BECKER MEISEL
ATTORNEYS AT LAW

THE RIGHT CHOICE
STANDS OUT

SPRING 2013

Cybersecurity and Data Protection: The New Age of Vigilance

By Timothy J. Szuhaj, Esq.

An onerous aspect of the almost ubiquitous use of technology, one that individuals, businesses, and government agencies must effectively address, is cybercrime. Cyber attacks can come in a variety of forms and are often an attempt to bring down a computer system, or an intrusion seeking to access and steal intellectual or proprietary data and information. At risk are such things as trade or industry secrets, corporate reputation, customer data, and even physical damage to equipment.

Threats to Data

Headlines about cyber attacks, security, and data privacy breaches abound, and have increased the focus on the vulnerabilities of IT security and the profile of cybercriminals. The cost of these attacks to the global economy is estimated to exceed $1.5 trillion.

The wide-spread problem of cyber attacks are highlighted in the statistics:

- ⇒ In 2010, there were more than 370 data breaches, exposing more than 12.8 million records. In the first six months of 2011, there were 385 companies that had data breaches.
- ⇒ The average malicious insider attack takes up to 42 days to address and resolve.
- ⇒ 80% of all cybercrime is the result of insider attacks.
- ⇒ 59% of employees who leave a company steal data on the way out.

Responsibilities of Businesses

Businesses that possess personally identifiable information have numerous responsibilities under state, federal, and – in some cases – international law. Businesses have a responsibility to shareholders and customers to safeguard proprietary, confidential, and trade-secret information. Regardless of size, businesses must comply with the laws that pertain to their possession or ownership of data. Actions may be brought against businesses as a result of breaches, including actions filed under federal laws such as Gramm–Leach–Bliley Act, Computer Fraud and Abuse Act, Electronic Communications Privacy Act, HIPAA, and numerous individual, state and local consumer protection laws.

Pursuing Cybercriminals

Data breaches may result liability for cybercriminal. Such wrongdoers may face prosecution for claims caused by security breaches, including actions filed under the Computer Fraud and Abuse Act and the Economic Espionage Act.

Practical Steps

Becker Meisel can help businesses take certain practical steps to begin to mitigate these risks. At a minimum, businesses should consider the following 5 steps:

1. Identify Important Data

Business owners should identify and segregate important data. Becker Meisel can guide business owners through an inventory process designed to capture and record the type and location of important data. Specifically, the process would determine: (i) the proprietary nature and legal significance of the data; (ii) whether the data is it widely accessible by employees and others involved with the business; and (iii) what measures have been taken to guard the data.

Continued...

Cybersecurity *continued ...*

2. Create a written security policy for employees.

Business owners should create a written security policy for employees. Becker Meisel can collaborate with business owners to craft such a policy. At a minimum, the policy should address whether employees should be allowed to have personal data on business devices. Conversely, businesses should also determine whether business data should be permitted on employees' personal devices and what to do in case a device is lost or stolen. Employees should be educated about the policy and the policy should be readily available. Business owners should monitor compliance with the policy and enforce the policy uniformly.

3. Have formal procedures for New Employees, Departing Employees and Third Parties.

Formal procedures to implement business-wide policies are key. Becker Meisel can help craft formal procedures related to employees and third-parties. New employees should be briefed on protection expectations early. Owners should explain the importance of safeguarding data. Departing employees should have access to data limited and monitored as departure date approaches. All hardware and access devices should be returned. Becker Meisel would help create third party access to data policies including contractual restrictions such as a Non-Disclosure Agreement.

4. Use stronger passwords.

If a business' password is a common word, or something that can be guessed based on public information, consider changing it to something more difficult to crack. It is recommended that business owners create passwords that are at least 12 characters long and contain upper and lower case letters, as well as numbers and special characters. Also, using the same password across multiple accounts should be avoided--the more layers of passwords between cybercriminals and a business' data or money, the better.

5. Encrypt your data.

Businesses cannot always keep cybercriminals out of their computer systems, so it is highly recommended that businesses take steps to protect the data contained within those systems. One means of accomplishing this is the use of encryption. Disk encryption tools come standard on most operating systems. These types of programs essentially convert data into unreadable code that is not easily deciphered by cybercriminals.

Conclusion

In light of the expanding use of technology and the retention of data by businesses of all sizes and the threats posed to both, it is strongly recommended that businesses adopt the best practices to protect their valuable proprietary information and to fulfill their obligation related to the use and storage of such data.