Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches

Lance Bonner*

I. INTRODUCTION

In 2011, a number of high profile data breaches made national news.[1] Companies such as Epsilon Data Management and Nasdaq experienced data breaches that posed serious risks to their business operations.[2] Total data loss incidents numbered in the hundreds, and multiple incidents involved millions of records.[3]

Large amounts of information have been involved in some of the most recent data breaches. Epsilon, the target of a data breach in April 2011, sends forty billion marketing emails on behalf of its business clients each year, and its clients include two of the largest banks in the United States.[4] As a result of the breach, more than forty of Epsilon's clients, including TD Ameritrade, Eddie Bauer, and

* J.D. Candidate (2013), Washington University School of Law; B.A. (2010), University of Pittsburgh. I thank my fiancée, Sam Miller, for her unwavering love and support throughout all of law school. I would also like to thank my family, especially my sister, Blair, and my mother, Gail, for giving me inspiration to push forward. Lastly, I want to thank Tom Mielenhausen for helping me develop the idea for this Note. I dedicate this Note to the fond memory of my late father, T.S. Bonner.

1. *See, e.g.*, Matthew J. Schwartz, *Six Worst Data Breaches of 2011*, INFORMATION WEEK (Dec. 28, 2011, 9:05 AM), http://www.informationweek.com/news/security/attacks/232301079. According to at least one source, four of the top ten largest data breaches ever recorded occurred in 2011. *Largest Data Loss Incidents*, DATALOSSDB, http://datalossdb.org/index/largest (last visited Sept. 9, 2012) (citing the breaches of Sony Corporation, Tianya, SK Communications, and Valve, Inc.).

2. Schwartz, *supra* note 1.

3. *See* DATALOSSDB, http://datalossdb.org/.

4. Lisa Greim, *Breached E-Mail Marketer Sends Billions of E-Mails A Year*, PCWORLD (Apr. 5, 2011, 4:45 PM), http://www.pcworld.com/article/224373/breached_email_marketer_sends_billions_of_emails_a_year.html.

Ethan Allen, contacted their customers to inform them their personal information might be at risk.[5]

Of all the data breaches in 2011, the string of data breaches that plagued Sony Corporation were arguably the most high profile.[6] Sony made headlines for breaches of its Playstation Network and Qiocity services in April as hackers accessed Sony's clients' personal information.[7]

As news spread of the mounting data breaches hitting Sony, an ancillary issue involving Sony's insurance coverage surfaced.[8] Zurich American Insurance Company, one of Sony's insurers, filed suit in New York state court asking the court for a release from any duty to defend or indemnify Sony as to claims surrounding the data breaches.[9] The suit brought to light the growing realization among businesses that traditional commercial liability policies will not cover damages and other costs incurred as a result of a data breach.[10] To fill the void of coverage under traditional commercial liability policies, insurance companies are now offering alternative specialty products, often referred to as "cyber risk" policies.[11]

The Sony data breaches and other data privacy issues have inspired a renewed and forceful discussion among privacy advocates,[12] practitioners,[13] and politicians[14] on what role government

5. *Id.* Epsilon's customers include TiVo, Capital One, US Bank, JPMorgan Chase, Citi, Home Shopping Network, Ameriprise Financial, McKinsey & Company, Ritz-Carlton Rewards, Marriott Rewards, Walgreens, Best Buy, and Robert Half Technologies. Jared Newman, *Epsilon E-Mail Hack: What You Need to Know*, PCWORLD (Apr. 4, 2011, 1:35 PM), http://www.pcworld.com/article/224213/epsilon_email_hack_what_you_need_to_know.html.

6. One source counts as many as twenty-one digital attacks against Sony in 2011. *A Concise History of Sony Attacks*, ATTRITION.ORG (June 4, 2011, 4:17 AM), http://attrition.org/security/rant/sony_aka_sownage.html.

7. Bryan Petrilla, *"Anonymous" Hacks Sony PlayStation Network: The Increasing Importance of Obtaining Cybersecurity Insurance Coverage*, MONDAQ BLOG (May 12, 2011), *available at* 2011 WLNR 9433823.

8. Jaikumar Vijayan, *Zurich Lawsuit Against Sony Highlights Cyber Insurance Shortcomings*, COMPUTERWORLD (July 26, 2011 6:00 AM), http://www.computerworld.com/s/article/9218639/Zurich_lawsuit_against_Sony_highlights_cyber_insurance_shortcomings.

9. *Id.*

10. *Id.*

11. Scott Godes, *Cybersecurity Risks and Insurance Coverage*, *in* 3–18 NEW APPLEMAN LAW OF LIABILITY INSURANCE § 18.03 (Matthew Bender 2011).

12. *See, e.g.*, *Data Breaches: A Year in Review*, PRIVACY RIGHTS CLEARINGHOUSE (Dec. 16, 2011), https://www.privacyrights.org/data-breach-year-review-2011.

