

CYBER

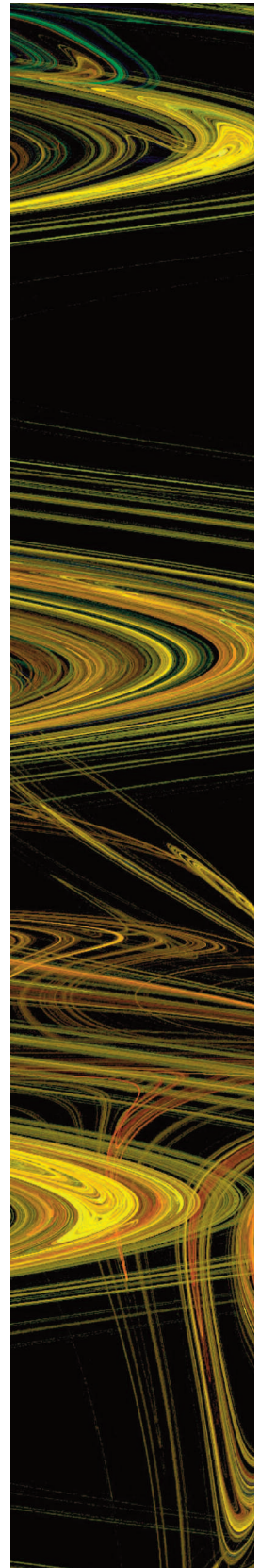
CYBER RISK GOES MAINSTREAM

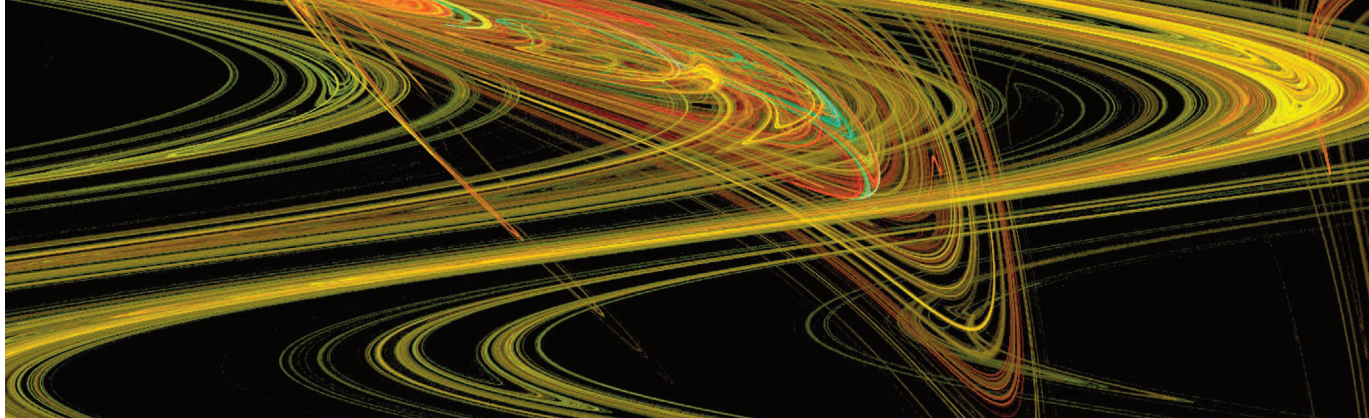
Data privacy continues to be a major risk issue for any organization that uses, retains, manages, processes or outsources personally identifiable information (PII) or protected health information (PHI), and the exposure has garnered attention at the highest levels of management. To help mitigate the financial risk associated with breaches of data privacy, organizations are increasingly turning to Cyber Risk insurance despite the almost universal pressure to reduce or limit spending in every category. Cyber Risk insurance is now a mainstream product.

A few statistics illustrate the factors driving the Cyber Risk purchasing decision:

- Data breach incidents have occurred at a rate of 425 a year or more since 2006, with the number increasing 31% from 2007 to 2008.¹
- Of 558 incidents in 2008, 11% involved third parties, but these accounted for 42% of the 83 million records affected.²
- Of 128 incidents in the first three months of 2009, 9% involved third parties, but these accounted for 52% of the 1.75 million records affected.³
- Average cost per compromised record is \$202.⁴
- Average total cost per incident is \$6.65 million.⁵
- Several incidents have resulted in costs in excess of \$20 million.

There is no evidence to suggest that the increase in data breach incidents will abate. On the contrary, in a severe economic downturn, historic evidence points to a sharp increase in crime, and we can reasonably expect that in the current economic crisis, data theft will increase significantly. Add to this the growing sophistication of computer attacks plus the entrance of organized criminal hacker rings, and the next 12 to 24 months may be a period of heightened risk for organizations with PII.





Companies appear to recognize the need to engage experts to help them address the continuing threat. A recent study found that 72% of companies are maintaining or increasing 2009 budgets for outside privacy advice.⁶ Lawmakers are busy as well – data privacy breach notification laws now appear on the books in at least 45 states.

Protecting privacy has a price. With the confusing patchwork of federal and state laws, along with positions staked out by state attorneys general and federal agencies such as the Federal Trade Commission, the cost of compliance when a data privacy breach occurs only goes up. Notification laws, intended to make owners of PII inform their customers when personal data may have been stolen, also serve to notify the plaintiffs' bar of potential class action opportunities. A class action defense will likely be very costly as a data breach will almost always involve e-discovery – a very expensive process.

Despite the rather grim trend in incident frequency and loss costs, the insurance market for Cyber Risk remains stable. Insurers are competing for market share in what they see as a growth area and putting resources into their Cyber underwriting teams to achieve this. Overall, rates are stable or down 5-10% for renewals with good loss experience. First-time buyers are attracting strong competition on price and policy terms and conditions.

The Cyber Risk market has seen no withdrawals, and several insurers have entered or are planning to enter the market on a primary or excess basis, fueling existing competition. Scope of coverage has remained broad, with policies protecting private and corporate information online, offline and with a vendor. Limits available are in the \$200 million range with more organizations

electing higher limits than in the past, including a growing number of \$100+ million programs. Some insurers are offering policy limits rather than sublimits on the all-important notification cost coverage, which covers the cost to comply with data privacy breach notification laws. Policies generally cover credit monitoring, public relations and forensics as well as fines and penalties and the cost to defend regulatory actions in addition to civil suits. While buyers want higher notification cost limits, and there is some competition now helping in this regard, insurers are looking closely at these costs. Some contend that security breach notification coverage hands a blank check to the insured. We expect that underwriters will tighten their underwriting of this exposure.

CONTACT

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

¹ *2008 Annual Study*, Open Security Foundation, DatalossDB.

² Ibid.

³ Ibid.

⁴ *Cost of a Data Breach*, February 28, 2009, Ponemon Institute, LLC sponsored by PCP Corporation.

⁵ Ibid.

⁶ "Survey: The best privacy advisers in 2008," December 4, 2008, *Computerworld*.