IRON COVE
PARTNERS
INSURANCE & FINANCIAL SERVICES

June 28, 2011

DATA SECURITY/CYBER & PRIVACY INSURANCE

INDSUTRY ANALYSIS & COVERAGE OVERVIEW

Prepared by:

Louis D'Agostino, Partner, SVP
Gregory Sibilio, Esq., Vice President

Iron Cove Partners, LLC *a Whitmore Group, Limited Company*
370 Old Country Road, Suite 200
Garden City, New York 11530

IRON COVE PARTNERS
INSURANCE & FINANCIAL SERVICES

EXECUTIVE SUMMARY

The number of cyber attacks, privacy infringements & data security breaches have increased exponentially over the past few years. Increasing statutory and existing Federal Privacy Laws/Legislation mandate that companies notify every affected individual as well as all other clients of the affected employer. The subsequent costs related to notification and ongoing credit monitoring can be extremely onerous and in some instances catastrophic.

The Facts:

- ✓ *In the past two (2) years alone, announced security breaches have affected more than 150 million records containing sensitive personal information, exposing millions of people to the possibility that their identity or personal information will be exploited by thieves.*

- ✓ *According to the 2010 Poneman Study, the most expensive data breach cost the employer $35.3 million to resolve, up $4.8 million from the year prior. The least expensive data breach was $780,000 up $30,000 from the year prior.*

- ✓ *In 2010, data breach victims had a per-record cost of $268, up $49 (22 percent) from $219 in 2009*

- ✓ *The most expensive cause of breach are Malicious Attacks; 31% of all cases in the 2010 Poneman Study involved a Malicious or Criminal Attack*

Things to Consider

- Are you aware of the state and federal privacy laws and your notification requirements?
- Do you have any personal confidential client information stored on computers or in paper files on premises?
- Do you sign any confidentiality agreements regarding any information provided to you by others?
- Do you outsource any services to third party vendors which may involve a client's information?

Ever-changing Regulatory Environment

Lawmakers in at least 18 states introduced security breach legislation in 2010. Since 2004, 46 states have passed laws requiring organizations and government agencies to notify customers, employees, and other affected individuals when a breach of protected personal information occurs due to human error, technology problems, or malicious acts. Failure to do so can result in significant fines and penalties by regulators.

Ever-changing Regulatory Environment (Cont'd)

At the federal level, the "HI-TECH Act", which makes significant changes to HIPAA as respects notification responsibilities, went into effect this past February. Additionally, the Red Flag Act becomes effective in June 2010. Better known as the Red Flags Rule, this regulation will be enforced by the Federal Trade Commission (FTC), all federal bank regulatory agencies and the National Credit Union Administration.

The Red Flags Rule requires that all organizations subject to the Fair and Accurate Credit Transactions Act of 2003 (FACTA) develop and implement a formal, written and revisable "Identity Theft Prevention Program" to detect, prevent and mitigate identity theft.

Most Recent Cyber/Privacy Breaches

PinnacleHealth: On December 17, 2010, Pinnacle released a press release that state that 1,086 outpatients whose personal medical information may have been accessed through an independent medical transcription company. PinnacleHealth explained that a company that provided the system with medical transcription services had a data security incident involving its computer server. The incident occurred in 2008 when the company's server was inadvertently opened to access through the Internet. PinnacleHealth immediately began an investigation and hired an outside computer investigating firm. Pinnacle's internal infrastructure was not affected, however the outside company that they hired was. The information in the dictated reports included social security numbers, dates of birth, dates of interviews or examinations, medications, and the dates that the reports were dictated. The investigation determined that some reports were accessed, but the investigator was unable to ascertain if the users were authorized to do so.

Pinnacle took measures to notify its patients of the impending breach and reported themselves to the Federal Agency responsible for overseeing privacy.

It doesn't have to be your internal breach!

Heraeus Inc.: On November 18, 2010, the company noticed that a steel cabinet that contained a safe with back-up tapes was missing. The company believes (but cannot be sure) that the cabinet was discarded as part of a massive cleanup prior to building demolition. If the cabinet was discarded, it was sent to a transfer station, crushed, sent to Pennsylvania where it was crushed again and then buried in a landfill. Approximately 514 people had personal information on the tapes, including names, addresses, Social Security Numbers, driver's license numbers, financial account numbers, medical information, and other personal information.

