UIC John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 3 Article 4

2014

Cyber-Security Insurance: Navigating the Landscape of a Growing Field, 31 J. Marshall J. Info. Tech. & Privacy L. 379 (2014)

Daniel Garrie

Michael Mann

CYBER-SECURITY INSURANCE: NAVIGATING THE LANDSCAPE OF A GROWING FIELD

DANIEL GARRIE* & MICHAEL MANN**

I. INTRODUCTION

In today's marketplace where businesses are constantly being threatened by data breaches and cyber-attacks, it is imperative that a global company obtain cyber-security insurance. The cyber-security insurance market is now the fastest growing segment of the insurance industry as cyber-threats are on the rise and business trade partners and consumers are insisting on safeguards for their confidential and sensitive information.[1] Given how great the potential liability and damages resulting from a data breach can be companies cannot afford to be without cyber-security insurance. As this new form of insurance continues to emerge and develop, it is important for companies to understand the current state of the market and the nature of the protection that they need in order to prudently obtain coverage for cyber-security breaches.

This article will address these issues in turn, focusing first on the market, pointing out the need for this specific type of coverage, the inadequacy of general liability policies for cyber-risks, and general issues related to cyber-security insurance. Then we will turn to the relevant considerations in obtaining a cyber-security policy, including the cyber-threats to be aware of and the types of coverage available.

---

* Daniel Garrie is a Partner of ZEK's Cybersecurity Practice, and coordinates the firm's privacy, forensics, and e-discovery practices. He is the Executive Managing Partner at Law & Forensics LLC, a global forensic, cybersecurity, and e-discovery technology consulting firm. Mr. Garrie has a broad and diverse expertise in the areas of data governance and electronic discovery, including serving as an E-Discovery Special Master where he has served in federal and state courts across the United States. Mr. Garrie has written over 100 articles on legal and technology topics and has lectured to the bench and bar across the United States. He is also the author of *Plugged in Guide to Software*, *E-Discovery & Dispute Resolution*, and *Cyber Warfare and the Law*.

** Michael Mann is a legal associate at Law & Forensics and third year law student at New York University School of Law

1. Cadie Thompson, *Cyber insurance becoming more mainstream*, CNBC (Apr. 17, 2014, 2:51 PM), http://www.cnbc.com/id/101591858#.

II. CURRENT STATE OF THE MARKET

A. CYBER-SECURITY COVERAGE IS NEEDED

Data breach incidents are increasing at an alarming rate.[2] According to the United States Government Analysis Office, for the fiscal years 2006-2012, the number of incidents "that have placed sensitive information at risk, with potentially serious impacts on federal operations, assets, and people" has risen from 5,503 in 2006 to 48,562 in 2012.[3]

In April 2014, the Securities and Exchange Commission (SEC) issued a risk alert in which it announced that it will conduct an initial set of examinations of more than 50 registered broker-dealers and registered investment advisers to collect information relating to cyber-security. The information gathered will include details pertaining to industry's recent experiences with cyber-security threats and the level of the industry's preparedness for cyber-attacks, including information on cyber-security insurance.[4] While currently limited to broker-dealers, it is expected that the SEC will expand its examinations to all regulated companies.5

Additionally, the Financial Industry Regulatory Authority (FINRA) announced that part of its "examination priorities" for 2015 include hiring a team of technology savvy expert examiners who will be tasked with looking into the measures that brokerage firms have in place for securing clients' data and testing the integrity of firms' technology.[6]

Regulatory pressures aside, cyber-security insurance should be getting companies' attention because cyber-security breaches can be ex-

---

2. PONEMON INSTITUTE, 2013 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS (May 2013), *available at* https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf.

3. GREGORY C. WILSHUSIN, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-462T, CYBERSECURITY: A BETTER DEFINED AND IMPLEMENTED NATIONAL STRATEGY IS NEEDED TO ADDRESS PERSISTENT CHALLENGES 2 (Mar. 7, 2013), *available at* http://www.gao.gov/assets/660/652817.pdf.