13. Stephen J. Rancourt, Articles, *Hacking, Theft, and Corporate Negligence: Making the*

should play in regulating how companies and organizations protect data. At least some observers believe insurance should play some role in this discussion.[15] Part II of this Note will review the Sony data breach to highlight the growing risks to businesses and organizations in storing electronic data, and the current and proposed governmental response. Part III will discuss why the inadequacy of traditional general commercial liability insurance policies in covering claims related to data storage has made new cyber risk insurance policies necessary for entities subject to cyber risk. Lastly, Part IV will call for governmental action in facilitating the expansion of cyber risk policies through incentives and infrastructure building to solve the coverage gap plaguing U.S. businesses and organizations.

II. DATA BREACHES

A. A Cyber Catastrophe

In late April of 2011, Sony, Inc. shut down its online PlayStation Network (PSN) in response to a data security breach.[16] Over seventy-seven million users use the network in countries across the globe, and it is an integral part of Sony's video game system.[17] For almost a week, Sony failed to inform PSN users as to the reason for the network shutdown.[18] A message was subsequently posted on Sony's

Case for Mandatory Encryption of Personal Information, 18 TEX. WESLEYAN L. REV. 183, 186 (2011) (calling for federal regulation to "incentivize the proper storage and transmission of personal data").

14. *See, e.g.*, Juliana Gruenwald, *Lawmakers Say Sony Data Breach Underscores Need for Legislation*, NAT'L J. (Apr. 27, 2011, 4:34 PM), http://techdailydose.nationaljournal.com/2011/04/lawmakers-say-sony-data-breach.php.

15. *See, e.g.*, Rancourt, *supra* note 13, at 214–15.

16. PRIVACY RIGHTS CLEARINGHOUSE, *supra* note 12. The network includes an online store that users can access through their PlayStation® 3 consoles allowing them to purchase games, movies, and various entertainment products. *PlayStation® Network*, PLAYSTATION, http://us.playstation.com/psn/ (last visited Sept. 9, 2012).

17. Petrilla, *supra* note 7. One of the network's games, "Call of Duty: Black Ops," quickly made over $1 billion. *Id.* The game features online multiplayer capability that pits player against player in real time, commanding soldiers outfitted with various guns. *Call of Duty: Black Ops*, CALL OF DUTY, http://www.callofduty.com/blackops/game (last visited Sept. 9, 2012).

18. Nick Bilton, *Sony Defends Security Actions*, N.Y. TIMES, May 23, 2011, at B4, *available at* 2011 WLNR 10233618.

website stating that the company suspected unidentified individuals had stolen PSN users' personal information.[19] Stolen data included names, home addresses, e-mail addresses, birth dates, network passwords and login information.[20] A later e-mail sent to all PSN users revealed that Sony suspected credit card information had also been obtained.[21] Sony kept the PSN down for almost a month until the network resumed on May 14, 2011.[22]

Sony was highly criticized for waiting a week to inform customers of the reason for the network shutdown.[23] Some observers took the opportunity to draw unfavorable comparisons to some of Sony's biggest competitors such as Apple and Microsoft.[24] After another attack in June, one security expert even referred to Sony as the "whipping boy of the computer underground."[25] The data breach also prompted members of Congress to call for private and public reforms in standards for protecting online personal information.[26] With

19. Petrilla, *supra* note 7.

20. *Id*.

21. Seth Schiesel, *PlayStation Security Breach a Test of Consumers' Trust*, N.Y. TIMES, Apr. 28, 2011, at C3, *available at* 2011 WLNR 8221249.

22. Bilton, *supra* note 18, at B4.

23. *Id*.

24. Schiesel, *supra* note 21, at C3. As the author observes:

> Can anyone imagine Microsoft allowing hackers to ravish its network or Apple allowing crooks to steal tens of millions of customers' intimate information on iTunes and then having to hire an outside company to figure out what happened?

Id.

25. *Sony Slammed over New Data Breach*, CBC NEWS (June 3, 2011), http://www.cbc.ca/news/world/story/2011/06/03/sony-2nd-data-breach.html.

26. *See, e.g.*, *Blumenthal Calls for DOJ Investigation of Sony PlayStation Data Breach*, FEDERAL INFORMATION & NEWS DISPATCH (Apr. 28, 2011), *available at* 2011 WLNR 8346908. In a letter to Attorney General Eric Holder, Senator Richard Blumenthal, a Democrat from Connecticut, criticized Sony and the handling of the breach:

> I am especially concerned about Sony's failure to promptly notify its customers about the breach and what data may have been compromised. . . .
>
> . . . .This week-long delay in disclosing a possible breach of financial information is unacceptable, and left consumers highly vulnerable . . . . Any investigation of this matter should include a thorough inquiry into whether Sony's handling of events in the wake of its security breach gives rise to civil or criminal liability. If it does not, I would welcome comments from the Justice Department regarding how the law can be updated to best hold companies accountable for inadequate protection of personal consumer information, and inadequate notification when breaches occur.

