. 25, 2017).

[2] For more information on WannaCry, see generally US Department of Homeland Security/US Computer Emergency Readiness Team (US-CERT), Indicators Associated With WannaCry Ransomware, Alert (TA17-132A) (originally released May 12, 2017, last revised May 19, 2017); National Cybersecurity and Communications Integration Center, What Is WannaCry/WanaCrypt0r?.

[3] For example, the National Institute of Standards and Technology (NIST) Cybersecurity Framework 1.0 (Feb. 12, 2014) provides a useful flexible approach to assess and manage cybersecurity risk.

[4] For a listing of the data breach notification statutes, see National Conference of State Legislatures, Security Breach Notification Laws; *see also* LawFlash: New Mexico to Become 48th State to Enact Data Breach Notification Statute (Mar. 28, 2017).

[5] *See, e.g.*, M. Krotoski, L. Wang, & J. Rosen, The Need to Repair the Complex, Cumbersome, Costly Data Breach Notification Maze, BNA's Privacy & Security Law Report, 15 PVLR 271 (Feb. 8, 2016).

[6] Ransomware: What It Is and What To Do About It (June 2016).

[7] 6 U.S.C. §§ 1501-1510; Pub. L. 114–113, div. N, title I, § 111, 129 Stat. 2956 (Dec. 18, 2015).

[8] *See* Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information (Apr. 10, 2014).