Silent Internet Data and Hacking Threats

Introduction Recently disclosed information concerning online encryption methods may serve to undermine confidence that web transactions are safe and remain private. In addition, well-publicized attacks on such seemingly secure organizations as the CIA, the FBI and the White House continue to raise red flags.

P. Blake Keating
Vice President, Media Claims
Content, Technology, and Services Liability Division
OneBeacon Professional Insurance

onebeaconpro.com/whatwedo

OneBeacon
PROFESSIONAL INSURANCE®

Recently disclosed information concerning online encryption methods may serve to undermine confidence that web transactions are safe and remain private. Additionally, individuals, businesses and government agencies that utilize intellectual property that the Chinese and Russians know of, and may have an interest in, are now adopting new security methods.

All of this comes on the heels of well publicized hacking attacks on a wide variety of organizations such as the CIA, the FBI, the Department of Defense, the White House, the U.S. Chamber of Commerce and the Vatican. News has even leaked of a recent compromised telephone call between the FBI and Scotland Yard about the hacking group known as "Anonymous". Somehow "Anonymous" hacked into computers and telephone systems that enabled it to listen to the call between the two well-known law enforcement agencies in real time as the call took place. Ironically, the call's subject matter was itself concerning "Anonymous" and the dangers posed by the increasingly brazen outlaw organization. The call was later broadcast on the internet, both in voice and in the form of written transcript much to law enforcement's chagrin.

The FBI's head of cyber security, Shawn Henry, who is soon to step down, recently opined that hackers are too talented to be stopped by current defense measures without changes in both technology and behavior. He believes that many organizations have already been hacked as they are unknowingly operating vulnerable networks. Other cyber defense experts have agreed that there is not one secure, unclassified computer network in America.

Most recently, the FBI has disclosed that the hacker known as Sabu, leader of "LulzSec", a subgroup of the hacking confederation "Anonymous", has been identified and has become an FBI informant. His identity was determined from analysis of data from online evidence, including chatrooms and social networking sites.

As deficient as technological defenses currently are, many experts still believe that the behavioral patterns of computer users may actually pose a greater problem. Password fatigue from the repeated use of many different and changing password requirements mean that individuals seek to develop easy to remember – but therefore easily discovered – passwords, that are unfortunately, easily cracked or guessed.

While in the past many of the hacking activists have proudly announced the results of their illegal conduct, this behavior may become less prevalent in the future because of the recent monitoring of internet sites including message boards and online forums by law enforcement at a number of government levels. But the reduction of online "chatter" about hacking will likely not mean hacking incidents have themselves become more rare, only that the bragging about it has subsided.

American and European mathematicians have recently learned of unexpected vulnerabilities in the encryption methods used across the world for banking, online shopping and other internet transactions that are intended to remain private and secure. The flaw involves a relatively small, but sizably significant, number of cases in which the encryption systems are to generate random numbers. The discovery means that website operators will need to make changes to ensure their encryption systems are, in fact, random and secure. Previously undetected, such flaws erode confidence in the worldwide online commerce system, which is based on purported security afforded by "public key cryptographic infrastructure". The researchers were able to prove that some percentage of numbers were not truly random, thereby making it possible to determine underlying numbers or secret keys used to generate the so called public key. The researchers say that they inadvertently learned of some 27,000 different keys that offered no security and

which are, at least theoretically, accessible to anyone. The researchers concluded that it was highly unlikely that these flaws had not been previously discovered by organizations or individuals known for their curiosity and malicious intent in breaking such information codes, adding that the researchers' own methods were not themselves sophisticated.

In the sphere of international business, what once would have been thought of as scope and methods of secret agents have now become routine procedures for many persons. These include leaving personal or business electronic devices such as computers or phones at home in the U.S. if traveling to Russia or China, countries well known for digital espionage both to American government agencies and corporations. To counteract fears that electronic or digital devices might be compromised, many persons acquire loaner devices which they wipe clean before they leave the U.S. and then again when they return here. Some individuals also not only turn off their loaner phones when not in use, but also remove the batteries to combat a fear that system microphones could be turned on remotely by others.

In years past, theft of confidential information or trade secrets typically involved disgruntled employees or corporate moles. Today it is much easier to steal information remotely due to the internet, the proliferation of laptops and smart phones, and the propensity of employees to plug personal devices into workplace networks that carry proprietary information. By tapping into such portable devices, hackers can steal secrets without leaving any evidence of the hacking and data theft on corporate networks. The U.S. Chamber of Commerce, for example, was unaware that it had been the subject of continued hacking incidents from servers in China that were stealing confidential information from it until months later, when they were informed by the FBI.

Consultant Mike McConnell, former Director of U.S. National Intelligence indicates that virtually all computer systems for government agencies, and for companies with trade secrets that he has examined, have been infected or compromised by advanced security threats. He notes that most companies do not realize that they have been hacked until months or years later, e.g., when a competitor introduces the very same product much sooner than had been anticipated, typically at a less expensive price.

Anxieties about various computer systems that hackers might exploit with heretofore unthinkable results include national security, public safety and financial institutions. False or inappropriate information posted online relating to any of these areas are additional things for companies and persons to worry about, in addition to the security of their own personal and organizational information. Even if self-proclaimed victories by hackers become less numerous and noteworthy, we should all remember that quiet and unknown hacking will undoubtedly continue to pose serious security threats for years to come.

For information on data protection and risk management, contact David Molitano at dmolitano@onebeaconpro.com to learn what OneBeacon Professional Insurance may be able to do to assist you with these critical issues.