Id.

mounting criticism over the lack of data security and poor financial performance, Sony cut its Chairman's salary and bonus by 15 percent.[27]

According to one observer, Sony's exposure as a result of the breach could reach into the tens of billions of dollars.[28] Costs include an identity theft protection policy for PSN users and an ongoing electronic forensics exam and investigation.[29] Sony also faces mounting liability from class action lawsuits accusing Sony of negligence and breach of privacy.[30]

With such extremely high costs, Sony is understandably seeking coverage from its insurers.[31] With at least one insurer, Sony has faced substantial challenges in seeking coverage for many of its losses.[32] Zurich American Insurance Company (Zurich) petitioned a New York state court to find that Zurich does not have a duty to defend Sony in the increasing number of lawsuits filed against Sony in the wake of the breach.[33] Zurich also joined other Sony insurers in the suit so that the court can clarify their respective responsibilities.[34] The lawsuit claims Sony has a commercial general liability (CGL) policy with Zurich that does not cover cyber-related third-party claims.[35]

The challenges Sony faces in seeking coverage for cyber-related losses are a telling sign of the new landscape of cyber-related liability as it relates to insurance coverage.[36] Sony will most likely have a difficult time getting coverage under its CGL policy for most

---

27. *Sony Cuts Howard Stringer's Pay Package as Chairman by 15%*, N.Y. TIMES, June 29, 2011, at B8, *available at* 2011 WLNR 12898643.

28. Petrilla, *supra* note 7.

29. Lori Chordas, *Sony to Offer $1M Insurance Policies to US Gamers Impacted by Massive Cyber Breach*, BESTWIRE SERVICES (May 11, 2011), *available at* http://fpn.advisen.com/articles/article144465919972383322.html.

30. Petrilla, *supra* note 7. As of July 21, 2011, a reported fifty-five class-action suits had been filed against Sony in the United States. *Sony Insurer Sues to Deny Data Breach Coverage*, 21 NO. 42 WESTLAW J. INS. COVERAGE 1, July 29, 2011, *available at* 2011 WL 3236597.

31. Patricia Vowinkel, *A Carrier Draws a Line in the Sand: Zurich Tries to Delineate Where CGL Policies End and Network Security Risk Policies Begin*, RISK & INS. (Aug. 1, 2011), http://www.riskandinsurance.com/story.jsp?storyId=533340443&topic=Main.

32. *Id.*

33. *Zurich Asks Court to Vacate Sony Claims*, RISK & INS. (Sept. 1, 2011), http://www.riskandinsurance.com/story.jsp?storyId=533340682.

34. *Id.* Sony's insurers also include Mitsui Sumitomo Insurance, AIG, and ACE Ltd. *Id.*

35. Vowinkel, *supra* note 31.

36. *See, e.g.*, *id.*

expenses associated with the data breach.[37] Companies seeking to protect against cyber risks must now seek cyber risk-related insurance policies, which have become increasingly available over the past decade.[38]

B. The Rising Storm

Although unprecedented in the amount of information stolen and the prominence of the company, Sony is not the first to experience a major security breach. Around 2000, academic commentators and practicing risk professionals began to recognize the significant liability risks that the movement towards electronic data storage and Internet business posed to companies and organizations.[39] Over a decade ago, businesses were confronting "information theft, insertion of malicious codes, denial of service attacks, access violations, failure of computer security, programming errors, and misuse or misappropriation of intangible assets."[40] In the late 1990s, some estimates put business costs related to computer security breaches in the hundreds of billions of dollars.[41]

In 2000, the Love Bug virus circulated, causing estimated damages upwards of $15 billion to business, individuals, and governments across the globe.[42] Damages as a result of electronic security breaches have not slowed since. Over the past few years, cyber criminals have infiltrated data networks at major companies including TJ Maxx/Marshalls, Barnes & Noble, Bank of America and

37. *See* discussion *infra* Part III.A.

38. *See* discussion *infra* Part III.B.

39. *See, e.g.*, Hazel Glenn Beh, *Physical Losses in Cyberspace*, 8 CONN. INS. L.J. 55 (2002).

40. *Id.* at 58–59 (citations omitted).

41. *Id.* at 58 n.12.

42. *Id*. at 60. *See also* Charles Piller & Greg Miller, *Fast-Moving Virus Hits Computers Worldwide*, L.A. TIMES, May 5, 2000, *available at* http://articles.latimes.com/print/2000/may/05/news/mn-26739. The Love Bug spread through e-mails and destroyed files once opened on computers. *Id*. The virus would then replace destroyed files with new files that would further spread the virus when the new file was opened. *Id.* Companies affected included AT&T Corp., Microsoft Corp., Time Warner Inc., Southern California Edison Co., Merrill Lynch & Co., and Ford Motor Co. *Id*. The Pentagon, CIA, NASA, and British House of Commons were also hit. *Id*.

