nerej
CELEBRATING 55 YEARS

Examining personal data and your responsibilities

May 06, 2009 - Financial Digest

2008 may be considered one of the most tumultuous years in the world's economy ever. Adding to the economic hardships, companies faced some of the largest data breaches in history. In 2008, over 285 million personal records were compromised, and these breaches have a compelling story to tell. A "breach" is defined as "the unauthorized acquisition, access, use, or disclosure of protected information which compromises the security or privacy of such information..." Such high profiles cases as TJX or Heartland Payment Systems have brought to the forefront the exposures faced by most of corporate America.

Breaches are typically the result of internal or external access to private data. Up to 98% of the compromised data continues to be attacked from external organized sources. Attackers exploit mistakes committed by the company or their employees; they hack the IT systems, or they gain access through employee's unintentional installation of malware. In a recent interview on WBZ's radio show "What's @ Risk" (http://www.wbz.com/pages/4131583.php?), Steve Wong, vice president at Clearsight Networks, points out that, "as quickly as security measures, such as firewalls, are developed the cyber thieves are creating ways to breach those security measures." Companies must continue with their diligent efforts to thwart cyber crime; by focusing on their mitigation efforts to make sure all essential controls are met, that they track access to data on the corporate systems, that they collect and monitor all event logs, audit employee user accounts and credentials, and review and test all web applications.

As the exposure increases, what are the potential ramifications if a company's data has been compromised? Regulations in 44 states, the District of Columbia, Puerto Rico, and the Virgin Islands require that individuals (customers, employees, citizens, students, etc.) be notified in the event their personal data has been lost, stolen or compromised. Federal regulations include the Federal Trade Commission Act Section 5, the Health Information Technology for Economic and Clinical Health Act (HITECH Act), and the Fair and Accurate Transaction Act of 2003 (FACTA). Most of the rules governing data loss require the specific notification to individuals if there is a discovered breach of personal information. Federal and state government is empowered to enforce privacy breaches through Section 5 of the FTC ActA, making sure companies keep consumers information private, including the precautions they take to secure consumers' personal information. Using its authority under Section 5 of the FTC Act, the Federal Trade Commission has used its unfairness authority to challenge information practices that cause substantial consumer injury.

Although the damages associated with unlawful disclosure of private information are normally not large on an individual basis, collectively they can be massive, and defendants commonly join together in class action lawsuits. Settlements can include monetary damages as well as the cost of credit monitoring services and ID theft coverage. In addition, companies can incur millions of dollars in expenses to secure compromised networks, assess damages, and notify customers.

Protection on any corporate database will never be 100% secure. Internet security protection is a continual process that cannot be solved entirely by technical means. To provide a financial backstop to data security technology, Cyber Liability insurance has been introduced. Traditional insurance products, including property, general liability and professional liability, do not address cyber risks. As with most special types of risks, it takes a specialty insurance product to address the exposure. Cyber Liability policies have been expanding in coverage as well as the number of carriers underwriting the exposure.

Coverage can include:

* Disclosure Injury, including suits by customers of your clients arising from a system security failure that results in the unauthorized access to or dissemination of private information on the Internet.
* Content Injury, including suits arising from intellectual property infringement, trademark infringement, and copyright infringement.
* Reputational Injury, including suits alleging disparagement of products or services, libel, slander, defamation, and invasion of privacy.
*Conduit Injury, including suits arising from system security failures that result in harm to third-party systems.
* Impaired Access Injury, including suits arising from a system security failure that results in your clients' systems being unavailable to customers.
* Business Interruption, including first dollar extra expense.
* E-Threat, including the cost of a professional negotiator and ransom payment.
* Privacy Notification Expenses, including the cost of credit monitoring services for affected customers.
* E-Vandalism Expenses, even when the vandalism is caused by an employee.
* Crisis Management and Reward Expenses, including the cost of public relations consultants.

The bottom line is all companies are exposed to electronic data security breaches. The financial consequences can be enormous, but most companies have relied almost exclusively on technological solutions to manage the risk. The insurance marketplace has designed sophisticated products, higher policy limits, and competitive pricing. There is a growing awareness at many companies that data security should not be exclusively an IT issue, making these products a standard part of a company's risk management strategies.

Spencer Macalaster is the senior vice president at Risk Strategies Co., Boston, Mass.