

E&O/CYBER

INTO THE BREACH

- **Claims are on the rise: 60% more claims were reported since the same period a year ago.**
- **Legal exposure continues to increase.**
- **E&O/Cyber products are the fastest growing part of our Executive Risks Practice – for the third year running.**

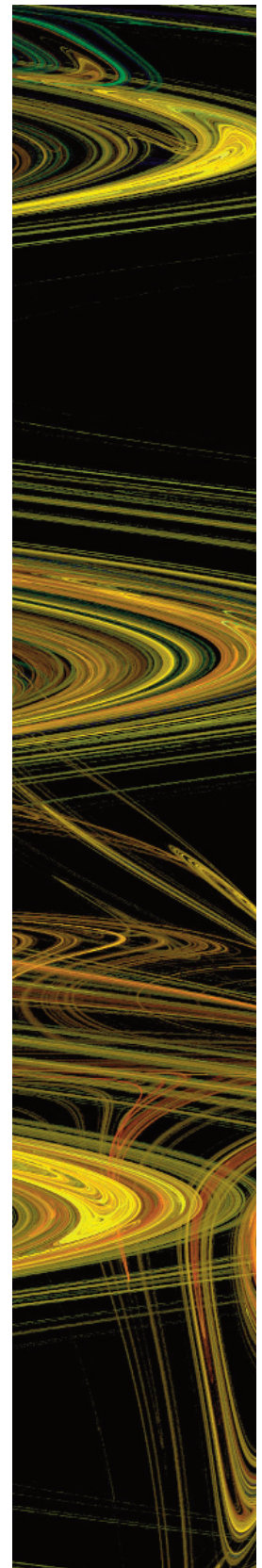
In the past year there has been no respite from the epidemic of security breaches exposing private information. Scores of reported breaches exposed personal data files (some with sensitive information about dependents and medical history) on more than 32 million individuals, according to the Privacy Rights Clearing House.¹ Stakeholders of all kinds, including company management, regulators, consumers, legislatures, credit card issuers, the security community and insurance underwriters, have gotten involved in the search for responses. Unfortunately, nothing has stemmed the tide of information security failures. As we have seen in the past, economic size and a focus on cyber defense cannot guarantee immunity. Companies large and small continue to fall prey to cyber theft and attacks.

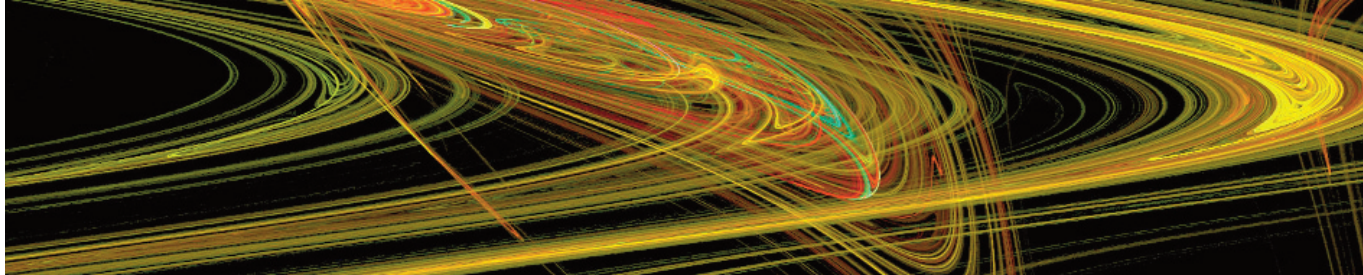
Risk management attention on information privacy was captured by a much publicized retailer data breach discovered in 2006 that generated costs surpassing all previous notions of loss from a cyber crime. This incident, which confirmed the fears of many in the risk management and information security communities, was not an isolated phenomenon. Since then, large privacy

breaches arising from a variety of causes have become only more common, as have the costs associated with:

- Defending class actions
- Complying with various state security breach notification laws
- Investigations and public relations efforts
- Regulatory actions
- Claims by credit card issuers for the expense of reissuing cards
- Claims by merchants for fraud, business interruption and extra expenses

Today, companies in all industry segments that directly (or indirectly through outsourced service providers) hold or process personally identifiable information (PII) or protected health information (PHI) are looking at Cyber Risk insurance as a necessary part of a well designed insurance and risk management program. Since a large number of privacy breaches occur at vendors or business partners, risk managers are closely evaluating the need for Cyber Risk coverage for those holding





or processing PII or PHI on their behalf. Increasingly, companies are requiring proof of Cyber Risk coverage from such vendors. The purchase of Cyber Risk coverage is up significantly since our last report. So too are the limits being elected.

