

The State Of Cyberinsurance

By Christine Phan and Catherine Colinvaux

Published in [Insurance Law360](#)

Insurance Law360 recently noted that litigation over cybersecurity claims will be among the “Insurance Cases to Watch in 2011.” Indeed, recent high-profile cybersecurity breaches – the denial of service attacks on Visa, Mastercard, Paypal, and Amazon associated with the Wikileaks releases in late 2010 and the attack on Nasdaq’s confidential document sharing service in February, to name a few – have highlighted the need for every business to consider ways to protect against cybersecurity losses.

The Federal Trade Commission estimates that approximately nine million Americans are the victims of identity theft each year, and according to the Privacy Rights Clearinghouse, over 500 million sensitive records have been breached since 2005. With the explosive growth of cloud computing services, companies are increasingly virtualizing at least some aspects, if not all, of their businesses. Ranging from personal customer information and credit card numbers to intellectual property, the kinds of data at risk in the event of a cybersecurity breach are extremely diverse.

According to the Open Security Foundation Data Loss Database, data breaches occur frequently. Based on a study conducted by Javelin Strategy & Research, losses flowing from data security breaches decreased from \$56 billion in 2009 to \$37 billion in 2010, suggesting that institutions may be taking stronger and more effective precautions to prevent data security breaches. Still, in 2009, only one-third of American companies carried “cyberinsurance,” a property and liability insurance package specifically designed to cover risks related to data security breaches.

Current Digital Risk Management Measures

With the interconnectedness facilitated by the internet, the risk of a cybersecurity breach is unavoidable. A company may employ several strategies to manage this risk: it can retain the risk; it can mitigate the risk; or it can transfer the risk. Insurance is the classic medium for risk transfer. Statistics indicating that approximately two-thirds of American companies have yet to purchase cyberinsurance suggest that companies are retaining and attempting to mitigate the risk of cybersecurity breaches through front-end measures like firewalls and data security policies. However, just as with more traditional types of insured risks of loss, such as fire or hurricanes, front-end protections alone may not suffice. With high profile data breaches happening frequently, a total risk management system often requires more than up-front risk mitigation measures.

Data breaches expose a company to a number of potential direct financial losses, ranging from lost business opportunity and profit to statutory liability. The Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act of

1996, and the Federal Information Security Management Act all protect against identity theft at the federal level. Furthermore, the Federal Trade Commission has imposed heavy fines for privacy breaches and requires companies to self-report data breaches. Finally, nearly every state has enacted some form of privacy or identity theft law, potentially subjecting a company that falls victim to a data breach to broader statutory liability.

Companies without cyberinsurance may plan to rely on traditional commercial general liability insurance (CGL) and property insurance policies to protect them in the event of cybersecurity breaches. However, coverage under property insurance often hinges on whether the insured has suffered “direct physical loss of, or damage to, or loss of use of, covered property,” while CGL policies often require “physical injury to tangible property” in order for coverage for property damage-related liabilities to attach. Whether and to what extent data losses constitute “physical” loss or injury within the meaning of traditional insurance policies has split the courts which have considered the question. For example, in *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.*, No. 99-185 TUC ACM, 2000 U.S. Dist. LEXIS 7299 (Apr. 18, 2000), the District of Arizona found that damage to a computer system resulting in lost data constituted physical damage despite the fact that the computer that housed the lost data was still able to perform its usual function. Conversely, in *America Online, Inc. v. St. Paul Mercury Insurance Co.*, 347 F.3d 89 (2003), the Fourth Circuit declined to find that damage to software constituted physical damage to tangible property based on the fact that, though the software in question was rendered unusable, the hardware itself remained available and intact.

Though virtually every company faces risks related to data loss, traditional insurance policies generally will not provide the best approach to mitigate this risk. Indeed, many such policies expressly exclude coverage for typical cyberlosses. In 2001, many insurance companies revised their standard CGL insuring agreements to state expressly that electronic data is not considered tangible property. Furthermore, many large-scale cyberattacks are international in nature, while many insurance policies are domestic in scope. For example, the Love Bug virus which struck in 2000 affected 45 million users in 20 countries, causing approximately \$9 billion in lost productivity and software damage.

Cyberinsurance

To meet this need, a few insurers, including Travelers, Zurich, and Lloyds of London, have begun offering insurance specifically tailored to cybersecurity and other digital exposures. Current cyberinsurance products offer both first-party and third-party protection. First-party cyberinsurance may cover destruction or loss of information assets, the costs of investigating access violations, internet business interruption, cyber-extortion, loss due to denial of service attacks, reimbursement for public relations expenses in the wake of a data breach, and reimbursement for fraudulent electronic funds transfers. Third-party cyberinsurance may cover claims for defamation or invasion of privacy, the costs of data breach notification, claims related to internet content and

copyright/trademark violations, claims for internet security liability stemming from those harmed by viruses and denial of service attacks, technology errors and omissions and defense costs. Common exclusions include computer malfunctions due to programming errors, ordinary wear and tear, and losses due to failure of electric and telecommunications facilities.

In 2001, Lloyds of London predicted that “e-commerce will emerge as the single biggest insurance risk for the 21st century.” That prediction appears increasingly prescient, and yet companies are still wary to invest in broader protections against cybersecurity breaches. Part of the reason for this hesitation is likely the prohibitive cost of cyberinsurance, especially in view of the large percentage of companies that are deciding to forego cyberinsurance. Even though the risks and repercussions of a data breach are very real, it appears that cyberinsurance may still be priced too high for its perceived value.