Wells Fargo.[43] At least one of these data breaches went undiscovered for almost two years, and some most likely have never been discovered.[44] In 2008, the Department of Justice recorded a 47 percent increase in reported data breaches from the previous year.[45]

Despite large numbers of data breaches over the past decade, 2011 saw a number of high-profile incidents make headlines and ignite public discussion. Citigroup,[46] Heartland Payment Systems,[47] RSA Security Division of the EMC Corporation, and Lockheed Martin[48] are just a few of the companies that made headlines for major data security breaches. Some of these breaches involved interrelated cyber criminal activity and greatly impacted existing business relationships.[49]

Companies face an array of costs as a result of a data breach.[50] Along with any costs associated with fixing security insufficiencies that led to the data breach, companies must often expend money contacting customers, offering and paying for the services of credit reporting agencies, any costs in assisting law enforcement, business disruption expenditures, and litigation expenses.[51] The aftermath of the Sony data breach is a threatening example of the damage to institutional goodwill that is possible as a result of a data breach.[52]

---

43. John Winn & Kevin Govern, *Identity Theft: Risks and Challenges to Business of Data Compromise*, 28 TEMP. ENVTL. L. & TECH. J. 49, 50 (2009).

44. *Id*. at 51.

45. *Id*. at 50.

46. *See* Eric Dash et al., *Citi Data Theft Points Up a Nagging Problem*, N.Y. TIMES, June 10, 2011, at B1, *available at* 2011 WLNR 11587410. Hackers reportedly stole personal information from over 200,000 credit card holders. *Id*.

47. *See id.*

48. Christopher Drew, *Stolen Data is Tracked to Hacking at Lockheed*, N.Y. TIMES, June 4, 2011, at B1, *available at* 2011 WLNR 11167661.

49. *Id*. Lockheed determined that the breach of its network was made possible through the use of data stolen from the RSA Security Division of the EMC Corporation. *Id*.

50. Winn & Govern, *supra* note 43, at 52.

51. *Id*.

52. *See supra* Part II.A.

C. A Crime for the New Millennium

A "data breach" is the unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information.[53] As was the case with the security breach of Sony's PSN, data breaches may be achieved through "hacking."[54] The most traditional form of hacking involves electronically stealing commercially valuable data that can be sold or used for profit.[55] Hacking is broadly defined as "attempts to intentionally access or harm information assets without (or in excess of) authorization by thwarting logical security mechanisms."[56]

Traditionally, hacking was only for determined individuals with extensive computer programming abilities.[57] Now, hacking can be achieved through the use of reasonably accessible programming tools.[58] A recent trend in hacking is the use of "botnets."[59] Botnets

---

53. Kimberly Kiefer Peretti, *Data Breach: What the Underground World of "Carding" Reveals*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 375, 377 (2009).

54. *See* discussion *supra* Part II.A.

55. *See* Douglas Wood, *The Four Horsemen of the Apocalypse, Class of 2011: Recreational Hacking*, CORPORATE COUNSEL (Aug. 11, 2011), http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202510773996.

56. *2011 Data Breach Investigation Report*, VERIZON, http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.

57. *See* Rizgar Mohammed Kadir, *The Scope and the Nature of Computer Crimes Statutes—A Critical Comparative Study*, 11 GERMAN L.J. 609, 618 (2010) ("In the earlier days of the computer and prior to the internet, insider computer crimes predominated and perpetrators were generally computer specialists: programmers, computer operators, data entry personnel, systems analysts, and computer managers. The advent of the Internet, however, soon made it possible to commit such crimes from outside a victimized computer.") (citation omitted).

58. *See, e.g.*, Kelly Jackson Higgins, *New Firefox Plug-In offers WiFi Cookie-Jacking For 'Average Joe'*, SECURITY DARK READING (Oct. 25, 2010, 4:40 PM), http://www.darkreading.com/security/news/227900742/new-firefox-plug-in-offers-wifi-cookie-jacking-for-average-joe.html. Firefox, an Internet browser, has a plug-in that makes "it possible for the average Joe to hijack a WiFi user's Facebook, Twitter, or other unsecured account session" without much difficulty. *Id.*

59. *See, e.g.*, Press Release, U.S. Dep't of Justice, *Another Pleads Guilty in BotNet Hacking Conspiracy*, June 10, 2010, *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2010.html. *See also* Riva Richmond, *U.S. Dismantles Large Network Of PCs Infected by Criminals*, N.Y. TIMES, Apr. 15, 2011, at B2, *available at* 2011 WLNR 7356153; Byron Acohido, *An Invitation to Crime: How a Friendly Click Can Compromise a Company*, U.S.A. TODAY, Mar. 4, 2010, at 1A, *available at* 2010 WLNR 4482026. Botnets involve infecting a computer, which "gets slotted into a network of thousands of other bots. These 'botnets' then are directed to execute all forms of cybercrime, from petty scams to cyberespionage." *Id.*

have been used to hack into and control computers as well as extract data from user databases.[60] Large and small companies have been vulnerable to botnets, and at least one botnet was created to target international businesses for the purpose of stealing business secrets.[61]

"Recreational hacking" is another example of the evolving landscape of cyber risk and data breaches.[62] Recreational hacking involves "hacking for the simple purpose of shutting down corporate sites not for pecuniary gain, but because of ideological or otherwise selfish views . . ."[63] Recreational hackers have started forming associations that hack under a common name, many of which have been responsible for the data breaches over the past few years.[64] These online organizations include groups like Anonymous and LulzSec.[65]

Originally formed in opposition to the Church of Scientology, Anonymous has recently taken up international political causes and defended WikiLeaks with attacks on MasterCard and PayPal.[66] LulzSec, the group purportedly responsible for the Sony attack, has operated under motivations that are not as clearly defined.[67]

---

60. Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer On Cybercrimes in the United States and Efforts to Combat Cybercriminals*, 16 VA. J.L. & TECH 116, 132–33 (2011).

