BARNES & THORNBURG LLP

CYBERCRIME & YOUR COMPANY – FAILING TO PREPARE = PREPARING TO FAIL, Part 1

May 22, 2014 | | Privacy,The GEE Blog

George E. Horn, Jr.
Partner

I. The Threat

"If you don't lock your car, it's vulnerable. If you don't' secure your computer, it's vulnerable." "Reduce your vulnerability, and you reduce the threat." Information on how to protect your computer. There are over 2 billion people worldwide using the Internet. An alarming number of these people make a decent living as cybercriminals. In doing so, they cower behind the anonymity provided by the Internet. They destroy lives. They injure businesses and compromise the integrity of the global economy.

II. The Reality

In a report recently released by the FBI's Internet Crime Complaint Center ("IC3"), the agency disclosed that it had received 262,813 "consumer" complaints of suspected internet crime in 2013. These complaints involved an adjusted dollar loss of $781,841,611, a 48 percent increase in losses over the 2012 total of $581,441,110. (See FBI, 2013 Internet Crimes Report at 3 (2014)). On July 22, 2013, the Wall Street Journal estimated a total cost of up to $100 billion per year to the U.S. as a result of cyberespionage and cybercrime.

III. Some Examples

Information has been compromised and denial-of-services attacks have been successfully waged against high profile company systems and websites. Among them are business giants Yahoo, Amazon, eBay, Target, eHarmony, Zappos, LinkedIn and too many banks to mention. Media leaders have also served as fodder for cybercriminals. CNN was victimized. On April 23, 2013, the Associated Press' twitter account was hacked and the following false tweet posted: "Breaking: Two Explosions in the White House and Barack Obama is injured." The hoax tweet caused an immediate and substantial impact on domestic financial markets. The Dow Jones industrials plunged 130 points and $136 billion was removed from the S&P 500 Index. While the Dow later recouped these losses, the damage that can be caused by even a brief but well-placed cyber-intrusion was clear.

IV. Cryptolocker Ransomware

This new cyber-scam came to light in September of 2013. Cryptolocker

RELATED PRACTICE AREAS

Financial and Regulatory Litigation
Government Litigation
Securities and Capital Markets
White Collar and Investigations

RELATED TOPICS

Cybercrime

Ransomware brings the concept of corporate kidnapping to the cyber world. It essentially holds your computer hostage. It tends to target and extort money from victims through intimidation. It usually enters a computer system through unwanted email attachments or questionable websites and propagates rapidly. The virus spreads, encrypts file types on local drives and mapped network drives, rendering them unusable. This is followed by a pop-up window appearing on the target's computer stating that the target's data has been encrypted. The perpetrator then informs the target that the only way to retrieve access to the data is by sending a specific sum of money to the perpetrator. Cryptolocker usually provides the target with a timeline by which to pay the ransom and provides a "convenient" countdown clock to further terrorize the target. Should the target fail to pay in time, they not only risk losing the ability to pay the ransom, but may have their data permanently encrypted and unusable. Once a computer or network is infected with Cryptolocker, little can be done. Efforts at decryption have generally proven useless. Dell SecureWorks estimated that approximately 250,000 computer systems were infected globally with Cryptolocker during the first 100 days following its detection.