E&O/CYBER

Cyber incidents are on the rise, and so is spending on security, data breach notification, credit monitoring and regulatory compliance. What are vulnerable organizations doing about it?

Outsourced IT, disgruntled employees and regulatory risk highlighted Cyber Risk developments in 2009.

- In January, a security breach was discovered at a leading credit card processor affecting thousands of corporations. Hackers installed malicious software that lifted data as it crossed the credit card processor's network. The data included credit card numbers, expiration dates and additional information on the magnetic stripes of cards owned by the customers of thousands of merchants and financial institutions. The loss will exceed $100 million. *Scary Fact:* The processor was payment card industry (PCI) compliant.

- Regulators imposed fines and penalties for organizations remiss in protecting personally identifiable data or health information.

- The downturn in the economy and consequential employee layoffs coincided with the rise in internal hacks.

- "Encrypt, encrypt, encrypt." This cyber security chant was apparently ignored too often by organizations with sensitive data. *Scary Fact:* Only 21% of the systems breached in 2008 had encryption or other strong security features in place to thwart fraud (Source: Identity Theft Resource Center).

- Underwriters paid large losses arising out of data breaches. *Scary Fact:* In one case, hackers accessed more than one million credit cards and stole more than $10 million – in two days. The underwriter paid their policy limit.

- Notification and credit monitoring expense coverage under Cyber policies is expanding. *Scary Fact:* One underwriter paid $4 million in notification and credit monitoring expenses following an insured data breach. *Scary Fact:* Each breached record can cost a responsible party $90-$305, depending on whether or not fraud was perpetrated and whether the breached corporation was in a regulated industry, according to a 2008 Forrester survey.

- Premiums flattened, even in the face of increased litigation and regulation.

- E&O/Cyber products are the fastest growing part of our Executive Risks Practice – for the fourth year running.

RISING REGULATORY BAR

As the year draws to a close, thousands of organizations are grappling with new regulations imposed by:

- HIPAA/HITECH Act (Health Information Technology for Economic and Clinical Health Act) – Greatly expands the scope of HIPAA's applicability and enforcement and increases civil monetary penalties for violations for failure to protect the privacy of health information.

- Federal Trade Commission (FTC) Red Flags Rule – Requires certain businesses to develop a written program to spot the warning signs – red flags – of identity theft. Compliance will be enforced by the FTC beginning November 1, 2009.

- State security breach notification laws – 46 states plus the District of Columbia, Puerto Rico and the Virgin Islands have now enacted laws requiring companies to notify consumers of security breaches when personal information about those consumers may have been acquired by an unauthorized person. The Massachusetts law is one of the toughest. Though pushing compliance to March 2010, the state will require encryption, access controls and written information security programs to protect personally identifiable information of customers and employees. Some expect other states to follow suit.

RESPONSES

Cyber incidents are on the rise and so is spending on security, data breach notification, credit monitoring and regulatory compliance. What are vulnerable organizations doing about it?

- Implementing robust intrusion detection services – In the January credit card processor incident and several other recent data breaches, hackers were inside the network several months before they were detected. Most were found out by an outside vendor performing an assessment.

- Access controls – Employers are encouraged to limit employee access to certain applications that contain personally identifiable information, especially employers going through workforce downsizing.

- Encryption – More corporations are focused on not only the encryption of laptops, thumb drives and other peripherals, but encapsulating or masking data sent over transmission lines.

- Vendor indemnification and insurance requirements – Review of new and existing contracts has revealed limitations in indemnification and vendor insurance coverage. Transferring Cyber Risk to the responsible party (i.e., the credit card processor) is now a major goal of risk management and procurement. Data breaches are often caused by a third-party service provider or business partner (44% of the time, according to the Ponemon Institute's February 2009 "Cost of a Data Breach").

- Incidence response plans – Damage to reputation and loss of customers/clients often depends on how a breached entity responds to an incident. Organizations are preparing for breaches by documenting plans that will send the right message to affected customers. Timely notification and the offer of credit monitoring services have mitigated potential damages.

- Cyber Risk insurance – Risk managers and IT security professionals reviewing Cyber Risk insurance coverage for the first time in 18 months or two years have been astonished at how the insuring agreements and language have responded in almost real time to the developing risks. They are also pleased to find that despite a rising demand, the premiums for cover have decreased.

Key insuring agreements in Cyber products focus on privacy breach coverage and privacy liability – liability arising out of the breach of personally identifiable or health information, whether the disclosure is committed intentionally, negligently, electronically or non-electronically (i.e., laptop theft, dumpster diving, lost thumb drives, etc.).

Cyber policies will usually cover:

- Vicarious liability for intentional or negligent acts committed by IT vendors when systems or processes are outsourced

- Intentional acts committed by a disgruntled or dishonest employee or a former employee

- Fines, penalties, "consumer redress" and defense costs incurred by regulatory action alleging the failure to comply with state or federal laws designed to protect against consumer identity theft

- Notification costs required by state or federal law

- Credit remediation and credit monitoring – the cost to protect the identity of your customers/patients/clients

- Public relations expenses

- Forensic costs in identifying the cause of the breach or intrusion

- Liability as a result of the physical theft or loss of hardware or firmware

MARKETPLACE CONDITIONS

Several new underwriters and revised policy forms entered the market in 2009, responding to the demand for coverage. Key underwriters of Cyber Risk coverage include ACE (U.S. and London), Arch, AXIS, Beazley, Chartis, CNA, Chubb, Darwin, Hartford, Hudson (Euclid Managers), Hiscox, Kiln and St. Paul/Travelers. New forms from Beazley, Chartis, Hartford, Arch, RLI, ACE, Valiant and others have kept pace with the developing risk and pushed the competition for both primary and excess placements.

Capacity of up to $350 million is available, depending on the exposure and loss experience. Companies seeking catastrophe-level coverage should find the market capable of meeting their needs. Most carriers cannot support more than $20 million each. Towers of follow-form coverage/limits are built to satisfy the capacity need.

The demand for notification expense coverage and the increased market competition has allowed buyers to build notification sublimits with the excess markets. The excess sublimit drops down to sit above the sublimits of the underlying layers, hence building a large sublimit to respond to the initial costs arising from a breach.

Pricing remains very competitive. Companies with demonstrably strong IT security risk management policies and procedures (with a focus on developing risks) have a negotiating advantage that will reap benefits in policy wordings as well as cost. Despite the recent large insured losses, pricing is generally flat or down (by 5% at most) for renewals, while coverage has expanded. Underwriter appetite continues to vary by industry sector.

SUGGESTIONS FOR RISK MANAGERS

The Cyber Risk insurance market has continued to mature in terms of the underwriting process and core coverage, but policy wordings still vary substantially. Careful analysis, interpretation and customization are, as always, a necessity for those seeking optimal protection at the best price.

CONTACT

Geoffrey Allen
E&O/Cyber Leader
Executive Risks Practice
Willis North America
212 915 7951
geoffrey.allen@willis.com