The current application process for cyberinsurance is complex and expensive. To evaluate a company’s potential for cybersecurity losses, an insurance company must understand the likelihood the company will experience a loss, the likelihood such an event will cause damage to the company, the severity of such a loss in the event it occurs, and the prevention and mitigation efforts the company uses to avoid or reduce the loss and its consequences. The difficulty with quantifying cybersecurity risks comes from the fact that the value of digital assets is hard to ascertain due to their intangible nature, the fact that a cybersecurity breach may have far-reaching repercussions due to the sheer volume of data stored, and the fact that many companies, even when they are well-established companies, are new to the business of e-commerce and other online transactions. Unlike with traditional insurance, where decades of actuarial information is available to help price the insurance, *everyone* is relatively new to e-commerce. Without concrete information on the kinds of losses an insurer can expect to incur, it is difficult to offer affordable premiums. According to the Small Business Review, cyberinsurance premiums currently range from \$5,000 to \$25,000 per \$1 million of coverage. Deductibles are often high as well, with coverage sometimes beginning only after the first \$25,000 in losses.

Though the price of cyberinsurance is arguably not yet in alignment with the market, cyberinsurance and its underwriting process have evolved considerably since cyberinsurance’s introduction in the late 1990’s according to numerous studies by Jay Kesan, Ruperto Majuca, and William Yurcik of the University of Illinois at Urbana-Champaign. Insurers writing cyberinsurance have begun tackling the traditional insurance problems of adverse selection and moral hazard. Adverse selection stems from information asymmetry regarding an applicant’s current data security practices and the insurance companies’ resulting inability to distinguish between high- and low-risk applicants. To balance the asymmetry in the case of cyberinsurance, the insurer must undertake a thorough risk assessment to find any security vulnerabilities. An insurer usually gains an understanding of the applicant’s data security through a detailed questionnaire of more than 250 questions, which seeks information concerning the applicant’s network security policies, the applicant’s specific internet activities, and the

applicant's physical on-site security. To combat moral hazard – the potential failure of an insured to maintain its data security systems after obtaining cyberinsurance – cyberinsurers often require that the insured maintain security systems that are equal or superior to those in place at the inception of the policy. Cyberinsurers have also implemented provisions to encourage insureds to mitigate a loss by, for example, setting up a reward fund for those who give information resulting in the conviction of a cybercriminal. Cyberinsurers have also universally excluded losses stemming from the failure to back up systems, creating incentives for regular backups.

By tying lower premiums to higher data security standards, cyberinsurance holds the potential to increase the cybersecurity of the entire e-commerce world by encouraging industry best practices. Commentator Anna Lee suggested in a 2001 Vanderbilt Journal of Entertainment Law and Practice article that given the importance of nationwide cybersecurity, the government should subsidize cyberinsurance in the same way the government runs the National Flood Insurance Program. Some members of Congress have recently recognized the importance of cybersecurity insurance for improving national cybersecurity. Last year, Senators Rockefeller (D-W.Va.) and Snowe (R-Maine) introduced a bill calling for the government to encourage cyberinsurance by creating a public-private information clearinghouse where government and private firms could exchange cyberthreat information. Such information could potentially help cyberinsurers better assess the risk potential of applicants for cyberinsurance.

The cyberinsurance underwriting process is currently in need of further standardization to make the insurance more accessible to more companies. Clearly, the cyberinsurance market has not reached its full potential. According to a Betterly Cyber Risk and Privacy Market Survey, the cyberinsurance market is estimated to be around \$600 million, a 16-25 percent increase from 2009. Still this figure only includes the one-third of American companies who have chosen to purchase cyberinsurance. An insurance company that is able to offer competent cyberinsurance at an affordable rate has the potential to enter a rare growth area in the insurance world.

Conclusion

The internet revolutionized how companies do business and made digital assets among the most valuable for many companies. Cloud computing has increased the virtualization of still more companies. Nonetheless, only a fraction of American companies have chosen to protect their digital assets with cyberinsurance. Part of the reason for this lack of protection is the relative nascence of cyberinsurance. Though the product has existed since the late 1990's, the inherent difficulty in quantifying cyber risks has kept cyberinsurance pricing high. Still, high-profile, international breaches happen frequently, and it has become increasingly clear that standard front-end protection like firewalls and traditional property and liability insurance may be inadequate to protect companies' most important assets.

For insurers, cyberinsurance represents an opportunity to enter a new market. The cyberinsurance market has not reached its full potential because of the prohibitive

cost of the insurance. The cyberinsurance market is still in need of metrics and standardization that will streamline the application and underwriting processes and, in turn, make cyberinsurance more accessible to more businesses. An insurer that can quickly and efficiently quantify cybersecurity risks will be able to pass affordable premiums and deductibles on to its clients, and can potentially capture a piece of the burgeoning cyberinsurance market.

Christine Phan (cphan@zelle.com) is an associate at Zelle Hofmann Voelbel & Mason LLP in the firm's Boston, Massachusetts office. Catherine Colinvaux (ccolinvaux@zelle.com) is a partner in the firm's Boston office. Zelle Hofmann is a national law firm representing clients in their most challenging insurance-related disputes, antitrust claims and other complex litigation.

The opinions expressed are those of the authors and do not necessarily reflect the views of their clients, their firm, or Portfolio Media, publisher of Law360.