4. Office of Compliance Inspections and Examinations, *OCIE Cybersecurity Initiative*, 4 NAT'L EXAM PROGRAM RISK ALERT, Apr. 15, 2014, at 1, 4, *available at* http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

5. Daniel Garrie, *Cybersecurity Becoming Real Issue for Boards of Directors*, DAILY J. (Jun. 2, 2014), https://www.dailyjournal.com/subscriber/SubMain.cfm?shCenFileName=SEARCH&shNewsType=Search&selOption=Search&NewsId=7#section=tab3.

6. Suzanne Barlyn, *Wall Street watchdog to bolster reviews of brokerage security*, REUTERS (Oct. 29, 2014, 4:57 PM), http://www.reuters.com/article/2014/10/29/us-finra-cybersecurity-examinations-idUSKBN0II2DA20141029.

tremely costly. A 2013 study conducted by the Ponemon Institute, analyzing cyber-security breaches of 277 companies in nine countries over a ten month span in 2012, reported that the average cost per record for a data breach in the United States was $188, which was second highest to Germany.[7]

B. MAJOR CORPORATIONS ARE PAYING THE PRICE FOR INADEQUATE CYBER-SECURITY

A number of well-known multi-billion dollar companies have suffered major data breaches recently, resulting in hundreds of millions of dollars in losses. It is alarming how unprepared many of these companies were for cyber-attacks, highlighting the need for cyber-security insurance.

The following is a brief overview of the high-profile cyber-security breaches that have occurred in the last few years:

- In April of 2011, a cyber-security breach in Sony's Play Station Network cost Sony an estimated $171 million.[8]
- Between November and December 2013, Target's computer system was hacked, and credit and debit card information was stolen, in addition to the names, mailing addresses, email addresses and phone numbers of over 40 million customers.[9]

---

7. PONEMON, *supra* note 2.

8. Mark Hachman, *PlayStation Hack to Cost Sony $171M; Quake Costs Far Higher*, PC MAG. (May 23, 2011, 4:38 PM), http://www.pcmag.com/article2/0,2817,2385790,00.asp. The cyber-attack forced Sony to shut down the network for over three weeks and they confirmed that names, addresses and credit card information belonging to more than 77 million user accounts were stolen. Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS (Apr. 26, 2011, 7:36 PM), http://www.reuters.com/article/2011/04/26/us-sony-stoldendataidUSTRE73P6WB20110426. A lawsuit was brought against Sony on April 27, 2011 in Alabama, by Kristopher Johns, a Play Station user, on behalf of all Play Station users, alleging Sony "failed to encrypt data and establish adequate firewalls to handle a server intrusion contingency, failed to provide prompt and adequate warnings of security breaches, and unreasonably delayed in bringing the PSN service back online." Johns v. Sony Computer Entm't Am. LLC, No. 3:11-cvN263-EDL (N.D. Cal. Apr. 27, 2011). The complaint also alleged that Sony failed to notify members of a possible security breach and improperly stored members' credit card information. Id. Earlier this year, the court approved a settlement granting about $15 million in compensation to affected users. Mike Futter, *Court Approves Sony Settlement In 2011 PSN Data Breach Case*, GAMEINFORMER (Jul. 24, 2014, 10:50 AM), http://www.gameinformer.com/b/news/archive/2014/07/23/court-approves-sony-settlement-in-2011-data-breach-case.aspx.

9. *Data Breach FAQ*, TARGET, https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888 (last visited Sept. 24, 2014). Target reported that it lost $148 million due to the breaches and their insurance covered 25% of this cost.

- In May 2014, it was first reported that eBay suffered a data breach in which identity information, including customer names, encrypted passwords, email addresses, physical addresses, phone numbers, and dates of birth for 145 million customers was exposed and stolen.[10]
- Home Depot announced in September 2014 the results of an investigation into a cyber-attack estimated to have put payment card information at risk for 56 million payment cards.[11]
- In late November 2014, Sony Pictures was hacked, exposing a huge and wide ranging amount of sensitive information

