COMMENTARY: Risk managers can't afford to overlook cyber liability insurance

May 06 2016 David Owen and Benjamen Starkweather

Almost every news cycle brings another story about a business losing valuable customer data and electronic information to hackers, both foreign and domestic. As ever more valuable information becomes potentially accessible to cyber thieves, the resulting losses seem certain to increase both in frequency and severity. While much public focus is on the scale of exposed data and the numbers of affected customers, little attention is paid to the rapidly evolving efforts to insure against these events and the substantial liabilities that can result from them. In fact, there is no area of corporate liability coverage that is developing faster than cyber liability insurance.

In a 2014 cryber crime study (PDF), cyber security provider McAfee estimated that such attacks costs the global economy more than $400 billion annually. According to recent reporting, the market for cyber security services is expected to more than double to $170 billion by 2020, while cyber security insurance premiums are expected to triple to $7.5 billion over the next five years.

In 2013, Target Corporation felt the sting of cyber crime when a data breach released the credit card information of over 70 million of its customers, resulting in over $250 million in related expenses. Although Target recovered $90 million from insurance, it appears that Target's original expectations for coverage were substantially eclipsed by restrictive policies.

Additionally, regulators and state authorities are expanding their reach to impose increasingly large penalties for data breaches. In April 2015, for example, the Federal Communications Commission (FCC) penalized AT&T $25 million for a breach that exposed the information of less than 300,000 customers. The regulatory action included substantial remedial measures and related expenditures, with AT&T agreeing to mandatory compliance and monitoring plans lasting up to seven years.

Although it has arrived only recently on the marketplace, the expanding presence of cyber liability insurance reflects the rapidly evolving threats and consequences of data breaches, as well as the proliferation of laws intended to deal with them. Most commercial general liability (CGL) policies presently exclude cyber liability

from coverage, as do the most recent ISO forms. Filling that gap in coverage can be both expensive and fraught with uncertainty, with many companies yet to focus adequately on the issue.

Most companies are at least aware of cyber security risks. A September 2015 Wells Fargo survey (PDF) of 100 U.S. companies showed that 85 had purchased some form of cyber security insurance, and almost half had already filed a breach-related claim.

Coverage considerations

When acquiring cyber liability coverage, it is vital to know exactly what needs protecting and what are the likely future risks. There is insufficient loss history and data to make these assessments reliably, given the diverse and expanding nature of cyber threats and associated liability. And because many past predictions have underestimated the problem, insurance companies are now pricing such policies to reflect that trend.

Premiums negotiated today are likely to depend heavily on policy provisions. It is therefore vital to break down identifiable risks into discrete elements, in order to optimize coverage and costs to a firm's needs and risks. Although answers to the relevant coverage questions may be elusive, particularly for specialized data applications, key questions include:

- How sensitive is the data held by the organization? What are the anticipated legal and financial exposures in the event of a breach?
- Are state-of-the-art security measures in place, and is there a continuing program to monitor and improve security?
- What additional security protocols may be implemented? Does the cost of implementation mitigate risks and lower the premium?
- To what extent has the firm addressed the risks from third-party data access?
- Are malicious acts by employees covered?
- What will be the impact of claims made on future premiums, and can premiums be reduced over time if no claims are made?
- How are conflicting laws handled (especially for companies holding personal information data related to EU citizens) for coverage purposes?
- What happens if important claim information (e.g., timing of a breach) cannot be established with

certainty?

Cyber insurance policies typically cover both first-party losses (i.e., direct or extra expenses from responding to a breach) and third-party losses (i.e., expenses associated with the aftermath of a breach). First-party costs can include hiring of information security firms, public relations campaigns, notification of affected parties, credit monitoring for affected individuals, restoring data or systems, and legal services. First-party losses might also include business interruption from malware, including lost revenues and remediation expenses. Third-party losses can include consumer damage claims, legal costs, media liability, data loss, and regulatory penalties.

Obtaining a policy may itself entail significant compliance expense. Insurance provider AIG, for example, offers a $75 million policy for cyber attacks, but only for large companies with sufficient resources to meet high security standards. Renewing policyholders also face tough decisions as premium renewal costs have doubled or even tripled in many instances over the past year.