61. *Id.*

62. Wood, *supra* note 55.

63. *Id.*

64. *Id.*

65. Riva Richmond & Nick Bilton, *Saying It's Disbanding, Hacker Group Urges New Cyberattacks*, N.Y. TIMES, June 27, 2011, at B1, *available at* 2011 WLNR 12745202.

66. *Id.*

67. *Id.* Although LulzSec has disbanded, security experts believe attacks are unlikely to decrease against websites. In declaring its dissolution, LulzSec encouraged other hackers to continue attacks on governments and corporations. *Id. See also* Jerry Brito, *'We Do It For The Lulz': What Makes LulzSec Tick?*, TIME: TECHLAND, June 17, 2011, *available at* http://techland.time.com/2011/06/17/we-do-it-for-the-lulz-what-makes-lulzsec-tick/ (stating that LulzSec does not seem to be motivated by money and members do not appear to be state-sponsored spies). LulzSec's motivations could be described as anarchistic, existentialist, or nihilistic. *Id.* The group's press releases, Twitter account, and website have often featured less than serious messages. *Id*. However, they also appear to have occasionally operated under some political motivations. *See* Adam Martin, *Highlights of What's Been Found In LulzSec's Arizona Documents*, ATLANTIC WIRE, June 24, 2011, *available at* http://www.theatlanticwire.com/national/2011/06/highlights-whats-been-found-lulzsecs-arizona-documents/39244/ (describing LulzSec's attack on Arizona law enforcement in retaliation for Arizona immigration policies).

Most data breaches are a result of external actors such as hackers.[68] However, hacking is not the only source of data breaches.[69] Other sources include malware,[70] social attacks,[71] misuse,[72] physical action,[73] and error.[74] Cyber espionage is also posing a looming threat to businesses.[75]

Cyber criminals are often after data that includes contact information, birth dates, medical data, social security numbers, passport numbers, bank information, and credit card information.[76] Loss of information can result in various negative effects for consumers, including identity theft,[77] loss to credit and reputation, emotional distress, out-of-pocket expenses, and lost opportunities.[78]

D. Current Cyber-Security Related Legislation

Consumers subject to personal data exposure have had a hard time seeking remedies in U.S. courts against businesses that have been the

68. VERIZON, *supra* note 56, at 26, 31.

69. *Id.* at 24–42.

70. *Id*. at 27. Malware can be "any software or code developed or used for the purpose of compromising or harming information assets . . ." *Id.* According to the 2011 Verizon study, almost half of data breaches in 2010 were caused by malware, resulting in almost 80 percent of data lost. *Id*.

71. *Id.* at 36. The Verizon report characterized social tactics as "deception, manipulation, intimidation, etc. [employed] to exploit the human element, or users, of information assets." *Id.* These tactics include solicitation and bribery, pretexting, counterfeiting/forgery, and phishing. *Id.*

72. *Id.* at 38 (defining "misuse" as "using entrusted organizational resources or privileges for any purpose or in a manner contrary to that which was intended"). Misuse includes embezzlement, skimming, and other fraud. *Id.* It can also entail abuse of system access as well as use of unapproved hardware and devices. *Id.*

73. *Id.* at 40 (defining physical action to include "human-driven threats that employ physical actions and/or require physical proximity"). Specific actions include tampering, surveillance, and theft. *Id.*

74. *Id.* at 42. According to the Verizon report, this was the smallest source of data loss. Error includes "omissions, misconfigurations, programming errors, trips and spills, malfunctions, etc." *Id.*

75. Pinguelo & Muller, *supra* note 60, at 123–25.

76. Vincent R. Johnson, *Cybersecurity, Identify Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 256 (2005).

77. Identity theft has been on the rise since the late 1980s, and some estimates put the resulting costs to businesses in the billions of dollars per year. Winn & Govern, *supra* note 43, at 49. Costs to consumers have been reported to be as high as two billion dollars per year and millions of hours are spent on cleaning up the resulting mess. *Id.*

78. Johnson, *supra* note 76, at 256–57.

target of cyber attacks.[79] For example, in *Pisciotta v. Old National Bancorp*, plaintiffs sought compensation after their personal information was taken from the defendant's website.[80] The *Pisciotta* plaintiffs sought costs incurred for credit-monitoring services as well as emotional distress based on a negligence theory.[81] The court held that "[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."[82] The plaintiffs had relied on a state data security breach notification law to assert that the legislature intended for individuals to have a legally recognizable and compensable injury when personal information is exposed.[83] The court refused to recognize this inference and noted that other jurisdictions confronting a similar issue had failed to accept such an argument.[84]

As of February 2012, forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted customer data breach notification laws similar to the law plaintiffs attempted to rely upon in *Pisciotta*.[85] However, as demonstrated in *Pisciotta*, consumers generally do not have a cause of action for the exposure of their personal information resulting from a data breach.[86] Federal laws also provide very few, if any, meaningful remedies and private

79. *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 637 (7th Cir. 2007); Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006) (denying recovering for credit monitoring costs); Hendricks v. DSW Shoe Warehouse, 444 F. Supp. 2d 775, 779-81 (W.D. Mich. 2006) (denying claim as failure to show personal information has been used barred recovery).

