FUNKHOUSER VEGOSEN LIEBMAN & DUNN LTD.

Legal Update

March 2017

DON'T GET HELD HOSTAGE BY RANSOMWARE

By Peter T. Berk

Following up on our February newsletter on email scams (yes, it's ok to click the links in this article), another way criminals use technology to harm, and steal money from, companies and individuals is "ransomware". This method of attack has virtually exploded. In fact, as reported by SonicWall, "[r]ansomware attacks in 2016 grew by 167x year-over-year to *638 million*." (emphasis added)

What Is Ransomware?

Ransomware is a type of malware that infects a user's computer when the user clicks on malicious links or files in emails or on websites, or, in some more recent cases, browses a site with malicious adware – without even clicking on it. Upon installation, the ransomware encrypts files and folders on the infected computer and all connected drives, servers, and other devices with a complex encryption algorithm. Once the encryption is complete (which can take anywhere from a few minutes to hours depending on the data), the ransomware notifies the user(s) that the data has been encrypted and will be deleted within a certain timeframe unless a ransom is paid (usually in hard to trace bitcoin). More sophisticated ransomware attacks will also encrypt on-line backup information, preventing a reinstall from recently backed-up data. Once infected, a company can: (a) pay the ransom (70% of infected companies paid the ransom in 2016 according to an IBM study as reported by CNBC); (b) pay an outside consultant or utilize significant internal resources to attempt to break the encryption; or (c) take the time to clean the system of the encryption software and restore data from a backup, which may be days or even weeks old depending on company practices.

Additionally, a company that falls prey to a ransomware attack can expect future attack attempts from multiple sources because the company's server, computers, and users are seen as more vulnerable.

How FVLD Can Assist You And Your Business.

The best method of dealing with ransomware, and other technology attacks, is to take preventative measures and be prepared. Steps you can take include:

(1) creating electronic use policies;
(2) training employees on the policies and best practices;
(3) auditing and updating your data security and disaster recovery policies and protocols;
(4) evaluating insurance options; and
(5) creating a company response plan, including evaluating and selecting a team of necessary professionals, that can be implemented if a ransomware attack occurs.

The attorneys at FVLD are prepared to help you and your business address and limit your risks.

FVLD publishes updates on legal issues and summaries of legal topics for its clients and friends. They are merely informational and do not constitute legal advice. We welcome comments or questions. If we can be of assistance, please call or contact Peter T. Berk 312.701.6870 pberk@fvldlaw.com, Twitter: @BerkPeter, LinkedIn: www.linkedin.com/in/pberk, or your regular FVLD contact.

FVLD®