Costs and consequences

Depending on the amount and type of information exposed, the risk and consequences of a breach can vary significantly. In most cases, a breach limited to customer names and addresses would raise a relatively small prospect of injury or liability. In contrast, the Ashley Madison "dating" site hack, which exposed all its customer names, posed an entirely different and very significant risk to the company, because it guaranteed its users privacy.

Organizations with a prominent public presence can also face unexpected risks and consequences from cyberattacks. For example, when North Korea hacked Sony Pictures Entertainment, in apparent retaliation for a satirical movie, the company's co-chairwoman was forced to resign, partly due to the embarrassing nature of her leaked emails.

For most companies, the theft of customer social security or credit card information would trigger numerous legal obligations in almost every U.S. state, which can be particularly costly. Breaches involving payment information would also typically activate expensive investigation and remedy requirements contained in contractual agreements between and among the company, the issuing bank(s), and the credit card networks. Most companies holding customer credit card numbers are unable to survive the loss of that payment method.

For multinational banks, many of the laws and risks are distinct, as are some of the regulatory challenges and uncertainties. Banks often collect extremely large databases of highly sensitive personal information from large numbers of individuals all over the world. This data is also among the most targeted by hackers, given the potential rewards. Additionally, multinational financial firms face differing and sometimes inconsistent

jurisdiction-specific data protection requirements.

While the encryption of sensitive data can eliminate legal obligations under many different privacy laws, it can nevertheless be cumbersome for employees and company operations. Insuring against doomsday breach scenarios for such entities is not for the fainthearted.

Healthcare is another data-intensive industry that routinely stores and transmits some of the most sensitive personal information, and as such, it faces an uncertain prospect of potentially huge cyber liabilities. Notwithstanding that risk, the use of electronic health records (or EHRs) is strongly incentivized by healthcare regulations. Unsurprisingly, cyber liability coverage costs in healthcare have been exploding recently.

Finally, many of the most damaging consequences flowing from a data breach may be unquantifiable or un-insurable, such as reputational damage or a drop in stock prices. Following Target's widely publicized breach, for example, its profits declined by nearly half, and its stock price initially fell 11 percent.

Shifting regulations

Complicating the cyber risk environment are unpredictable shifts in regulatory and legal circumstances. For example:

- In October 2015, European courts invalidated the "safe harbor" provision of a data transfer agreement that allowed multinationals to share European citizens' data with U.S. subsidiaries and processors. A key triggering event for that ruling was the unprecedented leak by former U.S. National Security Agency (NSA) contractor Edward Snowden, which revealed that American intelligence agencies had virtually unfettered access to EU citizens' private data.

- The U.S. government's recent dispute with Apple over iPhone encryption suggests that legal and technical uncertainties will continue for the foreseeable future.

- The fallout from the recent "Panama Papers" leak continues to touch prominent heads of state and businesses leaders around the globe.

- In 2014, the New York Supreme Court ruled that Sony Corporation's commercial general liability policy, which covered publication of material in violation of privacy rights, did not apply to information stolen and disclosed by third parties (i.e, hackers). In other words, because Sony itself did not publish the materials, the policy did not apply. This ruling was among the first decisions to address data breach coverage and reinforced the need for companies to buy specialized cyber insurance policies in order to avoid a potential lack of coverage under their CGL policies.

Conclusion

The trends driving this increased need for and focus on cyber security and cyber insurance coverage will likely endure. The scope and volume of information accessible or disclosable by electronic means will continue to rise. As more companies fall victim to hacking and other breaches, and as others realize that their traditional CGL policies will not cover the consequences of a substantial data breach, increasing resources will be allocated to security systems and insurance to mitigate the distinct and growing risks.

Although no one can predict where hackers will strike next, or where negligence or misconduct may lead to data loss, the companies that can self-assess and respond with sensible security and insurance coverage will be best positioned to manage the growing risk as efficiently as possible.

David R. Owen *is a partner at Cahill Gordon & Reindel LLP, and a member of the firm's Litigation and Corporate Governance & Investigations practice groups.* ***Benjamen Starkweather*** *is an associate at Cahill, focusing on litigation.*