Munich RE

Focus On: Cyber Liability – Data Compromise

Commercial operations with their trove of sensitive personal information have been the target of record setting data breaches, but any organization – public or private – that handles or stores personal data can become a victim of a costly cyber crime.

Munich Reinsurance America, Inc.
555 College Road East
P.O. Box 5241
Princeton, NJ 08543-5241
Tel.: 609.243.4200
Fax: 609.243.4257
www.munichreamerica.com

Printed May 2012

In 2007, the discovery that hackers had infiltrated the systems of a major retailer, and over a period of months stole some 94 million credit or debit card numbers and more than 455,000 merchandise return records with customers' personal data, was big news. The cost of the loss was more than $171 million. But it pales in comparison with the estimated $300 million that may develop for the breach in 100 million customer accounts of a major electronics manufacturer discovered in 2011.

While far above the average loss, these events highlight the magnitude of loss that may arise from hacking, lost or stolen data, violations of privacy laws, intellectual property infringement, employee error such as data leaks and breaches by business partners, among other exposures.

Finding ways to manage these exposures has become a stiff challenge, especially for those in retail, education, healthcare or financial services where operations often call for a heavy use of credit or debit cards or storage of large amounts of sensitive data, or may have large numbers of computer terminals accessible to the public.

The largest source of data compromise however does not involve penetration of a company's online security. Stolen computer equipment such as laptops and memory sticks makes up 33 percent of breaches and is the leading cause of data compromise, according to a 2012 report by insurance broker Lockton Inc. Closely following the top cause is theft by hackers and criminals, which accounts for 32 percent. Acts of rogue employees cause 19 percent of breaches.

The security steps a company takes behind the scenes however are only one aspect of the security picture. While most states have regulations that set deadlines for notification after a breach has occurred, the question of how early a company should inform stakeholders is more difficult. Notifying too early can limit a company's ability to perform a thorough investigation and determine the extent of the breach. Moving too slowly may result in fines incurred as a result of challenging notification requirements. If the breach becomes public before customers have been notified, the delay could also damage the company's reputation.

Losses

The costs associated with a data compromise tend to stem from: detection efforts which can take months to complete; notification; mitigation; lost business; fines and penalties; restitution; lost productivity; implementation of additional security and audit requirements; and miscellaneous costs such as attorney or consultant fees.

For the past seven years, costs associated with data compromise have risen, according to the Ponemon Institute. But its 2012 report, which examined the costs incurred by 49 U.S. companies – each of which experienced a loss or theft of protected data which required customer notifications – found that the business cost of a data breach declined from $7.2 million in 2010 to $5.5 million in 2011. The 24 percent drop was the first time in the seven years the security firm had conducted the study that any type of decline had been observed.

According to Ponemon, the average per capita cost of a data breach declined from $214 in 2010 to $194 in 2011. As much as 70 percent of these costs stem from indirect costs such as turnover of existing and prospective customers. Of the 49 participating organizations, 39 indicated that negligence was the main cause for the data breach.

It is far too soon to tell whether these decreases in loss costs signify a trend. If so, what role, if any, does loss prevention, improved response strategies, or other factors play in bringing about the improvement?

Legislative and Regulatory Concerns

Over the past 10 years, new requirements related to data privacy have been imposed by states, the federal government and industry, a trend that is only likely to accelerate with the rapid changes in technology.

Of special significance was a move by the Securities and Exchange Commission in October 2011 to require publicly traded companies to disclose material cyber attacks and their costs to shareholders and to provide a "description of relevant insurance coverage."

At present 46 states have data breach notification requirements which are based on both the consumer's state of residence and the home state of the company where the breach occurred.

At least in the short-term, many of these laws are likely to raise more questions than solutions. Variations in state notification requirements complicate companies' abilities to comply with them, and limited case law has challenged the ability of legal experts to predict how a law may be applied and what penalties may be imposed.

In 2011, at least 14 states introduced legislation expanding the scope of laws, setting additional requirements related to notification, or changing penalties for those responsible for breaches.

Federal Laws

At present there is no uniform, comprehensive federal cyber law but instead a patchwork of laws and regulations related to information privacy or directed at specific industries. This legislation includes Financial Modernization Act of 1999, commonly known as the Gramm-Leach Bliley Act; Health Information Portability & Accountability Act (HIPAA); Health Information Technology for Economic & Clinical Health Act (HITECH) and Red Flags Clarification Act of 2010, among other measures.

Between December 2011 and March 2012, a number of pieces of legislation were introduced in Congress. Many of these proposals contain provisions that would remove obstacles for sharing cyber threat data between the government and private sector or among entities within the private sector.

International Initiatives

The Obama administration and the European Justice Commissioner have each proposed new national and cross-border data breach notification and data privacy laws that, among other provisions, would require companies to notify regulators and consumers every time a data breach occurs, even if no records have been accessed.

Over 45 countries currently have data protection or privacy laws, and others are in the process of developing them.