---

Samantha Sharf, *Target Shares Tumble As Retailer Reveals Cost Of Data Breach*, FORBES (Aug. 5, 2014), http://www.forbes.com/sites/samanthasharf/2014/08/05/target-shares-tumble-as-retailer-reveals-cost-of-data-breach/. To add to the damages, Target suffered a 46% drop in profits for the 4th quarter of 2013. Maggie McGrath, *Target Profit Falls 46% On Credit Card Breach And The Hits Could Keep On Coming*, FORBES (Feb. 26, 2014), http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/. In a move to install confidence in its shareholders, customers and vendors, multiple senior officers of Target were fired or resigned, including the CEO and CIO. Elizabeth A. Harris, *Faltering Target Parts Ways With Chief*, N.Y. TIMES (May 5, 2014), http://www.nytimes.com/2014/05/06/business/target-chief-executive-resigns.html?_r=0. Additionally, the Institutional Shareholder Services called on Target shareholders to oust seven of the company's 10 directors for not doing enough to ensure Target's systems were fortified against security threats. Paul Ziobro & Joann S. Lublin, *ISS's View on Target Directors Is a Signal on Cybersecurity*, WALL ST. J. (May 28, 2014, 6:28 PM), http://online.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278.

10. Jim Finkle & Deepa Seetharaman, *Cyber Thieves Took Data on 145 Million eBay Customers by Hacking 3 Corporate Employees*, BUS. INSIDER (May 27, 2014, 6:02 AM), http://www.businessinsider.com/cyber-thieves-took-data-on-145-million-ebay-customers-by-hacking-3-corporate-employees-2014-5. The hacking of its customers' accounts was not detected for over a month. Id. In July 2014, a $5 million consumer privacy class action was filed against eBay in federal court in Louisiana, alleging that the security breach was the result of eBay's failure to properly provide cybersecurity to protect the identity information of its customers. Green v. EBay Inc., No. 2:14-cv-01688-SM-KWR (E.D. La. July 23, 2014). While the combined claims are allege massive damages, the real damages that eBay faces are reputational, including the loss of consumer confidence. The proceedings are still ongoing with eBay recently moving to dismiss the proposed class action. Jonathan Randles, *eBay Says Data Breach Lawsuit Too Speculative*, LAW360 (Oct. 1, 2014, 2:32 PM), http://www.law360.com/articles/583041/ebay-says-data-breach-lawsuit-too-speculative.

11. Gerry Smith, *Home Depot Admits 56 Million Payment Cards At Risk After Cyber-attack*, HUFF. POST (Sept. 21, 2014, 4:52 PM), http://www.huffingtonpost.com/2014/09/18/home-depot-hack_n_5845378.html. The cyber criminals used a never-before-seen custom-built malware that is believed to have gone undetected in Home Depot's system from April to September 2014. Id. While there is no evidence that debit PIN numbers were compromised, the attack is likely the largest breach of a retailer's computer system to date. *Id.*

> including employee passwords, medical information, as well as movie scripts and unreleased films.[12]

These incidents highlight how even major companies are vulnerable to cyber-attack. No company can be confident that it can escape the pitfall of a large scale data breach without adequate cyber-security and the protection of cyber-security insurance.

C. SCOPE OF COVERAGE FOR CYBER-SECURITY INCIDENTS UNDER GENERAL LIABILITY POLICIES & RECENT CASE LAW

It is important for companies to ascertain to what degree their current policies provide cyber-security coverage. Insurers are becoming increasingly willing to litigate the issue of whether commercial general liability ("CGL") policies provide insurance coverage for the theft of electronic data and harm to intangible property because the damages in such claims often do not fit cleanly into CGL policy coverage provisions.[13]

For instance, in the aftermath of the Sony data breach, Sony's insurer, Zurich American Insurance Company (Zurich), filed an action for declaratory judgment in the Supreme Court of the State of New York, seeking "declaratory relief to settle important questions concerning Sony Defendants' claims for insurance coverage relating to numerous class action lawsuits, miscellaneous claims, and potential actions …arising out of one or more of the cyber-attacks perpetrated by computer 'hackers' on the PlayStation Network."[14] Zurich asserted that they were not obligated to indemnify Sony under their CGL policy because the claims related to the data breach "do not allege injury of damages covered under Coverage A – Bodily Injury or Property Damage Liability or Coverage B – Personal and Advertising Injury Liability."[15] The court wound up ruling that Zurich was not required to indemnify

---

12. Dave Lewis, *Sony Pictures Data Breach and the PR Nightmare*, FORBES (Dec. 16, 2014, 3:00 AM), http://www.forbes.com/sites/davelewis/2014/12/16/sony-pictures-data-breach-and-the-pr-nightmare/. Former employees filed multiple lawsuits alleging inter alia that Sony was negligent in not being more prepared for the attack despite warnings and prior breaches. Ralph Ellis, *Lawsuits say Sony Pictures should have expected security breach*, CNN (Dec. 20, 2014, 10:55 PM), http://www.cnn.com/2014/12/20/us/sony-pictures-lawsuits/.