Sony, Inc.: The Internet Hacktivist Group, "Anonymous" was rumored to be behind the stolen data from the PlayStation Network. Whoever did hack into the network was able to steal data, such as names, addresses, and other personal information. Sony has been forced to shut down their network indefinitely, suffering a major blow to its reputation, and wallet. A law suit has already been filed contending that Sony was negligent in failing to "protect, encrypt and secure the private and sensitive data of its users," resulting in "the loss of their personal and private

information, including customer names, addresses, email addresses, birthdays, PlayStation Network and Qriocity passwords and user names, as well as online user handles and possibly credit card related data.

Hackers are still the #1 Cause of Cyber Threat! Even with Precautions, If You Are Hacked, Missing Information Needs to Be Covered!

Epsilon: An online marketing firm named Epislon had their system breached on April 4, 2011. Their clients consisted of Walgreens, Best Buy, Citigroup, and other large companies. Customer's information is exposed and customers are infuriated that they are now getting SPAM. The biggest danger however, is that spammers could then target you with email pretending to come from these organizations. Epsilon has not announced what precautions they are going to take, but the cost of notification and customer dissatisfaction is high.

A Breach Could Lead to Customer Dissatisfaction and True Business Interruption.

IMF/Whitehouse: Even the International Monetary Fund and the Whitehouse are not safe from Cyber Attacks. On June 3, 2011, the White House staff were among those targeted by China-based hackers who broke into Google Inc.'s Gmail accounts. On June 12, 2011, it was discovered that the IMF's computer systems had been breached. It is still unknown what information was gathered by the Cyber Assailants, but the underlying point is that even with the top of the line safeguards in place, a company can still be vulnerable to a breach.

Hackers are constantly staying one step ahead of the latest technology used to protect computer systems.

Citibank: On May 24, 2011, Citibank had 360,083 accounts breached by hackers who first logged in as credit card customers and then were able to "leapfrog" from account to account gathering as much information on individual customers as they saw fit. Citibank then launched a seven-day probe into finding out which accounts were hacked. Citi needed to alert every customer that there may have been a potential breach, and conduct a positive public relations campaign. The full extent of the damage has yet to be determined.

Insurance Solutions

Firms often assume that any privacy/security breach would be covered by its standard insurance (i.e. Errors and Omissions, Fidelity Crime Bond, etc.). While some protection may be afforded in certain circumstances, two key factors should be kept in mind. Traditional E&O policies will not cover "first party losses" such as notification/credit monitoring expenses, public relations expenses, crisis management, business interruption, forensic investigation costs, data restoration expenses and costs associated with extortion demands. And while Fidelity Crime Bonds do provide protection for 1st Party losses, it's typically only in the event of the loss of covered property, money, securities, certificates of deposit, etc. and **excludes the loss of confidential information, material or data**. Both of these forms of insurance protection also will not typically defend state or federal regulatory actions, including payment of any civil fines or penalties that might be levied for a violation of a privacy law and/or failure to notify.

Cyber Security insurance coverage fills in the gaps in both traditional first-party and third-party liability policies by protecting a company from losses associated with unauthorized access to or theft of data or e-business activities, computer viruses, denial of service attacks, as well as alleged unauthorized e-commerce transactions.

The Result

A variety of employers and organizations have finally recognized that this is a risk management issue that can no longer be ignored.

Making sure the company maintains proper procedures, crisis management response guidelines and IT Security measures are just some of the ways organizations have attempted to mitigate and transfer risk. A formal security program should be in place to protect against hackers, information extortionists, malicious code, and other exposures.

Companies must also seriously consider the more traditional insurance risk transfer via Cyber/Privacy Security Liability Insurance. This type of coverage, which has been offered for some time but has never been more prevalent, is offered by a variety of major insurance carriers; namely; Chubb, ACE, Zurich & Axis to name a few.

CYBER/PRIVACY COVERAGE INCLUDES:

Disclosure injury, including suits by customers arising from system security failures that result in 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 client's 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.

Regulatory Defense costs coverage for defense costs incurred in defending any claim brought by a federal, state, or local government agency or a licensing or regulatory organization.

Negligent Disclosure Injury coverage for injury sustained by an insured because of negligent loss, or mysterious disappearance, of a system or system output, or negligence of a natural person in the use or safeguarding of a system or system output.

Written records disclosure injury coverage for injury sustained by an insured due to loss, display, transmission, or dissemination of a written record.

E-theft, including coverage extended to networks outside of the insured's system.