Originally published in the Orange County Business Journal on August 28, 2017. Reprinted with permission.

Snell & Wilmer

Understanding what makes *you* unique.®

Handling Cyber Threats: Ransomware

By: James P. Melendres and Lyndsey A. Torp

Ransomware is a type of malware that encrypts or locks a company's valuable digital files and demands a ransom to release them. These types of attacks are skyrocketing, with over 3 million attacks in 2015 exploding to 638 million in 2016. A recent study estimates that ransomware extortionists have made more than $25 million in bounties over the last two years. Given the recent and particularly dangerous wave of ransomware circulating throughout the United States, it is critical that businesses have cyber policies to deal with these threats, including specific policies for ransomware.

Employees are often the weakest link from a security perspective, and likely targets for an attack. An employee may open an email addressed to them, and click on an attachment that appears legitimate, such as an invoice, or click on a legitimate-looking URL. But the attachment actually contains malicious ransomware code, or the URL directs them to a website that infects their computer with malicious software. More recently, criminals bypass the need for an individual employee to click on a link, and instead seed legitimate websites with malicious code, taking advantage of unpatched software on end-user computers.

> ***"Given the recent and particularly dangerous wave of ransomware circulating throughout the United States, it is critical that businesses have cyber policies to deal with these threats..."***

Once ransomware has been deployed, it encrypts files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network. The installed software permits hackers to load malicious programs which allow them to gather intelligence and gain control of systems on the network. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they receive a message advising them of the attack and demanding a ransom payment in exchange for a decryption key. These messages include instructions regarding how to pay the ransom, typically via Bitcoins – a largely untraceable method for transferring funds.

The recent WannaCry ransomware attack infected over 300,000 computers in over 150 nations. WannaCry was particularly problematic because it contained a worm component. It attempted to exploit vulnerabilities in a Windows server to remotely compromise systems, encrypted their files, and spread to other hosts. Notably, Microsoft had issued a patch to fix these vulnerabilities two months before the attack, but those affected had not updated their software to install the patch.

The fact that WannaCry was in most instances avoidable only serves to stress that businesses must develop cyber policies that include two main areas:

1. Prevention; and

2. A cyber incident response plan ("CIRP") that accounts for a ransomware attack.

The FBI published prevention considerations, which include the following:

- Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.

- Patch operating system, software, and firmware on digital devices through a centralized patch management system.

- Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.

- Manage and limit the use of privileged accounts, such as administrative accounts.

- Configure access controls, including file, directory, and network share permissions appropriately.

- Disable macro scripts from office files transmitted over email.

- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations, such as temporary folders.

A company should also maintain a CIRP that addresses ransomware as a distinct type of cyber attack. In particular, ransomware raises unique legal and operational questions distinct from those that arise in the course of "typical" data breach, including the critical question of whether to pay the ransom. Accordingly, in consultation with outside counsel, a company should ensure that its CIRP incorporates a decision-making framework that addresses the novel legal issues related to detecting, responding to, and limiting the effects of a ransomware attack.

For more information about Cyber Security, Data Protection, and Privacy, please visit https://www.swlaw.com/services/cybersecurity-data-protection-and-privacy.

James P. Melendres is co-chair of the Cybersecurity, Data Protection, and Privacy practice and the White Collar Defense and Investigations practice. He focuses on cybersecurity incident preparation and emergency response, related regulatory compliance and civil litigation as well as white collar criminal defense and government investigations. Reach James at 714.427.7071 or jmelendres@swlaw.com.

Lyndsey A. Torp concentrates her practice on business litigation, real estate litigation, construction litigation, and franchise litigation in state and federal courts. In addition, she has experience in cybersecurity with particular focus on ransomware and cyber extortion. Reach Lyndsey at 714.427.7529 or ltorp@swlaw.com.

James P. Melendres | 714.427.7071 | jmelendres@swlaw.com
Plaza Tower | 600 Anton Boulevard | Suite 1400 | Costa Mesa, CA 92626

Lyndsey A. Torp | 714.427.7529 | ltorp@swlaw.com
Plaza Tower | 600 Anton Boulevard | Suite 1400 | Costa Mesa, CA 92626

Denver | Las Vegas | Los Angeles | Los Cabos | **Orange County** | Phoenix | Reno | Salt Lake City | Tucson

Snell & Wilmer
LAW OFFICES

www.swlaw.com

Snell & Wilmer is solely responsible for the content of this article.