Cyber Risk & Insurance

by David L. Stegall & Joy M. Gänder | 1 Ct. J. Sci. Tech. 1 (2015)*

April 2015

INTRODUCTION

This article examines the issue of cyber risk and exposures to loss, including recent legal and legislative developments. It reviews and discusses the options for cyber insurance coverage and the coverage limitations of such policies and endorsements. The article also explains the first and third party exposures to loss that cyber insurance covers as well as other benefits of cyber insurance. To highlight the impact of cyber breaches and the benefits of cyber insurance, this article examines recent cyber breaches, including the cyber breaches at Target and Home Depot. The purpose of this article is to provide guidance to legal practitioners and other professional advisors regarding potential cyber risk exposures.

Cyber Risk & Insurance

While cyber threats have been a concern for more than a decade, the last eighteen months have been marked by a number of large-scale cyber breaches. These breaches caused companies and insurers to expend considerable financial resources to recover from the breach and mend their damaged public images. As a result of the increase in cyber threats, public and private entities are scrambling to ensure the security of their systems and the information and data these systems store. As part of the risk management analysis presented by cyber threats, companies of all sizes are evaluating their existing insurance policies to understand what, if anything, traditional insurance policies will cover with respect to cyber claims. In most instances, obtaining additional cyber coverage, either through special endorsement to existing policies or through a stand-alone cyber liability policy, is necessary.

How widespread is the Incidence of Cyber Threats?

Recently, there have been a number of sophisticated and costly cyber attacks, the most notable of which involved Target, Home Depot, Anthem and Sony. The first breach, which occurred in November and December of 2013, involved the installation of malware onto Target's point of sale system. As a result, payment card data for more than 40 million credit and debit card customers was compromised. According to Target's public filings, it has incurred a total net breach-related expense of approximately $160 million, reflecting approximately $250 million of gross expenses. They recovered $90 million from insurance.[1] In March of 2015, Target agreed to pay up to $10 million to settle a class action lawsuit in connection with the data breach. Individuals able to show actual damage could receive up to $10,000.[2]

In the Home Depot breach, a cyber criminal gained access to a vendor's log-in information, which then allowed the individual to breach the perimeter of Home Depot's network. The hacker installed custom-built malware on Home Depot's self-checkout system. As a result of the breach, Home Depot recorded expenses of $63 million, which Home Depot expects to offset by approximately $30 million of insurance payments.[3] The Home Depot breach exposed the credit and payment card information of more than 50 million customers and also allowed hackers access to the email accounts of more than 53 million customers.[4] Like Target, Home Depot also anticipates legal action by customers and payment card networks will be initiated against it.

More recently, the Anthem attack exposed 80 million records, including proprietary information, credit and debit card information and social security numbers. The Sony attack in November 2014 involved far fewer records (approximately 47,000) but was aimed at embarrassing Hollywood executives in an attempt to coerce Sony into withholding the release of a movie for political reasons.[5]

While the Target, Home Depot, Anthem and Sony breaches made international headlines because of their size and scope, few businesses are immune to cyber threats. In a recent study of 111 insured cyber claims, companies with revenues

[1] Target, Annual Report on Form 10-K for the fiscal year ended January 31, 2015.
[2] CNN Money, Charles Riley and Jose Pagliery, Target Will Pay Hack Victims $10 million.
[3] Home Depot, Annual Report on Form 10-K for the fiscal year ended February 1, 2015.
[4] https://threatpost.com/home-depot-breach-cost-company-43-million-in-third-quarter/109629.
[5] A Quick Guide to the Worst Corporate Hack Attacks, Bloomberg, Keith Collins, February 5, 2015.

under $2 billion accounted for 72 percent of cyber incidents.[6] This same study revealed the median number of compromised records was 3,500, and the average cost to the breached company was approximately $956 per record. In another study, interviews were held with representatives from 314 companies from 10 countries. The average breach cost for US companies was $201 per data record.[7]

The reader is cautioned to use care in drawing conclusions from these studies; one study examined data from a limited number of insured cyber claims, and the other is a function of self-reported information. However, every entity that electronically collects stores or uses customer and employee information should understand its own cyber exposures and the potential for incurring data breach response expenses. Since most businesses rely to some extent on computer networks, even companies that do not collect or store private or financial information from customers may still experience a cyber loss. Potential losses include hacking of critical business controls and loss of trade secrets and other confidential business information.