13. Angela Yu, Comment, *Let's Get Physical: Loss of Use of Tangible Property as Coverage in Cyber Insurance*, 40 Rutgers Computer & Tech. L.J. 229 (2014).

14. Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011, 2 (N.Y. Sup. Ct., Feb. 21, 2011) *available at http://ace-insurance-litigation.com/sites/default/files/Zurich%20American%20Insurance%20v.%20Sony,%20ACE%20Ltd.,%20et%20al.%20Complaint.pdf*

15. *Id*.

Sony under the provisions of the CGL policy.[16]

There is, however, some federal case law supporting coverage for cyber-security breaches under CGL policies and under the property damage provisions of some policies. The court in *Eyeblaster, Inc. v. Fed. Ins. Co*., for instance, held that the insurer was liable for litigation costs that the insured sustained in a lawsuit brought by a computer user whose computer performance was substantially impaired due to the insured's failure to protect against spyware.[17] The court found that the impaired computer performance was covered under the General Liability policy for "loss of use of tangible property that was not physically injured," even though the policy excluded coverage for "software, data or other information that was in electronic form."[18]

While the insurer in *Eyeblaster* failed to succeed with its software/electronic damage exclusion argument, it is important to be aware of these types of exclusions in CGL policies, as they are now common.[19] Provisions such as these along with the more general inapplicability of traditional CGL coverage to cyber-security breaches have given rise to a gap in coverage for cyber-risks that is only widening as businesses and individuals increasingly rely on technology.

D. CURRENT GENERAL STATE OF CYBER-SECURITY INSURANCE

As insurers are becoming increasingly reluctant to provide coverage for data breach losses under CGL policies, they are writing more and more policies specific to cyber-security, causing cyber-security insurance to become the fastest growing segment of the industry.[20] However, the unpredictable probability and costs of data breaches, among other factors, make cyber-security insurance rather expensive.[21] Premiums for cyber-security insurance totaled $1 billion in 2012 and $1.3 billion in 2013.[22] While the cost of cyber-security insurance has just recently be-

16. *Id*.

17. Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797 (8th Cir. 2010).

18. *Id* at 802.

19. *See*, *e.g*., Union Pump Co. v. Centrifugal Tech., Inc., No. 05-0287, 2009 U.S. Dist. LEXIS 86352 (W.D. La. 2009) (data breach losses not covered because electronic data losses specifically excluded from CGL policy).

20. *See* Thompson, supra note 1.

21. Russell Cameron Thomas, *Total cost of security: a method for managing risks and incentives across the extended enterprise*, *in* PROCEEDINGS OF THE 5TH ANNUAL WORKSHOP ON CYBER SEC. & INFO. INTELL. RESEARCH: CYBER SEC. & INFO. INTELL. CHALLENGES & STRATEGIES (Frederick Sheldon et al. eds., 2009), available at http://www.csiir.ornl.gov/csiirw/09/CSIIRW09-Proceedings/Abstracts/Thomas-abstract.pdf.

22. Nicole Perlroth & Elizabeth A. Harris, *Cyberattack Insurance a Challenge for Business*, N.Y. TIMES (Jun. 8, 2014), http://www.nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-

gun to go down to some degree, many businesses still consider it to be too costly.

One of the difficulties associated with the high costs of cyber-security insurance is that it can put companies in a position where they will have to choose between spending money on cyber-security insurance or investing in technology that will improve their cyber-security.[23] Should the insured purchase a cyber-security insurance policy that indemnifies it against state sanctions, administrative fines, property damage, business interruption, and consumer lawsuits arising from a data breach, it would have little incentive to devote sufficient resources to its information security infrastructure.[24]

This creates something of a lose-lose-lose scenario between (a) the parties entrusting their data to an insured; (b) the insurer; and (c) the insured itself. Those whose data are at stake are more likely to suffer from inadequate protection of their information;[25] insurers may lose money by becoming liable for unexpectedly large or frequent data breaches on those they have insured;[26] and the insured is more likely to be hacked, which, even if monetary losses are covered, can result in long term reputational damages and internal disruption for a company.[27]

More reasonably priced premiums can help improve the situation. Offering lower premiums for companies with better cyber-security would help incentivize companies to devote more resources to their cyber-security infrastructure.[28] The idea is that insurers are willing to offer reduced premiums to those seeking coverage if they take steps to decrease the likelihood or extent of the insurer's liability.[29] This type of model is common in other fields of insurance. In the context of flood insurance for instance, elevating buildings above the community's established base flood elevation will typically result in significantly lower

---

business.html?hp&_r=2.

