Is Cyber Liability Coverage as Essential as P&C Coverage?

by Elissa Doroff and Nancy Kelly

The potential benefits of cyber liability insurance coverage clearly outweigh its costs, making this type of coverage a must-have for businesses of all sizes across a myriad of sectors. Is cyber liability coverage as essential as property-casualty insurance coverage? Absolutely yes, for big and medium-size companies, especially considering the cost of the products available.

As cyber security threats continue to increase in frequency and ferocity, companies of all sizes now face serious risks that are both difficult to detect and complicated to remedy. And while recent breaches at large retailers and a prominent movie studio have captured the focus of the media, similar cyber crimes targeting smaller businesses, though far more common, often fail to gain national attention.

The average costs incurred because of a cyber security breach are also increasing, as companies have seen nearly a 10 percent jump in the costs of addressing a breach since last year (2014 Ponemon Institute Study). The damages from a cyber security incident can impact all aspects of a business, and the subsequent costs are rarely confined to those of a monetary nature.

The range of cyber security risks, although constantly evolving, can be generally categorized as commercial risks, litigation risks, and reputational risks, all of which can result in significant damage to the affected party.

To address these potential pitfalls, cyber liability insurance coverage is evolving to cover many of the damages associated with breaches and other cyber liability events. Companies can acquire coverage relating to breach response, cyber extortion, subsequent litigation, and a myriad of other risks. As the refinement of individual products drives down costs, companies must consider reducing their risk profile through the purchase of cyber liability insurance. Although

Continued on page 8

Continued from page 7

Elissa Doroff, JD, is a vice president and product manager for XL Group's Cyber & Technology team. In this role, she works to direct and manage XL's risk management services that are designed to minimize the frequency and severity of data breaches. Doroff has nearly a decade of cyber and technology insurance expertise, having worked as claims counsel at AIG and, most recently, as broker of cyber insurance at Marsh and McLennan, where she served as senior advisory specialist. Doroff has considerable experience presenting on technology, privacy and cyber topics for clients and industry associations, and she has published many industry-related articles. She is admitted to practice law in Massachusetts and Connecticut and is a licensed property-casualty claims adjuster and broker.

Nancy Kelly, JD, is a partner at Governo Law Firm. She previously worked as legal counsel for a reinsurance services provider in London, where she specialized in handling complex insurance and reinsurance coverage disputes and arbitrations, overseeing legal and regulatory compliance for broking and underwriting functions and drafting transactional documents for acquisitions of companies and portfolios. Kelly is also experienced in negotiating and drafting service agreements, nondisclosure agreements, and software licensing agreements and has developed expertise in international data protection and privacy issues. She is admitted to practice in Massachusetts, Rhode Island, and Maine and is a qualified solicitor authorized to practice in England and Wales. Kelly is rated "AV" by Martindale-Hubbell, signifying the highest level of legal knowledge, analytical capabilities, judgment, communication ability, and legal experience.

the decision of whether to use cyber liability insurance must be made on an individual basis, businesses of all sizes are finding that the benefits of cyber risk insurance coverage far outweigh its costs.

Commercial Risks

It is an unfortunate truth that in the immediate aftermath of a cyber security event, a business inevitably has to allocate significant resources simply to identify the source of the breach, ensure that it is no longer ongoing, and upgrade all systems to ward off future attacks. While companies often focus on these initial risks because they are most easily quantifiable, initial triage costs represent just the tip of the iceberg of potential damage stemming from a breach or other cyber security event. Commercial costs, such as the price to acquire new servers, recover damaged information, improve monitoring capabilities, or retain a public relations firm, can be significant risks for an entity.

Many companies exist under a false sense of security, believing that since they invest significant resources into cyber security systems, they have a very low risk of experiencing a breach. In fact, the sheer size of a company's cyber security capabilities is often less important than the company's ability to adapt, upgrade, and change existing systems. Constantly improving security system components, such as firewalls and encryption software, to stay ahead of sophisticated breaches is an important way to protect sensitive information; companies must not assume they are protected simply because their security systems were top-of-the-line when purchased.

While large corporations can be lulled into a false sense of security because of the size and sophistication of their existing security measures, small companies often overlook their cyber security risk because of the erroneous assumption that their diminutive size shields them from cyber criminals. In fact, many cyber security breaches target small to mid-size companies for this very reason. Hackers can easily scan multiple systems and only focus their resources on weaker systems that are easily breached. For this reason, small companies are not immune to cyber risk, but are, in fact, prone to it.

