



Data Security Vulnerabilities Coexist With Computer Capabilities and Convenience

By Blake Keating

In late July of 2008, news reports indicated that Internet service providers were racing to fix potentially dangerous flaws in the basic configuration of the Internet. The flaws allowed criminals to divert computer users to false web sites where personal and financial information could be stolen from unsuspecting consumers. The vulnerability was estimated to affect about forty percent of the Internet. Security experts recognized that by identifying and exposing the flaw, they would also – unfortunately – highlight the weakness for criminals eager to exploit it. The flaw potentially allowed a criminal to secretly redirect web traffic so that an individual keying a bank's web address would be diverted to a fake site set up to steal sensitive data from the unsuspecting user. Security consultants sought to balance the need to protect computer users against concerns of undermining consumer confidence in Internet banking and e-commerce.

Two weeks later, U.S. Attorney General Robert Mukasey and federal prosecutors charged eleven men in five countries in conjunction with a global high technology theft scam that involved more than forty million stolen credit card numbers from nine major U.S. retail chains, including Office Max, Marshall's, T.J. Maxx, BJ's Wholesale Club, Inc. and Barnes and Noble, among others. The government set forth details of a sophisticated operation that employed wireless interception of retailers' data transmissions - "sniffer" programs - that stole credit and debit card numbers as they were entered at points of sale. The stolen card numbers were stored on encrypted computer servers in Latvia, the Ukraine and Russia. The cost of the theft to just one of the retailers was estimated to be more than \$200 million, and this does not include loss of business from consumers whose data was compromised or loss of good will.

Internet Criminals

Internet criminals have perfected the use of software tools typically utilized by computer network administrators to infect thousands of computers with programs to steal passwords and other private data. While computer attacks against network administrators are not new, the widespread use of administrative software to spread malicious software is a recent development. The criminal indictments all pertained to a central program controlling 100,000 infected computers across the Internet that was run from a hosting center in Wisconsin and then the Ukraine. The system not only recorded keystrokes and stole information, it received screen information making it possible for the criminals to see sensitive information, such as bank balances, without having to log into stolen accounts. The new mode of attack is made possible because of the centralized administration of modern computer networks and how the networks update software. While it is convenient for network administrators to update systems at one time, criminals also find this an efficient way to send Trojan malware to every computer in the network. The number of Trojans removed from computers during the second half of 2007, as compared to the first half of that year, soared three-fold. Microsoft has indicated the problem is multinational and linked to organized criminal gangs. The majority of the problems are generated from computers in Russia, China and South America. Microsoft estimates that one million computers had been repaired after being infected with Trojans in 2006, but this number had exploded to more than nineteen million computers during 2007.

A number of security breaches in England recently occurred after the British government taxing authority lost personal information for nearly half the population, which was contained on two computer disks including names, addresses, bank details and insurance numbers – the greatest data security lapse in British history. Analysts concluded that data breaches in Britain could have been avoided, but for serious institutional deficiencies. It was recommended that these governmental entities make data protection a priority.

A recent study indicated that three quarters of companies that have had computers stolen did not have encrypted hard drives and had done nothing to prevent confidential data from being lost on memory cards. Unisys Corp., a large technology company under contract with the U.S. Department of Homeland Security, recently divulged that foreign cyber attacks were constantly taking place at the Agency. Because of global concerns over this criminal trend, a cyber crime treaty has been signed by forty-three nations, including the United States.

Recommendations from the Experts

Experts recommend that companies should make sure that confidential information – credit card numbers, social security numbers, and driver’s license numbers - be password protected with restricted access. Confidential and non-confidential information, i.e. “phone book” information, should be on separate computers so that individuals cannot be paired with their confidential information, which enhances the potential for identity theft. Likewise, the same diligence must be given to hard copy, off line data so that it is protected from theft, as well as laptops and flash drives. Unfortunately, many companies do not proactively change practices and procedures until they have experienced a data security breach disclosed to the public.

Media companies often collect personal information relating to subscribers, advertisers, clients, consumers or donors, which could be compromised if contained on a laptop or flash drive that is lost or stolen, or if a disgruntled employee, technology vendor or other individual gains access to unencrypted personal data.

There are a number of federal and state statutes that may be implicated in a data breach situation. The vast majority of states have passed data breach notification laws requiring people, businesses and state agencies to notify individuals if *unencrypted* personal information is reasonably believed to have been breached, lost or stolen. While the state laws vary in terms of scope, creating challenges for companies who conduct interstate business and who collect personal information from people residing in numerous states, it’s a given that the cost to comply with notification requirements will be expensive.

Technology and marketing analysts estimate that the average cost of a security breach can be as high as \$300 per compromised record after factoring in defense costs, regulatory fines, notification expenses, lost employee productivity and expenses incurred to repair damaged good will. The larger the compromised data base, the higher the costs.

Some of the state notification laws create private civil causes of action. Others limit enforcement to the attorney general’s office, while others consider a breach of the notification law as a violation of the state’s unfair competition law. While there is not a federal data privacy law at the present time, companies may face exposure from the Federal Trade Commission (“FTC”), which has adopted national data security standards for companies covered by the federal FTC Act. A failure to comply with such standards may give rise to an “unfair practice” by the FTC giving rise to significant civil penalties.

First Media has both first and third party insurance solutions for data breach that will assist media entities in the event third party electronic data relating to media operations has been compromised by theft, loss or unauthorized access by a third party or an employee. For more information, please contact Michelle Worrall Tilton at mtilton@firstmediainc.com or 913-384-4806.

Blake Keating
Vice President, Claims
First Media Insurance