What is At Risk for Cyber Breach?

Currently, cyber breaches seem aimed primarily at data and information. However, as discussed briefly below, the future will likely see an increase in the number, scope and success rate of attacks on the United States' critical infrastructure and systems.

Particularly vulnerable to cyber threats are: payment card information, personally identifiable information, private health information, intellectual property and other business and trade secrets. Personally identifiable information is any information that, by itself, or together with other information, can be used to identify a person. Examples of personally identifiable information include social security numbers, drivers' license numbers, addresses, phone numbers and email addresses. Private health information is generally defined by HIPAA (Health Insurance Portability and Accountability Act) to include any information created or received by a health care professional, health care or life insurer, public health department that relates to the past, present or future physical or mental health or condition of any individual.[8]

[6] NetDiligence Cyber Claims Study 2014 http://www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf.
[7] 2014 Cost of Data Breach Study: Global Analysis.
[8] HIPAA "'Protected Health Information': What does PHI Include?", www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/

While this article focuses primarily on private information breaches, it is important to note that many insurance and cyber security experts believe that the most serious breach exposure is to critical industries and infrastructure. Government agencies, financial institutions, healthcare organizations and other institutions are under continuous attack of one sort or another. Particularly alarming was the 2012 attack on Telvent, a manufacturer of smart-grid control software used in certain electrical grids and pipelines that transport oil, gas and water. In Telvent, hackers gained access to customer project files, which, in turn, gave the hackers access to Telvent's customers' industrial control systems. Although detected before the systems went into effect, industry experts understand it is simply a matter of time before another company's critical industrial controls are compromised as a result of a cyber breach.[9]

Less publicized is the cyber-breach at an un-named German steel mill that was reported in December 2014. Hackers used the steel mill's production network to access the mill's equipment control systems, which led to "massive" property damage resulting from malfunctions in the blast furnace. Prior to the cyber event at the German steel mill, the only other known example of physical damage caused by a cyber breach occurred when the United States and Israeli governments used a digital weapon, called Stuxnet, to shut down an Iranian uranium enrichment plant.[10] Interestingly, the Telvent cyber breach utilized the infected project files hacking tactic that was used by the United States in Stuxnet.[11]

Traditional vs. Cyber-Specific Insurance Products

In its simplest terms, any individual or business entity that conducts business over the internet uses the internet or other network system to collect or store data is exposed to cyber losses as the result of a breach or cyber attack. Unfortunately, the majority of standard property commercial insurance policies only provide insurance coverage for losses incurred in connection with damage to, or destruction of, the insured's ***tangible property***. Most policies specifically state electronic data is not considered "property" and any loss of, or to, will not be covered by commercial property or liability policies. In practice, this means if an employee's business laptop containing customers' personally identifiable

[9] The Biggest Security Threats We'll Face in 2015, Wired, Kim Zetter, January, 4, 2015
[10] A Cyber Attack Has Caused Confirmed Physical Damage for The Second Time Ever, Wired, Kim Zetter, January 8, 2015
[11] The Biggest Security Threats We'll Face in 2015, Wired, Kim Zetter, January 4, 2015. See also, The Real Story of Stuxnet, David Kushner, Spectrum, February 26, 2013 http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

information is stolen, the property policy will cover the cost of the lost equipment, but the far greater exposure – the loss or unintended release of confidential business information, including customer data and business secrets - will not be considered a loss recoverable under a traditional commercial liability policy. It is important to note that companies cannot avoid liability by contracting with a third party to provide hosting services. The entity that collects or gathers the information will remain liable for any breach or unauthorized use or disclosure.