80. *Pisciotta*, 499 F.3d at 631–32.

81. *Id.*

82. *Id.* at 639.

83. *Id.* at 636–37.

84. *Id.* at 637, 639.

85. *State Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecommunications-information-technology/security-breach-notification-laws.aspx (last updated Aug. 20, 2012). Security breach notification laws require customers to be notified of security breaches that compromise personal information. *Id.*

86. *See* Juliet M. Moringiello, *Warranting Data Security*, 5 BROOK. J. CORP. FIN. & COM. L. 63, 68–72 (2010) (observing that "there are two major impediments to recovery for the losses that individuals incur as a result of a data breach. The first . . . . is that the damages are seen as too speculative. Second, purely economic losses that are not coupled with personal injury or physical property damage are not recoverable in tort.").

rights of action against companies that fail to secure personal information.[87]

As a result of the void in private remedies for individual consumers victimized by data breaches, federal legislation has been proposed and several states have enacted legislation requiring data encryption.[88] However, proposals for widespread change have stayed just that: proposals.[89]

The Data Accountability and Trust Act, introduced in 2009, would have charged the Federal Trade Commission (FTC) with setting regulations on storing and the disposal of personal information.[90] Businesses and organizations that violated these promulgated rules would be subject to fairly steep fines.[91] The bill also called for consumers to be notified when their personal information was compromised.[92]

The Data Security and Breach Notification Act is one of the more recent proposed bills concerning data breaches.[93] Like its predecessor, the bill calls for FTC directed regulations, penalties, and standards for data encryption.[94] Although the proposed bills do not call for mandatory insurance to cover data breaches, at least one observer has noted the possibility of including such a provision in a new federal law.[95]

President Obama and White House Cybersecurity Coordinator Howard Schmidt recently called for national cybersecurity legislation.[96] President Obama mentioned cybersecurity legislation in

87. *See* Rancourt, *supra* note 13, at 201–05 (asserting that "[s]tatutory, not just economic, damages should be available to the persons affected by . . . . data breaches because the current federal statutory landscape is unable to provide adequate redress").

88. *Id.* at 205–12. *See also* NEV. REV. STAT. § 603A.215 (2010) (requiring data collectors to encrypt personal information); 201 MASS. CODE REGS. 17.00 (2008) (establishing requirements for security involving data breaches and requiring data encryption). For proposed federal legislation see Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009); see also Data Security and Breach Notification Act, S. 3742, 111th Cong. (2010).

89. Rancourt, *supra* note 13, at 212.

90. *See* H.R. 2221 § 2(a).

91. H.R. 2221 § 4(c)(2)(A)(i).

92. *See* H.R. 2221 § 3(a)(1).

93. Rancourt, *supra* note 13, at 212.

94. S. 3742 § 2(a).

95. Rancourt, *supra* note 13, at 215.

96. Elizabeth Montalbano, *White House Presses For New Cybersecurity Laws*, INFORMATIONWEEK (Jan. 27, 2012, 2:02 PM), *available at* http://www.informationweek.com/

his 2012 State of the Union address and stressed cooperation between the private and public sectors.[97] The new law would also include a national data breach notification requirement, instead of the patchwork system currently implemented at the state level.[98] However, this proposal has met with some opposition, specifically from the U.S. Chamber of Commerce, amid worries that increasing regulatory and financial burdens could be problematic for critical infrastructure companies.[99] Other critics assert that the president's proposal places too heavy an emphasis on regulatory action and not enough consideration of private sector capabilities.[100] It is in this climate that insurance for cyber risk liabilities enters the discussion.

III. DATA BREACH INSURANCE COVERAGE

A. Outdated Insurance for a Modern Problem

A "cyber" risk is comprised of the previously mentioned cyber crimes and more generally encompasses risks that are associated with Internet business activity.[101] As with any other risk, businesses and organizations seek to protect themselves against cyber-related losses through insurance policies tailored towards the specific risks that are responsible for these losses.[102] The majority of businesses purchase commercial general liability (CGL) insurance to cover a wide array of risks and are typically the first place businesses seek coverage related to possible future losses.[103]

---

news/government/security/232500639. Schmidt stated his desire "that members of Congress will look at the significant amount of public debate that has been occurring on these issues—as well as the work and debate on this issue over the years in the Congress—and continue to work in a bipartisan manner to quickly enact legislation to address the full range of cyber threats facing our nation." *Id.*

97. *Id.*

98. *Id.*

99. *Id.*

100. *See* Erich Schwartzel, *Cybersecurity Insurance: Many Companies Continue To Ignore the Issue*, PITTSBURGH POST-GAZETTE (June 22, 2010, 12:00 AM), http://www.post-gazette.com/pg/10173/1067262-96.stm.

