Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

STRENGTH IN PARTNERSHIP

ALERT

March 2014

I THINK SOMEONE IS STEALING OUR DATA. WHAT SHOULD WE DO?

A reference guide for what to do in the event of a cybersecurity breach

You own a small medical practice and you get a call from your outside IT consultant telling you that an employee has been accessing the practice's computer system late at night, apparently downloading patient files. What your consultant does not know is that three days ago you terminated this employee. While the employee had not engaged in a single, dramatic behavior, you had found her demeanor in the office to be troubling, her interactions with other employees to be challenged and her reliability to be questionable. The termination meeting had not gone well, with the employee threatening to "get even" with you. Now, you realize, she may have the ability to do so. What should you do?

Clearly, any reactions to a cyber-breach must be carefully molded to the individual business and circumstances. We recommend that you retain an attorney for legal advice tailored to your particular situation. Nonetheless, we offer below a "Top 10" list of issues to consider:

- **Retain experienced outside counsel.** Consider taking this step first. Not only can counsel guide you, but he or she can discuss with you whether the investigation and what is gathered as part of the investigation can be shielded from disclosure by the attorney-client privilege. Counsel should be experienced in all aspects of law that typically arise out of a cybersecurity breach, including privacy, employment, litigation, corporate/securities, regulatory, intellectual property and other practice areas.

- **Investigate the Problem.** Directly and through counsel and other experts, investigate the cause and extent of the breach.

- **Stop the Breach.** However serious the initial breach may (or may not be), make the necessary changes to infrastructure to stop the breach from continuing.

- **Correct the Problem.** Once the possibility of further breach is under control, make the necessary additional changes to infrastructure and company policies to reduce the risk of similar types of breaches in the future.

- **Get Expert Help in the Appropriate Manner.** You may need help investigating and correcting the problem, perhaps in the form of forensic or other experts. By having outside counsel retain experts, the experts' work may be protected by the

attorney-client and/or attorney work product privileges.

- **Notify.** Notify appropriate law enforcement, regulatory and other governmental agencies, as appropriate.

- **Notify (Part II).** Depending on the nature of the breach, the type of data breached, and your location, you may have legal obligations to notify certain people affected by the breach.

- **Notify (Part III).** Review existing insurance policies for coverage and notify all necessary brokers and insurance companies. Of course, this raises a separate issue for many companies: do you have insurance coverage that will protect you in the event of a cyber-breach?

- **Public Relations.** Retain a crisis-management/public relations firm to assist in the dissemination of all appropriate information in an organized manner and to aid in mitigating any brand-image damages.

- **Regulatory Compliance.** Make the necessary regulatory filings and disclosures.

Of course, not only medical practices have cybersecurity concerns. We could have made the subject of our hypothetical a building contractor with a disgruntled employee who remotely deletes customer records or tax files, or a real estate management company who receives a call from its bank that its operating and other accounts are seriously overdrawn and no rent deposits have been made. Each cybersecurity breach is unique and each response needs to be appropriately tailored.

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, heads the firm's patent practice where he concentrates his practice on all phases of patent-related matters, both domestically and internationally.

Mr. Trafimow, a partner with the firm, heads the firm's employment and labor practice where he 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