Companies managing the financial implications of cyber exposures can close gaps in coverage by purchasing a cyber endorsement to a traditional policy and/or obtaining a stand-alone cyber insurance policy, the latter of which traditionally provides many more coverage options and higher limits than the former.

Unlike most commercial property and liability insurance policies, cyber insurance policies and endorsements are not standardized. As such, special care should be given to reviewing these insurance products to assess any gaps in coverage.

What Does Cyber Liability Insurance Cover?

While the specifics of each policy vary, as a general rule, a cyber insurance policy provides coverage for breach response expenses associated with a cyber breach or cyber attack of a computer system (first party coverage). Cyber liability insurance policies may also provide coverage for damages caused by the insured's accidental or inadvertent release of payment card information, personally identifiable information or private health information (third party liability). In some instances, where the insured's information is stored by a third party (e.g., a Cloud service provider), the insurance policy will also cover any damages incurred as a result of the breach of that service provider's system or network[12].

Specific expenses and losses that a cyber insurance policy may cover include:

First Party Coverage:

- Expenses associated with damage to a computer system or network caused by a cyber threat.

- Expenses associated with the loss of and recovery of any data.

[12] Minda Zetlin, "5 Reasons You Should Have Cyber Liability Insurance", Inc. http://www.inc.com/minda-zetlin/6-reasons-you-should-have-cyber-liability-insurance.html

- Business continuity expenses and reimbursement of lost income arising out of an interruption of the insured's business, or ability to offer services as a result of the cyber breach.

- Expenses associated with notifying affected individuals of the disclosure of their PPI, including the establishment and maintenance of a dedicated call center to respond to inquiries regarding the cyber event.

- The cost of retaining public relations and crisis management teams to oversee and manage the public fallout in connection with the cyber breach or disclosure.

- Expenses associated with regulatory investigation resulting from the cyber event.

- Coverage for cyber extortion in the event the insured's computer systems and networks are rendered unusable as a result of the use of ransomware.

Third Party Liability:

- The cost of defending and paying judgments or settlements in connection with third party lawsuits against the insured for the disclosure of personally identifiable information.

- The costs of providing ongoing credit bureau monitoring, if necessary.

- Expenses associated with legal proceedings by the insured to protect intellectual property rights that were exposed, stolen or disclosed as a result of the cyber event.

- Liability coverage for the insured's website content alleged to be slanderous or libelous.

- Property damage or injury to persons resulting from a cyber event that endangers persons or property, including damages from a breach of critical infrastructure.

- Expenses, including attorneys' fees, associated with legal actions against third parties.

Other Benefits of Cyber Insurance

The primary purpose of cyber insurance is to manage the financial risk of a cyber event. Insurers underwriting cyber insurance frequently offer pre-loss guidance regarding an insured's cyber exposures and IT systems, and the best methods to manage those risks.[13] After a cyber breach or inadvertent disclosure, the insurance company and its affiliates and contractors can be invaluable in assisting with identifying the source of the breach, repairing the breach, and communication with customers, employees, the media and state or federal regulatory agencies. For instance, if personally identifiable information is stolen or inadvertently disclosed, the insured will need to notify the individuals whose information was compromised and may also need to deal with reputation damage and negative media attention resulting from the breach. Many cyber insurance companies have relationships with public relations firms and other entities that can ease some of the work and stress associated with a cyber breach.

Post-Breach Responsibilities

Once a company discovers a cyber breach, they must notify customers and other affected individuals and businesses. Discovery of the breach may also trigger a notification requirement to state and federal regulatory agencies. Depending on the circumstances, it is possible that a criminal investigation will be initiated.

One of the most important post-breach actions a company must take is notifying affected individuals of the breach. This notice should be straightforward and easy to read and should include the following information[14]:

- The time period during which the breach occurred.
- The number of records compromised and the type of information that was compromised.
- How the breach was detected and any actions taken or to be taken to limit or contain the impact of the breach, as well as any revision or modification of the company's existing data security procedures.

[13] Zetlin.
[14] Martin J. Frappolli, Managing Cyber Risk, The Institutes, January 2015, Section 2.15.

