Shook, Hardy & Bacon L.L.P.

AUGUST 3, 2012

DATA SECURITY ALERT

Shook, Hardy & Bacon understands companies face challenges securing information in an increasingly electronic world.

SHB guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage risks associated with maintaining and using electronic information.

For more information on SHB's data security and data privacy services, please contact:

Al Saikali
(305) 960-6923
asaikali@shb.com

WHY YOU MAY HAVE SUFFERED A DATA BREACH AND NOT EVEN KNOW IT

90% of organizations have suffered a data breach, a 2011 survey found.[1] A more recent study revealed that at least one in five financial businesses do not know whether they have suffered a data breach in the past three years.[2]

Why do so many data breaches go unidentified in the corporate world? One reason is that people equate data breaches with cyber attacks. While cyber attacks can result in a data breach, the far more common causes of data breaches are human error and common practices in the workplace that, until now, have not really been questioned. At a minimum, human behavior and corporate custom combine to make a company more susceptible to a cyber attack.

A review of the data security literature and recent actions by the Federal Trade Commission provide good examples of how data breaches occur. With each example below, ask yourself what your organization is doing to protect itself against the risk:

- An employee loses a mobile device (phone, laptop, tablet, etc.) or removable media, like a thumb drive, containing unencrypted personal information, or such a device/media is stolen.
- An employee receives an email asking her to click on a link that appears to be legitimate but is actually a vector for malware that will infect the company's IT systems.
- An employee sends mail ("snail" or email) containing unencrypted personal information that gets lost or is inadvertently sent to the wrong recipient.
- An employee installs software on his computer that inadvertently allows access by outsiders to company information.

1 *Perceptions About Network Security*, Ponemon Institute (Jun. 2011)
2 *One in Five Financial Firms "Don't Know" Whether They Have Suffered Data Breaches*, MarketWatch (Jun. 2012).

Shook, Hardy & Bacon L.L.P.

- A company shares confidential, personal, or protected information with a third-party service provider who has implemented little or no security measures to protect the information.
- An employee does not dispose of a customer's personal information in a secure manner when it is no longer needed.
- A company creates an unsecured WiFi hotspot for visitor access to its network, which makes the company's network susceptible to hackers.
- An employee accesses unsecured or unknown WiFi hotspots while traveling.
- A company uses a photocopy machine that stores information long after the copying takes place.
- An employee uses simple passwords (like "password" or "12345") and is never required to change it.

These are just some examples why companies are suffering data breaches. A common theme is that many of them seem like innocuous corporate custom, but in fact they pose significant liability and business risks to the company and its brand, particularly when the breach is discovered and notice is required by law.

The good news is that there are technical, administrative, and physical safeguards a company can adopt that will help minimize these risks. Increasingly, state and federal laws, the Federal Trade Commission, and industry standards are requiring these safeguards. Any company that collects, maintains, or uses personal information of its customers, employees, or other individuals, would be well advised to learn more about the safeguards that can be tailored to the size and needs of their organization. What policies, procedures, and other safeguards does your organization have in place to protect itself?

For more information about these and other issues relating to data security law, visit Al's blog at www.datasecuritylawjournal.com.

OFFICE LOCATIONS

Geneva, Switzerland
+41-22-787-2000
Houston, Texas
+1-713-227-8008
Irvine, California
+1-949-475-1500
Kansas City, Missouri
+1-816-474-6550
London, England
+44-207-332-4500
Miami, Florida
+1-305-358-5171
Philadelphia, Pennsylvania
+1-215-278-2555
San Francisco, California
+1-415-544-1900
Tampa, Florida
+1-813-202-7100
Washington, D.C.
+1-202-783-8400