23. Lawrence A. Gordon et al., *A framework for using insurance for cyber-risk management*, 46 COMMC'NS OF THE ACM 81 (2003).

24. Liam Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance*, 3 J. L. & CYBER WARFARE 1 (2014).

25. *Id*.

26. See Danny Bradbury, *Insuring Against Data Breaches*, 2013 COMPUTER FRAUD AND SEC., Feb. 2013, at 11.

27. This case discusses Target's recent data breach. *See* McGrath, *supra* note 15 ("'significant' internal distraction is the biggest consequence of a breach like Target's."); Sital Patel, *Data Breach is Not Real Reason for Target's Profit Warning*, MARKETWATCH (Aug. 2, 2014, 1:52 PM), http://blogs.marketwatch.com/behindthestorefront/2014/08/05/target-data-breach-is-distracting-it-from-its-core-mission-selling-stuff/.

28. Zichao Yang & John Lui, *Security adoption in heterogeneous networks: the influence of cyber-insurance market*, *in* NETWORKING 2012, 172 (Robert Bestak et al. eds., 2012).

29. See Bailey, *supra* note 24, at 7.

flood insurance premiums for the building.[30]

Differentiated premiums that correspond to the quality of the insured's information security infrastructure do exist to some degree in the cyber insurance market,[31] but are not standard, resulting in an inefficient marketplace.[32] The difficulty with applying a differentiated premium model to the field of cyber insurance is that it can be difficult to assess what the actual risks are for a given company.[33] There is often an information asymmetry between insurer and insured because the insurer typically does not have the resources to monitor an insured's actions that may affect risks for which the insurer is liable.[34] This can include "vital information regarding applications, software products installed by Internet users, and security maintenance habits, which correlate to the risk types of users."[35]

Adequately pricing premiums also requires a thorough understanding of cyber incident loss data, which is generally lacking because companies are often reluctant to make public their experiences with cybersecurity breaches.[36] Many times the companies themselves are not even aware of breaches in their systems. As a result, it is difficult for insurers to know the actual frequency and extent of cyber-breaches that have taken place among potential insurance purchasers. This lack of information concerning cyber-threats makes it even more difficult for an insurer to assess the strength of a company's cyber-security infrastructure and offer correspondingly priced premiums.

More broadly, cyber-threats remain a relatively new phenomenon that is always changing.[37] Even with reliable information sharing, insurers would not have all that much data to use in evaluating cyber-

---

30. FED. EMERGENCY MGMT. AGENCY, D671, CHEAPER FLOOD INSURANCE; 5 WAYS TO LOWER THE COST OF YOUR FLOOD INSURANCE (Oct. 1, 2007), *available at* http://www.fema.gov/media-library-data/20130726-1622-20490-2266/fema_d671.pdf.

31. *Allianz Cyber Protect*, ALLIANZ, http://www.agcs.allianz.com/services/financial-lines/allianz-cyber-protect/ (last visited Feb. 12, 2015).

32. Ranjan Pal et al., Realizing Efficient Cyber-Insurance Markets The Problem of Ensuring Positive Insurer Profits (2013), *available at* http://www-scf.usc.edu/~rpal/CYBERMR.pdf (unpublished manuscript) (on file with author at Personal Web Pages, Univ. Southern Cal.)

33. Bailey, *supra* note 24, at 22-23.

34. *Id*.

35. Ranjan Pal, *Cyber-Insurance in Internet Security: A Dig Into the Information Asymmetry Problem*, ARXIV 2 (Feb. 4, 2012), http://arxiv.org/pdf/1202.0884v1.pdf.