- Whether law enforcement has been advised of the breach and the status of any investigations by such authorities.
- Contact information for persons answering questions regarding the breach.

In addition to notifying affected individuals of the breach and managing any investigations pertaining to the breach, the company may want to maintain a call center to answer customer inquiries and provide post-breach, ongoing credit monitoring services so affected individuals will know immediately if their data is being used inappropriately.

The Cost of Cyber Insurance Policies

The cost of cyber insurance will vary depending on the size and type of business conducted by the entity, and the amount and type of information collected and/or stored[15]. The cost will also be impacted by the quality of the insured's e-security protections, as well as the policy limits and deductible levels chosen by the insured. However, there is a competitive market with robust interest and capacity to provide the necessary coverage and limits.

Legislative and Regulatory Framework

The Gramm Leach Bliley Act ("GLB Act") and the Sarbanes-Oxley Act ("SOA") place certain requirements on banks, financial institutions and public companies regarding personally identifiable information and disclosure. The GLB Act requires banks and other financial services companies to protect their customers' personal financial information and data. This includes the requirement that organizations institute written information security plans detailing the procedures taken to protect consumer information. The SOA indirectly requires that companies audit and assess the security of their financial reporting systems to comply with the requirements regarding accuracy of financial disclosures.

While not codified yet as law, the payment card industry has issued data security standards for domestic companies processing credit cards. This guidance delineates the standard of care for preventing, detecting and responding to security breaches, including the training of employees regarding security requirements and compliance.

[15] National Association of Insurance Commissioners, "Cybersecurity", Feb. 13, 2015. http://www.naic.org/cipr_topics/topic_cyber_risk.htm

Currently, statutes regarding cyber security are not uniform, though a number have been proposed. This can be especially problematic for companies that operate in multiple states or have customers or employees in multiple jurisdictions. For instance, almost every state has its own law regarding the notification process in the event of a cyber breach or inadvertent disclosure. These state laws may differ as to when the breach must be disclosed to its customers and employees.

Further, in some instances, a breach that may not necessarily trigger notification requirements to the individuals whose information was disclosed may trigger a notification requirement to the State Attorney General. Finally, regulations and statutes regarding notification are frequently being amended and updated by the states' legislatures, which makes it very difficult for companies in the midst of a cyber crisis to understand the scope of its obligations and duties. It is in this area that cyber insurance companies can be helpful.

Recent Governmental Recommendations and Actions Regarding Cyber Security

The field of cyber law is constantly evolving in response to changes in technology and the abilities and aggressiveness of cyber criminals. As the number and complexity of the breaches increase, so will the regulatory requirements and burdens placed on entities that collect and store payment card information, personally identifiable information and private health information.

Regulations and Guidance Related to Financial Industry. Recently certain state banking regulators have added cyber security inquiries to bank safety and soundness examinations. The Securities and Exchange Commission (the "SEC") has also advised that companies and their boards of directors must be prepared to prevent and respond to cybersecurity issues. The SEC's recommendations include:

- Boards of public companies should have directors with an expertise in information technology and security.

- Public companies should have a dedicated set of employees responsible for protecting the privacy and security of the company's information and data.

- Public companies should have and regularly test the effectiveness of a breach response and recovery plan.[16]

Regulations and Guidance Related to Health Care Industry.

HIPAA and the Health Information Technology for Economic and Clinical Health Act ("HITECH") set forth regulations regarding the collection, storage and disclosure of private health information by health care providers and any organization that collects private health information. Expanded notification requirements and penalty provisions are included in the HITECH Act.

Recent Litigation and Legal Implications of Cyber Events

A more recent development in the area of cyber losses is insurance companies pursuing legal action against third parties who may bear some responsibility for cyber threats or breaches sustained by the insurance policyholder. For example, Travelers Casualty and Surety Company[17] is pursuing an action against an insured's website designer. The claim alleges the web designer did not adequately design and maintain the insured's website to avoid cyber breaches, inadequate anti-malware software or software patches, and failure to adequately encrypt customer data collected by the insured.