101. Jayson W. Sowers, *Insurance Coverage for Cyberspace Liabilities*, 723 PRACTISING L. INST./LITIG. 199, 205 (2005).

102. Winn & Govern, *supra* note 43, at 53. Businesses traditionally seek insurance coverage to protect against potential liabilities such as fire, flood, and theft. *Id.*

103. Sowers, *supra* note 101, at 208.

Modern standard CGL policies can be traced to the 1940s.[104] CGL policies may differ based on the insured and the insurer, but most CGL policies are based on standard policies drafted by the Insurance Services Office (ISO), Inc.[105] Companies acquire CGL policies to mitigate liability for damages caused to third parties as a result of company negligence.[106] However, damages covered under a CGL policy are not unlimited. In 1965, the ISO modified its standard CGL policy to make it explicit that the only losses covered under its standard policy were losses for physical damage or loss of property.[107] The standard CGL policy was never designed to cover lost profits, loss of goodwill, or any intangible losses.[108] This coverage gap in CGL policies to cover intangible assets has been most problematic for companies seeking to recover for losses incurred as a result of data breaches.[109]

CGL policies today contain two coverage parts that might be relevant to cyber-related losses.[110] First, CGL policies cover damages as a result of "bodily injury" or "property damage."[111] "Bodily injury" will most likely not be relevant in cyber-related coverage issues, thus coverage under this first part is determined by the definition of "property damage."[112]

Property damage is most commonly defined as the "physical injury to" or "loss of use of tangible property."[113] Whether electronic data is considered "tangible property" has been a major issue in

104. Paula M. Yost, Paul E.B. Glad & William T. Barker, *In Search of Coverage in Cyberspace: Why the Commercial General Liability Policy Fails to Insure Lost or Corrupted Computer Data*, 54 SMU L. REV. 2055, 2062 (2001).

105. *Id.* Insurance Services Office, Inc. provides detailed information about risk, claims, and pricing based on language in its promulgated policies. *Id.* at 2063.

106. *Id.* at 2064.

107. *Id.*

108. *Id.* at 2064–65.

109. *See id.* at 2075 ("[T]angibility is the touchstone of 'property damage' coverage under a CGL. Because words are to be given their ordinary meaning, and because information and ideas cannot be 'touched or felt,' information and ideas—however, memorialized—are not 'tangible property' and no coverage will flow from their loss or corruption . . . . The [CGL] contract simply provides for nothing more.").

110. Sowers et al., *supra* note 101, at 208–09. CGL policies are typically divided into two parts: Coverage A and Coverage B. *Id.*

111. *Id.* at 209. The first coverage part is Coverage A. *Id.*

112. *Id.*

113. *Id.*

determining whether loss of or damage to data is covered under CGL policies.[114] To avoid this ambiguity, recent CGL policies explicitly exclude electronic data from the definition of tangible property.[115]

In addition to coverage provisions for property damage, CGL policies also contain provisions covering losses for personal and advertising injury claims.[116] A number of revisions of the personal and advertising injury clauses have been promulgated since the language was first inserted in standard form CGL policies in 1986.[117] Due to the revisions, a number of iterations of the personal and advertising injury language can be found in CGL policies.[118] However, under the common language of advertising injury clauses, coverage for cyber risk claims will be difficult if not impossible.[119]

B. New Cyber Risk Insurance Policies

Considering the possible coverage gaps that exist under traditional CGL policies, insurers and companies with potential cyber risk

---

114. *Compare* Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., No. 99-185, 2000 U.S. Dist. LEXIS 7299, at *6 (D. Ariz. Apr. 18, 2000) (holding that there was physical damage when information stored on random access memory was destroyed), *with* Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 96 (4th Cir. 2003) (holding that damage to software did not constitute physical damage to tangible property).

115. Commercial General Liability Coverage Form (CG 00 01 12 04), ISO (2003), *available at* www.ramsgate.com/forms/CG0001.pdf ("For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment."). *See also* Sowers, *supra* note 101, at 209.

116. *See* Sowers, *supra* note 101, at 210.

117. *Id.* at 210–11.

118. *Id.*

119. *See id.* at 212–20. Although the original advertising injury coverage grant was fairly broad, it has been limited by requirements insurers have put into CGL policy language. *Id.* at 212–13. An insured must meet four requirements: (1) the insured must have engaged in "advertising activities;" (2) the underlying claim must be among enumerated "offenses;" (3) there is a causal link between the alleged injury and activity; and (4) no exclusion bars coverage. *Id.* at 213. Among the issues businesses face in finding coverage under this provision include falling under "advertising activities," the meaning of "offense," and the scope of the requisite enumerated offenses. *Id.* at 213–19.