36. BRIAN CASHELL ET AL., CONG. RESEARCH SERV., RL32331, THE ECONOMIC IMPACT OF CYBER-ATTACKS 2 (2004), available at https://fas.org/sgp/crs/misc/RL32331.pdf.

37. *See generally* Michael Gervais, *Cyber Attacks and the Laws of War*, 1 J.L. & CYBER WARFARE 8 (2012) (discussing the challenges in categorizing various cyber-attacks under current law and determining what the nature of a given cyber-threat truly is, e.g. state actor versus non-state actor); Smith, *supra* note 11 (illustrating how an entirely new form of malware was used in the Home Depot breach).

risks compared to something like floods, which have been happening for considerably longer. Moreover, even the data that insurers do have could become obsolete overnight. The state of cybercrime is constantly in flux as new technologies are rapidly developing and hackers are becoming more sophisticated.[38]

With time more data is likely to become available for insurers to assess cyber-risk more accurately and we may see differentiated premiums become standard in the near future.[39] Already technologies are being developed to help insurers become more informed about cyber risks.[40] Yet, it remains important to be careful while navigating the cyber-security insurance market and proceed with the most up to date information as possible.

III. OBTAINING COVERAGE

A. CYBER-SECURITY THREATS/ACTORS THAT COMPANIES SHOULD UNDERSTAND

In order to obtain an appropriate cyber-security insurance policy, companies need to be aware of the actors who pose a threat to companies' cyber capabilities as well as the tools and vectors by which these actors can effectuate cyber-attacks.

Potential threat actors include a wide variety of characters such as state actors, hacktivists, cyber terrorists, and cyber criminals.[41] One of the many difficulties with this type of threat, however, is determining who is responsible for any given attack. Some investigations into cyber-attacks have gone on for years with little progress made on attribution.[42] The consequences of this can be dangerous if investigators jump to conclusions, as attacks perpetrated by independent actors can be disguised so that they appear to have been perpetrated by state actors.[43]

Employees can also be threat actors as either negligent or rogue employees. Negligent employees are one of the top causes of data breaches.[44] Relatively simple mistakes such as sending out incorrect da-

---

38. Chris Colvin et al., *Cyber Warfare and the Corporate Environment*, 2 J.L. & CYBER WARFARE 1, 3-4 (2013).

39. Bailey, *supra* note 24, at 5 (proposing a cyber-risk information sharing platform for insurers).

40. Mike Lennon, *New FireEye Services Help Insurance Industry Manage Exposure to Cyber Threat*s, SEC. WEEK Aug. 7, 2014, http://www.securityweek.com/new-fireeye-services-help-insurance-industry-manage-exposure-cyber-threats.

41. Gervais, *supra* note 37, at 41-43; Colvin, *supra* note 38.

42. Kenneth Geers, *The Cyber-Threat to National Critical Infrastructures*: *Beyond Theory*, 18 INFO. SEC. J.: A GLOBAL PERSPECTIVE 1 (2009).

43. *See* Gervais, *supra* note 37, at 39-49.

44. *Employee Negligence Cited as Leading Cause of Company Data Breaches*,

ta, losing or inappropriately using hardware, or becoming a victim of phishing have resulted in major cyber-security breaches.[45] Rogue employees can also be dangerous threat actors as they are often in a position to easily steal data and hardware, commit extortion, or sell data to a third party.[46]

The tools threat actors use are diverse and not necessarily limited to cyberspace. Prominent among them are the many varieties of malware that exist and continue to be developed, including spyware (software with spying capabilities such as user activity monitoring, collecting keystrokes and data harvesting) and ransomware (software that lures its victim to a web site and then locks the user's computer until user makes a payment).[47] A common method of cyber-breach is pin skimming, in which a counterfeit card reader placed over an ATM's card slot is used to steal personal information stored on debit card that are swiped.[48] Breaches can also take place by less technological means through social engineering (also referred to as phishing, whaling, pretexting, or baiting). With these methods, threat actors manipulate individuals with access to a targeted system into performing actions or divulging confidential information.[49]

ARRAYA (Oct. 2, 2014), blog.arrayasolutions.com/?p=362.

45. *Id*.

46. Carl Colwill, *Human Factors in Information Security: The Insider Threat–Who can you Trust these Days?*, 14 INFO. SEC. TECHNICAL REP. 175, 186 (Nov. 2009).

