Shook, Hardy & Bacon L.L.P.

MAY 15, 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

DATA SECURITY QUESTIONS COMPANIES SHOULD CONSIDER

Businesses are increasingly suffering significant losses as a result of data breaches. According to a study by Symantec and the Ponemon Institute, the average organizational cost of a data breach is $7.2 million or $214 per compromised record. A data breach can be as simple as an employee losing confidential information on a portable device, or as sophisticated as a targeted cyber attack. The same Ponemon Institute study shows that 90% of organizations have suffered at least one data breach.

If your company suffers a data breach, are you prepared to respond? How defensible are your information security policies, practices, and safeguards? Here are some issues every business should consider in evaluating the strength and defensibility of their data security policies, practices, and safeguards:

1. What personal information does your company maintain about its customers or its employees? How and where is that information stored and protected?

2. Have you performed an audit of your technical, administrative, and physical safeguards to evaluate the strength of your security measures?

3. Who is responsible for implementing and maintaining your information security measures? Who monitors and advises you of changes in data privacy law and laws that impose data security requirements?

4. Has your company developed an effective information security plan? How do you know that it is effective?

5. Does your company have policies and procedures that implement the information security plan? How are your employees informed and trained?

6. Does your company require its service providers and vendors to comply with the same security standards that the company adopted? Do the agreements with those service providers protect your company if they suffer a breach?

Shook, Hardy & Bacon L.L.P.

DATA SECURITY ALERT

MAY 15, 2012

7. Does your company have an incident response plan? Do you know how to identify and respond to a data breach?

8. Does your company have a relationship with law enforcement to stay abreast of cybersecurity threats that are specific to your industry?

9. How does your company stay informed of the changes in federal, state, and international laws and industry standards that govern your company's information security requirements?

10. If your company suffered a data breach or cyber attack, is it insured for some or all of the costs and loss of business associated with such an event?

If your company does not have an active information security plan in place, investing in one could save significant costs in the future. Al Saikali, of Shook Hardy & Bacon, and the firm's team of lawyers who specialize in data privacy and data security are well positioned to assist you with these and other similar issues.

For more information about these and other issues relating to data security and data privacy 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
San Francisco, California
+1-415-544-1900
Tampa, Florida
+1-813-202-7100
Washington, D.C.
+1-202-783-8400