PREVENTING AND REACTING TO A DATA BREACH

by Theodore P. Augustinos

Breach incidents have generated staggering costs to businesses in all industries. Nevertheless, a recent survey of IT practitioners revealed that nearly three-quarters do not believe their company views data security as a top strategic initiative, and a clear majority do not believe their organizations are proactive in managing privacy and data protection risks. Even among companies that have devoted significant resources to data security, breaches continue to occur. What is a business to do?

FIVE WAYS TO PREVENT A DATA BREACH

1. *Assemble a data security team and assess the data.* The data security team typically includes IT, legal, administrative and operations personnel and should at least have access to, and the support of, senior management. Their first job is to assess the scope of personal data maintained by the company, how the data is collected, used and transmitted, and the threats to the company's data security.

2. *Develop policies and procedures.* Most companies have privacy and security procedures in place. These existing policies and procedures are often disjointed, even contradictory, throughout different departments and lines of business. The data security team must fill any gaps in existing policies, eliminate redundancies and resolve inconsistencies.

3. *Train, test, update and monitor.* The best policies and procedures are worthless if the appropriate personnel are not trained to comply with them. A prevention program must also include routine, periodic testing of people and systems, built-in requirements for updating in the face of evolving security threats, and monitoring for compliance because the best policies will protect no one if they are just sitting on a shelf.

4. *Control hardware and software.* Laptops, PDAs and other mobile devices present additional challenges in the world of data security. For example, if your employees use their own equipment, how can you know that the equipment complies with your company's security requirements? A data breach prevention program must assess and control exposures related to the hardware and software used by all company personnel.

5. *Mitigate risk.* As the costs of data breaches escalate, data security programs should include an analysis of existing and available insurance coverages. Consider that while insurance may cover expenses for legally required steps, the company may decide to notify customers and provide credit monitoring services, even where not legally compelled to do so. Not all policies cover these voluntary costs and the company should consider whether such coverage would be desirable.

FIVE WAYS TO REACT TO A DATA BREACH

1. *Assemble a response team.* As soon as a data breach is suspected, a response team must be assembled. The team must include IT, legal and operations people but it may also require outside help in forensics to determine the facts surrounding the problem.

2. *Do the forensics.* The response team's first job is to figure out what happened and determine whether the incident was an actual security breach as defined by the relevant statutes and regulations. This is critical to determining the required response to the incident and to making the appropriate adjustments to prevent future breaches. Usually, the engagement of outside legal and forensic resources is appropriate. As time is of the essence, it would be best to identify the team prior to an incident.

3. *Assess the data.* The response team should assess all information as it becomes available to determine if a data breach occurred, what data was compromised, the identity and number of affected individuals, and all other salient facts. Once a review of the facts has revealed that the incident involved a data breach as defined by the applicable legal and regulatory requirements, the response team must then determine the company's responsibilities under these requirements. The team must also evaluate whether any existing insurance coverage applies, and if and when to notify the insurer of the breach.

4. *Prepare notices.* Legal and compliance resources will be needed to draft the required breach notices and to determine where notifications must be sent. There are technical requirements for the content and timing of such notices to individuals and regulatory agencies. All information acquired during the forensic review of the incident must be considered in preparing the notices.

5. *Review preventative measures.* The response team must review the preventative measures that the company has put in place, and make any appropriate improvements and enhancements that would prevent a recurrence of another incident, as well as address any other weakness revealed in the forensic analysis.

RISK MANAGEMENT

Reprinted with permission from *Risk Management*, December 2009 issue issue, page 45.