Is Your Firm's Private Data Susceptible to Breach?

PARKER | SMITH | FEEK

Thursday, October 02, 2008

By Cliff Rudolph, Account Executive

In today's data age, almost all organizations store some form of private or confidential information, whether it is employees, customers, or information obtained from vendors. Since 2005 more than 200 million records containing sensitive personal information have been reported in a security breach in the United States.

- Major banks, media companies, credit bureaus and many sizable local organizations have reported data breaches. Some examples include:
- Major Consumer Credit Bureau: Some 163,000 records were affected by ID thieves in which they set up bogus accounts. In 2006 the firm settled with the FTC for $10 million in civil penalties and $5 million for consumer redress. In January 2008 the firm settled a $10 million class action lawsuit.
- Airline Manufacturer: In 2005 a laptop was stolen with HR data including social security numbers and bank account information affecting more than 160,000 records. In 2006 a laptop was taken from an HR employee at an airport that included personal information on 3,600 current and former employees. Again in 2006 a laptop was stolen from an employee's car, with files contained personal information on more than 300,000 former and current employees.
- Major Bank: In January 2008 an international gang of cyber criminals hacked into the bank's records, stealing account numbers, creating fake PIN numbers, fabricating debit cards, and withdrawing funds via ATMs in six countries. It is still unknown how many were affected.

The Privacy Rights Clearinghouse, a nonprofit consumer organization, has compiled a chronological list of reported data breaches, available here: http://www.privacyrights.org/ar/ChronDataBreaches.htm.

Data Breaches and Privacy Rights

In 2003 California was the first state to require notice of security breaches. Since then more than 30 states have followed suit. The laws typically require that any state or local agency—or any person or business which conducts business in the state and that owns or licenses computer data that includes personal information—must notify in the most expedient time possible the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.

This means that a firm must give notice (written or electronic) immediately should the information be compromised regardless if the personal information that was compromised actually was used illegally. In some cases, substitute notice (such as e-mail, Web site postings and notification to statewide media) may be given in the event that notification costs exceed a certain dollar amount. It is important to check with state laws.

On March 4, 2008 the FTC settled a 17th Security Breach case (FTC File No. 072-3013) www.ftc.gov/os/caselist/0723013/index.shtm. The firm was alleged to not safeguard personal data of those applying for loan services and selling surplus hard drives that contained information on 34,000 consumers. The settlement bars the firm from future data security misrepresentations and requires the company to implement and maintain a comprehensive information-security program that includes administrative, technical, and physical safeguards. The settlement also requires the company to obtain, every two years for the next 10 years, an audit from a qualified, independent, third party professional to ensure that its security program meets the standards of the order.

1. Make sure that you have a clearly defined data-security program.
2. Properly train and educate employees on the confidentiality of information and proper use of network security tools.
3. Limit access to private information.

4. Take reasonable and appropriate steps consistent with current technology to make sure that data is secure and that the integrity of information stored and transmitted is not corrupted.
5. Develop written plans and procedures to detect any actual or attempted attacks on your systems, including an incident response policy.
6. Include confidentiality agreements in your contracts with service providers.
7. Adjust and evaluate your plan on a regular basis.
8. Hire an independent third party to evaluate your current data-security program.
9. Consider offsite storage of data, utilizing the services of a third-party data center.
10. Work with an attorney who has experience with privacy and security issues and can assist in offering legal advice and tools for complying with legislative and regulatory needs.

Finally, insurance products have been developed to cover financial losses that occur due to data breaches and unauthorized access. When considering insurance it is important th at you work with a broker who understands your organization and how an insurance policy will respond. Some key features of a strong data liability policy will include coverage for:

- Enterprise-wide coverage.
- Fines, fees and penalties from HIPAA, GLB, CA 1386.
- Network security to include unauthorized access and use, data privacy, malicious code, cyber-attacks and virus transmission.
- Sarbanes-Oxley.
- Prior acts coverage.
- 1st and 3rd party coverage.
- Contingent bodily injury.

The costs associated with notification and the liability that is arising out of privacy and security matters is costing millions of dollars to organizations of all sizes and types. One insurance carrier recently produced a data loss calculator that estimates that on average the costs associated with data loss are about $166 per record. It also provides information on pending class action lawsuits where plaintiffs are requesting $1 million to $21 million per person for damages due to data loss.

As more private data is stored electronically—and the definition of private data is broadened—it is important to understand how these issues impact your organization and how your organization will respond.

If you have any questions or would like to discuss please call us on 425.709.3600.

Cliff Rudolph is an expert on technology issues and a member of the Technology Practice Group for Bellevue,WA-based brokerage and risk management consulting firm Parker Smith & Feek, Inc., a partner broker in Assurex Global, the world's largest privately held risk management, commercial insurance and employee benefits group