Litigation/Regulatory Enforcement Risks

The evolving sophistication of the hacking community only increases the likelihood of a targeted cyber attack and forces companies to recognize the importance of protecting their valuable data. Additionally, human error accounts for a large percentage of compromised data resulting from lost laptops and smartphones and/or inadvertent disclosure of sensitive personal or corporate confidential information. Companies in all industries face heightened scrutiny in the regulatory realm because of enhanced enforcement by governmental entities. Nearly every state in the country maintains data breach laws requiring timely notification of individuals whose information may have been compromised as well as adherence to standards imposed by the payment card industry (PCI) for those companies accepting credit cards. Just one security failure or privacy breach could lead to intense regulatory scrutiny and costly civil litigation.

On almost a weekly basis, we read about data breaches affecting millions of individuals. However, the future of litigation regarding these breaches is largely unsettled. The main hurdles plaintiffs must overcome in privacy breach litigation are standing and damages. Generally, for a case to survive a motion to dismiss, there must be evidence that information was exploited or compromised. One example is posting victims' information in a public forum. Some plaintiffs' attorneys argue that when customers pay for services, there is an implied promise by the defendant to use some of that money to implement cyber security precautions and that, as such, plaintiffs should be compensated.

The courts have been somewhat split on the issues of standing and damages, but have usually taken a pro-defendant stance. However, the decision making is very fluid. The most compelling cases involve data

breaches that occur after the company either knew there was malware on the system and did not act or was late to know and to notify. Questions are often raised, such as, was there a plan in place? Was the company diligent? And, are they now working to prevent a breach in the future? The wild card in litigation is often statutory damages, as those amounts can far exceed any other damages. Presently, plaintiffs need a consequent. However, at the end of the day, that does not eliminate the fundamental problem (the breach) and whether the courts may start to embrace that standing is still in question.

In 2010, an opinion by the United States Court of Appeals for the Ninth Circuit was thought to be precedent setting. In *Krottner v. Starbucks Corp.* (No. 09-35823), the court reviewed a district court order ruling that plaintiffs whose personal information was stolen—but not yet misused—had suffered an "injury" sufficient to constitute standing under Article III of the U.S. Constitution. While the court of appeals ruled that plaintiffs had standing to bring their lawsuit, it also affirmed the district court's holding that they failed to adequately state a claim under Washington state law. As such, both of the district court cases were eventually dismissed. Notwithstanding the dismissals, the importance of this ruling was quite significant in illustrating the court's willingness to uphold the "injury-in-fact" requirement given to a future threat of only credible harm.

In a decision issued by the Supreme Court in 2013, the court took an entirely different view to that in *Krottner*. Specifically, in *Clapper v. Amnesty International* (No. 10-1025), the court, albeit by a narrow majority, held that mere assertions of reasonable likelihood of potential future injury, or harm or costs incurred to avoid potential threatened injury, were insufficient to establish standing by plaintiffs in federal court.

In *Clapper*, the plaintiffs; attorneys; and human rights, legal, and media organizations whose work required them to communicate with foreign nationals challenged the

> "Many companies exist under a false sense of security, believing that since they invest significant resources into cyber security systems, they have a very low risk of experiencing a breach"

constitutionality of Section 1881a of the Foreign Intelligence Surveillance Act. This act was signed into law after September 11, 2001, authorizing the government to regulate certain governmental electronic surveillance of communications for foreign intelligence purposes. It was subsequently amended in 2008 to provide that the government may intercept electronic communications of foreign nationals without establishing probable cause. The majority opinion in this case found that "respondents lacked standing because they could not manufacture standing by incurring costs in anticipation of non-imminent harm."

Although not a data breach case, this decision was significant in the continuously developing data breach case law, as it was used by defense counsel to oppose data breach class actions by arguing that there must be actual damages or imminent harm.

As further evidence of the unsettled legal landscape in this realm, a 2010 decision handed down by Judge Lucy H. Koh of the Northern District of California in *In re Adobe Sys., Inc. Privacy Litig.*, No. 13-CV-05226-LHK (N.D. Cal. Sept. 4, 2010), found that plaintiffs in a consolidated class action had standing to sue, despite plaintiffs' failure to allege actual improper use of stolen personal information. This holding is quite significant, as it again shows that the standing debate is far from settled.

Specifically, in July of 2013, hackers allegedly targeted Adobe's servers and spent several weeks undetected, removing customer names, login IDs, passwords, credit and debit card numbers, expiration dates, and physical and email addresses. Plaintiffs alleged violations of the California Civil Code in their complaint and sought injunctive and declaratory relief.

