HUNTON& WILLIAMS

Lawyer Insights

June 27, 2017

Ransomware Attacks Raise Key Legal Considerations

by Lisa J. Sotto, Brittany M. Bacon and Jeffrey Dunifon

Published in Law360[i]



On May 12, 2017, a massive ransomware attack hit tens of thousands of computer systems in over 150 countries. The ransomware, known as "WannaCry," leverages a Windows vulnerability and encrypts files on infected systems and demands payment for their release. If payment is not received within a specified timeframe, the ransomware automatically deletes the files. On June 27, 2017, another ransomware variant, "Petya," began affecting computers in the Ukraine before spreading worldwide. A wide range of industries have been impacted by these attacks, including businesses, hospitals, utilities and government entities around the world.

Ransomware is one of the many types of recent cyberattacks that can have significant legal implications for affected entities and industries for whom data access, integrity and availability are critical; health care and financial companies are particularly vulnerable. As affected entities work to understand and respond to the threat of ransomware, below is a summary of key legal considerations.

Considerations

FTC Enforcement
The Federal Trade Commission has used its authority under Section 5 of the FTC Act to pursue "unfair or deceptive acts or practices" to address data privacy and security issues. The deception doctrine has been used to pursue companies that misrepresent their use of personal information or the security measures used to protect such data, while the unfairness doctrine has been used to bring actions against companies that fail to employ adequate safeguards prior to a security incident (regardless of the company's representations). In a November 2016 blog entry, the FTC stated that "a business' failure to secure its networks from ransomware can cause significant harm to the consumers (and employees) whose personal data is hacked. And in some cases, a business's inability to maintain its day-to-day operations during a ransomware attack could deny people critical access to services like health care in the event of an emergency." The FTC also indicated that "a company's failure to update its systems and patch vulnerabilities known to be exploited by ransomware could violate Section 5 of the FTC Act." Nearly all data security actions brought by the FTC have been settled and have resulted in comprehensive settlement agreements that typically impose obligations for up to 20 years.

Breach Notification Laws
In the U.S., 48 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have laws that require notification to affected individuals (and in many states, regulators) in the event of unauthorized acquisition of or access to personal information. Certain federal laws, such as the Health

Information Technology for Economic and Clinical Health Act, also require notification for certain breaches of covered information, and there are an increasing number of breach notification laws being adopted internationally. To the extent a ransomware attack results in the unauthorized acquisition of, or access to, covered information, applicable breach notification laws may impose notification obligations on affected entities.

Data Security Laws

A number of U.S. states have enacted laws that require organizations that maintain personal information about state residents to adhere to certain information security requirements with respect to that personal information. As a general matter, these laws (such as Section 1798.81.5 of the California Civil Code) require businesses that own or license personal information about state residents to implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, destruction, use, modification or disclosure. To the extent a ransomware attack results from a failure to implement reasonable safeguards, affected entities may be at risk of legal exposure under the relevant state security laws.

Litigation

In the event that ransomware results in a compromise of covered information, litigation is another potential risk. Despite the difficulty of bringing successful lawsuits against affected entities, plaintiffs lawyers continue to actively pursue newsworthy breaches, as businesses are paying significant amounts in settlements with affected individuals. Affected entities also may face lawsuits from their business partners whose data is involved in the attack, and often battle insurers over coverage of costs associated with the attack. Businesses must also be cognizant of cyber-related shareholder derivative lawsuits, which increasingly follow from catastrophic security breaches.

Agency Guidance

Given the evolving nature of ransomware attacks, government agencies are continuously developing recommendations to help businesses respond. For example, the U.S. Department of Health and Human Services Office for Civil Rights, which enforces the Health Insurance Portability and Accountability Act and the HITECH Act, published a fact sheet advising health care entities on methods for preventing, investigating and recovering from ransomware attacks. The fact sheet also provides insight to help entities assess their potential breach notification obligations in the wake of a ransomware attack. The FBI similarly has developed ransomware resources directed towards chief information security officers and CEOs. This guidance should be carefully considered to help prevent and recover from ransomware attacks and to understand the potential criminal and enforcement implications of such attacks.

Industry Standards and Best Practices

In addition to complying with explicit legal requirements, organizations should continuously evaluate their practices against industry standards, which typically evolve and are updated more frequently than relevant legislation, and which help organizations better align their practices with the expectations of consumers, business partners and regulators. As a recent example, earlier this month the Health Care Industry Cybersecurity Task Force published a report addressing cybersecurity in the health care industry. The task force, which was established by Congress in 2015, is composed of government officials and leaders in the health care industry. Noting that "the rise and sophistication of ransomware attacks that hold IT systems and patient-critical devices hostage continues to grow," the report sets forth best practices for addressing cyber security threats that were gleaned from studying the financial services and energy sectors, including: (1) conducting comprehensive information sharing on current threats,

attack vectors and the systems within the enterprise; (2) implementing baseline protections such as patching against known vulnerabilities; (3) designing and testing security incident response and recovery efforts; and (4) enhancing communications and collaboration by engaging in more regular and formalized collaboration within the sector.

Conclusion

Ransomware is a growing concern, and while the recent global attacks have been some of the most high-profile to date, they are part of an overall trend in the evolving threat landscape. Businesses and other organizations should take into account the legal considerations discussed above in their efforts to prevent, investigate and recover from these disruptive attacks.

Lisa J. Sotto *is a partner in the New York office of Hunton & Williams LLP and chairs the firm's global privacy and cybersecurity practice. She chairs the US Department of Homeland Security's Data Privacy and Integrity Advisory Committee. She can be reached at (212) 309-1223 or LSotto@hunton.com.* ***Brittany M. Bacon*** *and* ***Jeffrey R. Dunifon*** *are associates in the firm's New York office. Brittany can be reached at (212) 309-1361 or BBacon@hunton.com. Jeffrey can be reached at (212) 309-1335 or JDunifon@hunton.com.*

[i] This article has been updated slightly to reflect more recent news since the article has been published by *Law360*.