Cyber Liability Insurance

An outgrowth of technology errors and omissions insurance, cyber liability is designed to mitigate the costs of data reconstruction, customer notifications, credit monitoring and other liabilities associated with a cyber event. Expenses such as diminished reputation or customer turnover, however, are typically not covered under cyber liability policies. Currently there are no statutes requiring an entity to purchase cyber liability coverage. However, the federal government is considering requiring that some government contractors carry cyber liability insurance.

And while any company that collects, stores or handles confidential information or relies on a computer network could have significant liability, interest in purchasing cyber insurance thus far has been mixed for a variety of reasons that include companies' perception of its cost and the mistaken belief that cyber liability is covered under a commercial general liability (CGL) policy. In other cases, IT departments may view coverage as unnecessary or deductibles too high.

CGL policies and errors and omissions (E&O) policies typically exclude coverage for electronic data loss and privacy breaches. A technology errors and omissions policy (Tech E&O) is intended to provide coverage for financial loss of a third party due to the failure of the organization's products to perform as intended or for errors or omissions committed in the course of performing a service for another.

Coverages that have been specifically designed to cover cyber exposures include:

- Internet Media Liability which covers claims arising from possible libel, plagiarism, copyright or trademark infringement of content posted on a company's website
- Internet Professional Liability which covers claims arising out of performance of professional services such as web design
- Data Privacy and Network Security Coverage which covers claims arising from failure to prevent transmission of a computer virus, theft of client data and identity theft
- Intellectual Property Coverage which covers theft of proprietary advertising, technology and trademarks
- Information Asset Coverage which covers claims for restoration or recreation of data, computer system resources, and information assets that are damaged by a computer attack

Other forms include:

- Network Business Interruption
- Crisis Management Coverage
- Cyber Extortion Coverage
- Crime/Insider Coverage
- Errors & Omissions Coverage
- Cyber Terrorism Coverage

Most of these coverages are manuscript or independently filed forms.

The strongest amount of interest has been shown by the middle markets, particularly nonprofit organizations, retailers, main street businesses and vendors. There is also some evidence that smaller businesses or those that outsource their computing to a third party have come to realize that they are not immune to cyber losses.

The level and scope of a company's coverage will depend on the amount of sensitive customer, client or other business partner's information that is provided to and stored by the company; the storage location of the information; the company's cyber exposures and their estimated loss potential; and the company's data security obligations based on contractual arrangements, state and federal regulations and foreign laws.

Cyber insurance also can be provided for first party coverage for direct financial losses to the insured caused by data destruction, extortion, hacking, theft or denial of service attacks among other exposures.

Insurer Considerations

Underwriting the cyber exposures of an account involves closely reviewing the risk's information protection practices including data and social media controls, its data breach procedures, relevant insurance coverage as well as its vendor relationships.

Companies may want to consider assembling a team that includes risk management, finance and IT officers who are responsible for conducting due diligence and handling breaches if they occur.

Organizations should consider implementing policies that require vendors and associates to meet the same network security and data protection standards as those it follows. Risk managers (or business owners for smaller companies or organizations) should include review of network security and data protection in their vendor due diligence process.

Assessing an organization's plan for responding to a data compromise is also an important component to underwriting. If a breach occurred, how quickly would the company be able to respond? Does it have a well-developed policy for responding to a breach?

An effective response to a data breach typically includes establishing and informing all employees of their specific responsibilities in the event of an incident; identifying and fixing the cause of the breach; notifying law enforcement officials if applicable, critical vendors and business partners, cyber liability insurer, regulatory agencies if applicable, loss subjects and other stakeholders such as investors; activating remediation or damage control activities; and implementing activities such as credit report monitoring services to mitigate potential future harm.

Moving quickly and effectively following the discovery of a breach is one of the best ways to mitigate the problem.

Data that is extracted and manipulated in Web browsers or applications – a state known as data 'in motion' – is now considered one of the greatest risk access points because of the growing use of mobile devices. Management of these portable devices also is critical.

Other risk management measures include checking the strength of passwords, controls on access and amount of data retained, level of data encryption, existence of logs or other procedures to monitor certain events that could aid in the speedy discovery of a loss, employee training, existence of social media policies and compliance with state and federal statutes.

Exposure Checklist

- What is the organization's risk management capability and, specifically, does it focus on the following?
  - Employees – hiring (screening) and training (awareness)
  - Security controls – policy, procedures and implementation, need-to-know access limitation
  - Data retention protocol and content quality control encryption protocol
  - Enterprise risk management – business partner screening and event response protocol
- How many third parties have access to sensitive data?
- If applicable, is the risk utilizing pre-approved vendors?
- Does the organization have third party risk assessments on file? Do these vendors adhere to a software update process? Do vendors have up-to-date anti-virus protection? Is there a written contract between the risk and the vendor?
- Does the organization have a written business continuity/disaster plan?
- Are back up systems tested annually?
- Is there a document retention policy?
- Does the organization have a dedicated individual or department responsible for IT security?
- Are employees allowed to store/download personally identifiable information on laptops or external storage devices? Is there employee training on information security?
- Does the company have a response plan in place in the event of a data breach that includes notification to appropriate stakeholders?
- Are all departments aware of the data breach response process?
- What is the state legislative approach concerning data protection and breach notification?