STATEHOUSE ACTION

State Security Breach Notification Laws –

At least 44 states (up from 37 last year) plus the District of Columbia, Puerto Rico and the Virgin Islands have enacted laws requiring companies to notify consumers of security breaches when personal information about those consumers may have been acquired by an unauthorized person. Details of these state notification requirements vary widely. In a noteworthy development, Massachusetts will require, starting May 1, 2009, a comprehensive set of security requirements, including encryption, access controls and written information security programs around customer and employee PII.

Merchant Liability for Security

Breaches – At least 10 states (Alabama, California, Connecticut, Illinois, Iowa, Massachusetts, Michigan, Minnesota, Texas and Washington) – up from six last year – have enacted or may soon enact legislation that shifts to merchants, on a strict liability basis, the financial responsibility for security breaches occurring within their merchant systems. In addition, a recent decision by the U.S. Court of Appeals for the Third Circuit expanded the potential liability merchants face for payment card security breaches.

The ruling in *Sovereign Bank v. B.J. Wholesale Club & Fifth Third Bank*, No. 06-3392/3405 (3rd Circuit, July 13, 2008) could increase the legal risk to merchants.

MARKETPLACE CONDITIONS

There has been no attrition among the key providers of Cyber Risk coverage, which include: ACE, AIG, Arch, AXIS (Media/Pro), Beazley, Brit, CNA, Chubb, Darwin, Hudson (Euclid Managers), Hiscox and St. Paul/Travelers. Recently, The Hartford joined the list. Despite significantly increased claim activity and losses, underwriters have not pulled back the broad protection for liabilities arising from the loss of personally identifiable information (data privacy protection) and confidential corporate information. Most policies now cover costs for security breach notification, public relations expenses and regulatory defense as well forensic expenses and regulatory penalties. The minimum coverage that most insurers now provide protects such information anywhere: on the insured's network, off-line in paper form, with outsourced service providers or in mobile devices such as laptops and portable memory drives. Insurers that previously avoided first-party coverage (business interruption or extra expenses caused by a computer attack on the insured's network) are broadening their forms to provide the coverage.

Capacity from \$150 to \$250 million is still available, despite the concerns regarding carrier financial stability that have recently arisen. Companies seeking catastrophe-level coverage should find the market capable of meeting their needs.

Pricing remains very competitive. Companies with demonstrably strong information security risk management policies and procedures have a negotiating advantage that will reap benefits in policy wording as well as cost. Despite the losses borne by these insurers over the past year, pricing is generally flat, with some decreases available, while coverage has expanded. Appetite varies by industry sector. Some insurers that previously avoided health care or financial institutions are now interested, creating more robust competition for these accounts.

SUGGESTIONS FOR RISK MANAGERS

As exposures increase and documented losses mount, risk managers can ill afford to ignore any weaknesses in their Cyber Risk coverage. Equally, the need for attention should extend to vendors and business partners. Collaboration with IT departments to define the exposure and assess the practical limits on risk management controls are key parts of this process, as is close interaction with the legal department. Legal advisers should ensure that vendor contracts have appropriate insurance requirements and other clauses dealing with responsibilities related to state security breach notification laws and the financial consequences of a privacy breach. The Cyber Risk insurance market has continued to mature in terms of the underwriting process and a baseline of standard, 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

Willis Executive Risks Practice

212 915 7951

geoffrey.allen@willis.com

¹ <http://www.privacyrights.org/ar/ChronDataBreaches.htm>