47. Nate Lord, *Common Malware Types: Cybersecurity 101*, VERACODE (Oct. 12, 2012), https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101. Some other types of malware are Trojan horses (malware that disguises itself as a normal file or program to trick users into downloading and installing malware, often allowing remote access to the infected computer), viruses (malware that is capable of copying itself and spreading to other computers in order to steal information, harm host computers and networks, create botnets, steal money, render advertisements, etc.), rootkits (malware designed to remotely access or control a computer without being detected by users or security programs), and worms (which can be thought of as a type of virus with the ability to self-replicate and spread independently that typically causes harm to host networks by consuming bandwidth and overloading web servers). *Id.*

48. *Debit and Credit Card Skimming*, PRIVACY SENSE, http://www.privacysense.net/debit-and-credit-card-skimming/ (last visited Nov. 7, 2014). A fraudster attempting to gain access to a debit account will also need the PIN number, which is obtained either through someone "shoulder surfing" to observe the code as it is entered by the cardholder or through the use of hidden cameras. *Id.* Skimming devices are readily available on the Internet from websites such as eBay for as little as $50. *Id.* These devices are usually disguised under the name of a "card reader" because they can also serve legitimate purposes. *Id.*

49. Linda Criddle, *What Is Social Engineering?*, WEBROOT http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering (last visited Nov. 7, 2014). A common form of social engineering attack is to gain access to someone's email account and use it to email the person's friends, often creating a compelling story in order to induce them to send money or exploiting their trust and curiosity by including links or downloads with malware embedded. *Id.*

Threat vectors are the paths used by the threat actor to infiltrate companies' data systems.[50] They include supply chain vulnerabilities, wireless access points, and removable media.[51] The scope and quantity of threat vectors is increasing as more and more companies are instituting Bring Your Own Device (BYOD) policies in which employees can access company data via mobile devices.[52] It is crucial to exercise caution in implementing BYOD policies and it is recommended that such policies require employees to install malware detection software on their mobile devices.[53]

Understanding how threat actors can penetrate a company's information security system is crucial to assessing where a company's cyber vulnerabilities lie and obtaining the appropriate cyber-security coverage.

B. TYPES OF COVERAGE

At this point, virtually all of the major insurers offer cyber-security insurance including, among others, Marsh McLennan,[54] Allianze,[55]

Fraudsters will also attempt to induce similar kinds of actions from their targets by using e-mails, IMs, comments, or text messages that appear to come from a legitimate, popular company, bank, school, or institution. *Id.*

50. *Attack Vectors*, HAPPY TRAILS COMPUTER CLUB, http://cybercoyote.org/security/av-top.htm (last visited Nov. 7, 2014). Threat vectors are not to be confused with payloads. A payload is the malicious code carried by or through the threat vector. *Id.* The distinction between the threat vector and the payload actually affecting a target device can be fine at times. A virus is often the threat vector as well as the payload. *Id.* A worm is always a threat vector and could carry a virus as the payload. Id. Trojan horses and spyware are examples of payloads. *Id.*

51. *See* MELINDA REED ET AL., OFF. ASSISTANT SEC'Y DEF. FOR RESEARCH & ENG'G, DEP'T DEF., SUPPLY CHAIN ATTACK PATTERNS: FRAMEWORK AND CATALOG 2, 21 (Aug. 2014), available at http://www.acq.osd.mil/se/docs/Supply-Chain-WP.pdf; Steven R. Chabinsky, *Cybersecurity strategy: A primer for policy makers and those on the front line*, 4 J. NAT'L SEC. L. & POL'Y 27 (2010). Email remains a major threat vector as well. A recent study found that 61 percent of energy firms view email as the biggest threat vector for cyber-attacks via malware. Karen Boman, *Energy Companies See Email*, *Hacktivists as Major Cybersecurity Threats*, RIGZONE (May 16, 2014), http://www.rigzone.com/news/oil_gas/a/133130/Energy_Companies_See_Email_Hacktivists_as_Major_Cybersecurity_Threats#sthash.qrAWL7HY.dpuf.

52. Daniel B. Garrie, *The BYOD Dilemma: How to Keep Your Assets from Turning Into Liabilities*, REUTERS (Feb. 14, 2014), http://blog.legalsolutions.thomsonreuters.com/wp-content/uploads//2014/02/BYOD-white-paper.pdf.