Based upon defendants' arguments in *Clapper*, *Adobe* moved to dismiss the plaintiffs' claims, stating that plaintiffs in data breach litigation must assert "certainly impending" injuries and, again, relying on *Clapper*, that possible future injuries are insufficient. Judge Koh disagreed, finding that *Clapper* did not change the established standing in *Krottner* and that, even if Krottner was no longer good law, the harm threatened by the Adobe breach was certainly sufficient and imminent to satisfy *Clapper*.

Further, the court reasoned that requiring plaintiffs to wait until they actually suffer identity theft of potential credit- or debit-card fraud in order to establish standing is counter to the well-established principle that harm need not already occur or be "literally certain" to constitute injury. The court also noted that requiring plaintiffs to wait for threatened harms to materialize in order to bring lawsuits poses a unique standing issue because the potential duration of time that passes between a data breach and actual identity theft provides defendants with the opportunity to argue that thefts are not related to their breach.

In addition to potential litigation in the wake of a security incident or privacy breach, a major detriment for businesses facing cyber

Continued on page 10

Continued from page 9

security breaches is the risk of subsequent regulatory fines and litigation. Currently, the vast majority of states have mandatory compliance standards that set a baseline for how private information must be protected, as well as breach-notification statutes that dictate what must be done following the discovery of a breach. Remaining in compliance with the evolving amalgamation of privacy laws is a significant task; however, ignoring these issues can leave a company facing severe legal consequences.

While noncompliance can lead to major problems for a company, compliance with breach-notification statutes also carry costs of their own. Notification of affected parties, as well as the potential for providing future credit monitoring, can quickly amount to millions of dollars, even for mid-size companies.

Recently, federal regulatory enforcement actions by the Federal Trade Commission (FTC) and the Department of Health and Human Services have resulted in major fines against companies ranging from hoteliers to healthcare providers. Additionally, state attorneys general have begun bringing suits against the victims of cyber security breaches for noncompliance with state regulations, further increasing the risk of regulatory enforcement actions.

Private lawsuits also present a significant risk for a company dealing with a cyber security breach, and some courts have begun to ease the significant barriers to certifying a class action against a breached party. As discussed earlier, in the *Adobe* case out of California, the court allowed a class action to move forward, even though the individuals who had their information stolen from Adobe could not prove that they had actually been harmed. In allowing a class action despite the lack of specific evidence of damage to the individuals who had been exposed, the court opened the door for a potential onslaught of litigation focusing on cyber security breaches.

Further, a company's internal management of a cyber security situation may give rise to the potential for shareholder derivative suits. While this type of litigation is less prevalent, the recent cases involving Wyndham and Target show that any missteps involved with the ensuing management of a breach may further expose companies to litigation from their own shareholders. While the range of fines and lawsuits following a cyber security event are vast and potentially expensive, procuring cyber liability insurance and working to remain in compliance with all applicable laws greatly reduces the back-end risks associated with breaches.

Reputational Risk

One of the most enduring risks associated with a cyber liability event is the damage to an entity's reputation. At a time when privacy is often at the forefront of consumers' minds, any perception of organizational insecurity can lead to disastrous results for a business. Companies such as Target have reported losses totaling hundreds of millions of dollars in the quarter following cyber security events, and these costs do not take into account the long-term effects of the breach.

As consumers become increasingly aware of their own security, they are demanding more protection from those tasked with storing their credit card information, medical records, and other sensitive data. Failure to maintain a strong reputation for security can find companies experiencing an exodus of previously loyal customers.

For entities that work solely with other businesses (B2B), the reputational damage arising from a cyber security breach has the potential to bankrupt the company by driving away vendors, partners, and clients. Many businesses are wary to work with companies that may serve as jumping-off points for hackers trying to access larger systems. If hackers can gain access to the files of smaller B2B companies, they may be able to use these companies to breach larger, more extensive systems. Often, the risks of working with a vendor that may have problematic cyber security measures are too great, and larger companies will simply find more secure vendors with better security measures.

Risk Mitigation/Risk Transfer

With a volatile threat environment coupled with the ever-changing legal and regulatory landscape, companies of all sizes must be prepared for a data breach. Essential preparedness should include either risk mitigation or risk transference.

Emerging threats are no longer simply emanating from disgruntled employees looking to publish coworkers' personal information on social media or from cyber extortionists seeking $50,000 to unlock your network. Instead, attacks are stemming from different constituents, ranging from malicious targeted attacks and foreign espionage to supply chain disruption and careless staff. Also, as discussed above, the regulatory landscape presents several requirements with which companies must comply.

