Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

STRENGTH IN PARTNERSHIP

ALERT

July 2014

COMMON SENSE TIPS TO PROTECT YOUR COMPANY FROM A DATA BREACH

News reports of data breaches have become commonplace. Here are a few suggestions you should consider taking now, before your business becomes a victim. The list is not exhaustive and each business may need to address its unique situation differently:

1. **Know What You Have.** In a written document available to key management, identify and inventory all physical devices and systems you have, including equipment (leased or owned) that you maintain offsite. Also, list all software platforms and applications used in operations, specifying the versions used and on which pieces of equipment the software is being used.

2. **Identify Sensitive Information You Store Electronically.** Sensitive information includes personal identifying information concerning your customers, vendors and employees, and confidential information you store concerning intellectual property, your outside vendors and third parties. Know if and how all information is encrypted and at what point(s) in the business process.

3. **Know What Your Computer System Controls.** Depending on your business, your computer system can control not only access to information, but your company's (and possibly, clients') infrastructure systems. This can be a high risk area, particularly if your business involves manufacturing, as someone from the outside could gain control of your machinery and cause production problems.

4. **Restrict Access.** Access to confidential information should be restricted. Know which of your employees and non-employees have access, and what they have access to. For such people, consider appropriate written agreements with them to limit your exposure to "internal" breaches.

5. **Assess Your Legal Obligations.** Consider, among other legal issues, the following:
    - Do you have the right to collect and retain information concerning your customers, vendors, business partners and employees?
    - Are there legal restrictions on your ability to use information you obtain from your customers, vendors, business partners and employees?
    - What are your legal obligations to protect the information you have obtained from your customers, vendors, business partners and employees?

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW
STRENGTH IN PARTNERSHIP

ALERT

6. **Determine How Your Outsourced Functions Are Dealing With Cybersecurity Risks.** You may be liable for any breaches to your outsourcing partners' networks. If you have outsourcing partners handling any data concerning your customers, you should inquire and/or audit their systems to assure that they are using best-business-practice procedures in securing your business data in their systems.

7. **Create a Risk Management Strategy.** Management must:
   - Prioritize what is the most important information in your company's computer network;
   - Implement appropriate technical, administrative and other controls; and
   - Prepare a response plan in the event of a breach (note that development of these protocols requires the commitment of upper management; in most cases, it will be insufficient to simply hand the issue off to your IT Director).

8. **Create A Network of Relationships With Experts Now.** Time is of the essence following a serious data breach. You can respond more quickly, cheaply and effectively if you already have relationships with experts you can call and who will respond quickly.

9. **Create A Written Cybersecurity Policy.** Such a policy should identify who has access, and what those persons are authorized to do with data in your network, and what should be done if a breach is suspected of having occurred. Each employee and outsourcing partner should be given a copy of these policies and procedures.

10. **Determine Your Insurance Needs.** Traditional business insurance typically does not cover losses from cybersecurity breaches. Numerous insurance carriers offer cybersecurity policies. These policies vary and you should determine what insurance coverage is best for your company's needs.

At Moritt Hock & Hamroff LLP, our cybersecurity practice group is available to assist you proactively on strategies to reduce the risk of harm due to a breach, to comply with industry "best practice" standards, and to respond appropriately in the event that a breach occurs.

◆ ◆ ◆ ◆ ◆

This Alert was written by Keith S. Braun, Steven S. Rubin and A. Jonathan Trafimow.

Mr. Braun, of counsel with the firm, concentrates his practice in all aspects of corporate and securities law.

Mr. Rubin, a partner with the firm, chairs the firm's patent practice and co-chairs its cybersecurity practice. Mr. Rubin concentrates his practice on all phases of patent-related matters, both domestically and internationally.

Mr. Trafimow, a partner with the firm, chairs the firm's employment practice and co-chairs its cybersecurity practice. Mr. Trafimow represents employers in all areas of workplace discrimination, retaliation, harassment and civil rights claims, and class actions. He also routinely advises employers on compliance with local and federal employment laws and regulations.

Any questions concerning the matters raised in the Alert should be addressed to Mr. Braun, Mr. Rubin or Mr. Trafimow. They can be reached at (516) 873-2000 or by email at kbraun@moritthock.com, srubin@moritthock.com jtrafimow@moritthock.com