This lawsuit exposes an entirely new type of business to the implications of cyber liability and highlights the need for these service companies to pursue their own cyber liability coverage. Had the Telvent breach ultimately led to the access of customers' control systems, it is possible that Telvent would have found itself party to a lawsuit by its customers and possibly its customers' insurance companies.

The Travelers lawsuit can guide attorneys and business advisers drafting and negotiating technology contracts for clients who store sensitive customer information on their computer systems. For example, an accountant's or attorney's computer network may contain a client's sensitive business information. If those networks are breached, the advisors may be subject to an action by their client's cyber liability insurance company.

---

[16] Frappolli, Section 3.23. SEC Commissioner Luis Aguilar (2014, June), *Boards of Directors, Corporate Governance and Cyber Risks: Sharpening the Focus*, Speech presented at the New York Stock Exchange, New York, New York.

[17] Steve Foresta, Silvia Babikian, Benjamin Trevsky, "Cyber Insurers on the Prowl for Liable Third Parties", Orrick, February 18, 2015. http://blogs.orrick.com/insurance/2015/02/18/cyber-insurers-on-the-prowl-for-liable-third-parties/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original

Attorneys and other business advisors deal in very time sensitive client matters, which could make them an attractive target for cyber extortion, where a hacker freezes a computer network until a financial ransom has been paid. Similarly, "hacktivists" who use cyber-attacks to protest against certain businesses or industries may target the computer networks of attorneys and business advisors for these businesses and industries.

An increase in the frequency and scope of cyber events has the potential to increase the number of class action lawsuits associated with cyber events. These class action lawsuits may be initiated to recover damages for the theft or disclosure of PII or to meet regulatory requirements (e.g., investment loss caused by failure to comply with SEC recommendations). As state and federal agencies issue regulations and increase oversight, there will be a resulting increase in administrative actions against companies failing to meet the regulatory requirements.

Conclusion

The recent experiences of the companies discussed above highlights the threat and liability associated with conducting business via the Internet and other networks. Both the cyber security industry and the insurance industry have made meaningful strides over the past decade to design security systems and insurance products to control and/or mitigate the exposures to loss. Advanced persistent threats will continue to threaten enterprise security, industry, commerce and government. They have changed how we manage and finance risks and the function and importance of the offices of the Chief Information Security Officer within any organization. Cyber threats are becoming more intelligent, resilient, and obscure than they have ever been in the past. Controlling these threats will require multiple disciplines, within multiple industries and by multiple institutions, all working together.

***Authors**

David L. Stegall, CPCU, ARM, ARe, RPA is Principal Consultant of Risk Consulting & Expert Services, a fee-for-service only, consulting practice in Birmingham, Alabama. Risk Consulting & Expert Services provides insurance, reinsurance and risk management consulting to commerce, industry and

government. Mr. Stegall has over 35 years of insurance industry experience. He is a Chartered Property & Casualty Underwriter, an Associate in Risk Management, an Associate in Reinsurance and a Registered Professional Adjuster. His career has included experience as an underwriter, an agent, a broker, a reinsurer, an MGA, a captive manager, and as an expert witness. He serves as Secretary of the Society of Risk Management Consultants, is an Associate Member of the American Bar Association-Litigation Section, a member of the Registered Professional Adjusters Association and a member of the Forensic Expert Witness Association.

Joy M. Gänder, CPCU, ARM is Principal Consultant of Gänder Consulting Group, LLC in Madison, Wisconsin. Gänder Consulting provides independent risk management consulting, expert witness and litigation support services to private, public and non-profit organizations. The firm sells no insurance. Ms. Gänder has over 30 years in risk management, insurance and coverage analysis experience with expertise in underwriting and claims negotiations. Ms. Gänder is a member, and immediate past-president, of the Society of Risk Management Consultants, member and past-president of the Dairyland Chapter of the Society of CPCU, and is adjunct faculty in the School of Business – Actuarial Science and Risk Management department at the University of Wisconsin.