For example, the National Institute of Standards and Technology (NIST) framework provides guidelines, as do international requirements and regulation. State attorneys general requirements have become more stringent, and any business that accepts credit cards must comply with PCI standards. In addition, the SEC, Federal Trade Commission, and Office for Civil Rights (OCR) have become increasingly aggressive in leveraging fines and penalties for noncompliance.

Accordingly, today's cyber security insurance responds to these risks. In general, the policies provide both first- and third-party risks. First-party coverage may include business income/extra expense coverage; data asset protection; cyber extortion; and, most importantly, event, or crisis, management. Policies may be tailored to include any or all of these coverages, but nearly all contain event response coverage.

Specifically, business income/extra expense coverage provides for loss of business income resulting from a data breach. It may also extend to provide coverage for dependent business interruption if caused by a critical vendor. Data asset protection is

afforded as well and typically includes the cost of repairing and restoring computer systems and intangible assets that are corrupted or destroyed by a computer attack.

Cyber extortion coverage provides for costs of consultants and extortion monies for threats related to interrupting systems and releasing private information typically targeted by ransomware, which requires payment to unlock the compromised network. Finally, the most important first-party coverage is event management, sometimes called crisis management. Encompassed within this coverage are the following costs resulting from a security incident: forensic investigation services, breach notification services (including legal fees and call center services), identity monitoring expenses, and public relations firm retainers.

Third-party risks include data breach incidents that result in unauthorized access to information or personally identifiable, nonpublic information, such as bank account numbers, credit card numbers, or Social Security numbers, as well as third-party corporate confidential information.

Third-party coverage typically includes privacy liability, privacy regulatory defense costs, and network security liability. Privacy liability provides for defense and liability coverage for failure to prevent unauthorized access, disclosure or collection of confidential information or third-party corporate confidential information, or failure of others to whom you have entrusted such information (such as a data-storage facility, credit card processor, or other critical vendor). It also extends to include liability for failing to properly notify of a privacy breach, with claims typically brought by customers, employees, and trading partners.

Privacy regulatory defense costs include costs to defend an action or investigation by a regulator because of a privacy breach, including indemnification for any fines and penalties assessed. These claims are typically brought by an attorney general or the applicable regulatory body, such as the FTC or OCR.

Finally, network security liability provides defense costs and liability coverage for failure of system security to prevent or mitigate against a computer attack, including but not limited to spread of a virus or a denial of service. Failure of system security includes failure of written policies and procedures addressing technology use; these claims are typically brought by third parties, customers, and employees. In addition, the policies have expanded to provide coverage for PCI fines and penalties if assessed in a jurisdiction where insurable.

As cyber and technology risks continue to evolve, cyber insurance coverage will as well. Insurance companies are continuing to accumulate more actuarial data, based on the loss history of various industries, each corporate customer's use of technology, and the corporation's own level of security.

Alternatively, if a company chooses not to transfer its risk, several risk mitigation techniques must be considered. Effective contract drafting may help to mitigate risk if designed to include provisions for defense and indemnification, limitations of liability, and mediation or arbitration provisions. Additionally, businesses should review their cyber security posture to ensure that an information security policy is in place. At a minimum, this policy should include an incident response plan (with annual testing), a privacy policy that the legal department keeps current with respect to regulatory requirements and privacy law, and background checks and privacy awareness training for all employees. Companies should also ensure that access to data is contingent on an employee's role and a strong password management process and that mobile devices connected to a company's network are secure and employ a data segregation scheme and encryption. Most importantly, all companies should be prepared for security incidents by maintaining agreements with reputational risk advisers and attorneys who are well-versed in privacy law.

Ultimately, as businesses of all sizes face increased cyber security threats, they must continually address those risks that have the potential to ruin a company. While preventative measures clearly decrease the risk of a breach, cyber liability insurance coverage also has the potential to greatly reduce a business's risk profile. As insurance products continue to evolve, all companies must consider purchasing this coverage to protect themselves from increasingly sophisticated cyber liability threats.

For more on this topic, the authors suggest the following sources:

- Sarb Sembhi, "An Introduction to Cyber Liability Insurance Cover," ComputerWeekly.com, www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover (accessed January 20, 2015).
- National Association of Insurance Commissioners & The Center for Insurance Policy and Research, "Cyber Risk," Nov. 24, 2014, www.naic.org/cipr_topics/topic_cyber_risk.htm (accessed January 20, 2015).
- Law360, "Adobe Data Breach Ruling Gives New Hope to Plaintiffs," September 24, 2014, www.law360.com/articles/579164/adobe-data-breach-ruling-gives-new-hope-to-plaintiffs (accessed January 20, 2015).
- Ponemon Institute, 2014 Cost of Data Breach Study, www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/ (accessed January 20, 2015).