53. *Id.*

54. *Cyber Risk*, MARSH, http://usa.marsh.com/RiskIssues/CyberRisk.aspx (last visited Nov. 7, 2014).

55. ALLIANZ, *supra* note 31 ("Our customers can opt for the standard of cyber protection that corresponds to their risk profile.").

AIG,[56] Apogee Insurance Group,[57] AXA,[58] Howden Broking Group,[59] and Chubb.[60] Cyber-security insurance can come in many forms.

The various types of coverage offered under cyber-security insurance policies include coverage for:

- Data breach/privacy crisis management: expenses related to the management of a cyber-security incident, including the investigation, remediation, data subject notification, call management, credit checking for data subjects, legal costs, court attendance and regulatory fines.
- Business/Network Interruption: loss of net profit that was caused by a material interruption to the insured's network, due to a cyber-attack or a network security breach.
- Multimedia/Media liability: third-party damages which can include defacement of a website, infringement of intellectual property rights or negligence relating to electronic content.
- Extortion liability: losses due to a threat of extortion and professional fees related to terminating an external threat.
- Network security liability: third-party damages resulting from denial of access to a system, costs related to data stored with third-party suppliers and costs related to the theft of data on third-party systems.
- Reputational Injury: third-party damages from disparagement or privacy violations caused by breach of the insured's system.
- Conduit Injury: damages to customers' systems affected by breach of the insured's system.
- Disclosure Injury: damages to individuals caused by the unauthorized access of their private information held on the

---

56. *End-to-End Cyber Risk Management Solutions*, AIG, http://www.aig.com/_1247_412514.html (last visited Nov. 7, 2014).

57. *Security and Privacy (Cyber Liability) Insurance*, APOGEE INS. GROUP, http://www.apogeeinsgroup.com/SecurityAndPrivacy-CyberLiability.html (last visited Nov. 7, 2014).

58. *Cyber Sphere and Cyber@Risk: Protecting Businesses Against Cyber Risks*, CORPORATE SOLUTIONS, http://www.axa-corporatesolutions.com/Cyber-risks-wake-up-call-for.html?lang=fr (last visited Nov. 7, 2014) ("Combining technical vulnerabilities analysis and the management of cyber risks within a single approach, Cyber@Risk allows risk managers and cyber security managers to visualize the levels of exposure and set mitigation priorities.").

59. *Cyber Liability Cover*, HOWDEN GROUP, http://www.howdengroup.com/brochures/cyber-liability-july-13.pdf (last visited Nov. 7, 2014) ("The policy Howden Windsor offers starts from as little as £300 per annum (excluding Insurance Premium Tax) for a £1,000,000 limit with a £500 excess.").

60. *Cybersecurity by Chubb*, CHUBB GROUP, http://www.chubb.com/businesses/csi/chubb822.html (last visited Nov. 7, 2014).

insured's system.

Most major insurers even offer special cyber-security products to cater to a company's specific cyber-security needs.[61] For example, AIG offers cyber-security insurance through a product called Cyber Edge. Cyber Edge offers coverage for data liability, which includes personal data, corporate data, outsourcing and network security with optional coverage for Business/Network Interruption, Multimedia Liability, and Cyber/Privacy Extortion.[62] The product additionally offers crisis management for a data breach, including public relations advice, and has a response team available 24/7 in the event of a cyber-security breach.[63] Following the occurrence of a security breach or data leak, Cyber Edge will provide data restoration, recollection and recreation services.[64]

IV. CONCLUSION

Obtaining cyber-security insurance coverage is an important part of a company's overall cyber-security plan and companies should consult with legal counsel to most effectively meet their overall goals. While cyber-security policies currently available may be expensive and limited to some degree, numerous coverage options remain accessible. In obtaining a suitable cyber-security insurance policy, it is important for a company to understand many important factors including the language of their current policies, the current state of the market, relevant risks which need to be insured, and the types of coverage available.

An experienced attorney in the cyber-security field can help guide a global company in navigating the broad options for cyber-security policies available and obtain a policy that addresses the company's risks and needs.

---

61. *See supra* notes 53-59.
62. AIG, *supra* note 56.
63. *Id.*
64. *Id.*