Few cases have interpreted the personal injury definition as related to cyber claims. *Id.* at 220. Under the personal injury definition, the only offenses that might be applicable to cyber-liability coverage issues are wrongful entry or eviction and violation of the right of privacy. *Id.* at 220–21.

liability have sought new insurance products to cover these new risks.[120] Many of the largest insurers now provide cyber risk policies to fill these gaps.[121] Policies include coverage for data compromise, network risk, computer data coverage, and other various cyber liabilities.[122]

ISO promulgates a standard policy form entitled "Internet Liability and Network Protection Policy," which insurers may use as a template for cyber risk coverage.[123] ISO's "menu-based policy" includes five possible coverage agreements: (1) website publishing liability;[124] (2) network security liability;[125] (3) replacement or restoration of data;[126] (4) cyber extortion;[127] and (5) business income and expense.[128] The senior vice president of ISO's Insurance Services unit stated that the policy was created "to protect companies from the rapidly evolving risk of using the Internet as a business tool."[129] When implementing these policies, insurers often require potential policyholders to provide an inventory of their computer software, past cyber threats, documentation of their employee hiring policies, and answers to a multitude of IT-related questions.[130] Insurers may require changes in policies and practices before providing coverage.[131]

120. *Id.* at 224.

121. *Id.* As of 2005, insurers offering new policies included AIG, Chubb, CIGNA, CAN, Liberty Mutual, St. Paul, and Zurich. Cyber-risk policies are also referred to as Network Risk, Privacy and Security, or Media Liability insurance policies. Godes, *supra* note 11.

122. Godes, *supra* note 11.

123. *Id. See also* Press Release, ISO, ISO Introduces Cyber Risk Program To Help Cover $7 Trillion E-Commerce Market (Jan. 11, 2005), http://www.iso.com/Press-Releases/2005/ ISO-INTRODUCES-CYBER-RISK-PROGRAM-TO-HELP-COVER-$7-TRILLION-E-COMMERCE-MARKET.html.

124. Coverage might include claims for copyright, trademark, and service mark infringement. Press Release, *supra* note 123.

125. This coverage includes claims for failure to prevent unauthorized access of personal information. *Id.*

126. Coverage protects against lost or corrupted data that might result because of a virus or other malicious cyber attack. *Id.*

127. Cyber extortion is "a threat to commit an e-commerce incident, disseminate . . . . proprietary information, reveal a weakness in [] source code or publish personal information belonging to [] clients." *Id.*

128. *Id.*

129. *Id.*

130. Schwartzel, *supra* note 100.

131. *See id.*

Despite their current availability, some observers question whether insurers will continue to find cyber insurance policies fiscally feasible products to underwrite.[132] As previously discussed, cyber risks involve the actions of criminals actively seeking to attack data holders and acquire personal information.[133] In comparison to other liabilities covered by insurance, cyber risk is unique in this respect.[134] A prominent insurance blog aptly describes the relevant problem:

> Here we have a constantly changing source of threats, some of them quite sophisticated, and they can be tweaked almost instantly to counter potential defenses. Techniques and tools can be updated quickly and shared with other black hats. Deployment is rapid, widely dispersed, and adaptable.
>
> Now, compare this with an industry that has to essentially rely on the insured to manage its own defense, relies on an annual process of applications that provides only a snapshot of the exposure at the time it is completed, and which is admittedly challenged at identifying the true risk of loss.[135]

Additionally, even in the face of the high number of data breaches in 2011, the majority of companies in the United States are not buying cyber risk insurance.[136] Various explanations are offered for why adoption is slower than expected, including the "economy, uncertainty about how the policies work, lack of awareness about the exposure and an assumption . . . . that existing general liability or errors and omissions policies will provide coverage."[137] One survey of companies with annual sales from $10 million to $500 million

---

132. *Cyber Insurance–I Am Growing Increasingly Concerned That Insurers Won't Be Able to Keep Up With The Threat*, THE BETTERLEY REPORT BLOG ON SPECIALTY INSURANCE PRODUCTS (Sept. 30, 2011), http://thebetterleyreport.wordpress.com/2011/09/30/cyber- insurance-i-am-growing-increasingly-concerned-that-insurers-wont-be-able-to-keep-up-with-the-threat/.

133. *See supra* Part II.A.C.

134. BETTERLEY REPORT BLOG, *supra* note 132.

135. *Id.*

136. Douglas McLeod, *A Surprising Reticence: Computer Network Risk Coverage Is Growing, But Not As Fast As One Would Expect Given The Recent Spate Of Corporate Data Breaches*, RISK & INS. (Oct. 15, 2011), http://www.riskandinsurance.com/story.jsp?storyId=533342180.

137. *Id.*

found only 35 percent of respondents currently had cyber risk coverage and 40 percent were not even considering purchasing coverage.[138] Lack of widespread adoption of cyber insurance can be a significant problem considering the insurance industry depends on spreading risk among a large number of policyholders.[139]

Some of the slow growth might also be attributed to companies believing they are too small to need coverage.[140] Yet according to a study conducted by Verizon in conjunction with the U.S. Secret Service, 63 percent of cyber attacks in 2010 were committed against businesses with one hundred or fewer employees.[141] This is troubling considering small businesses are more likely to have a difficult time affording cyber liability protection.[142]

Further adding to the unstable ground upon which cyber liability insurance stands is the lack of guidance on how courts will interpret the policy language.[143] A declaratory judgment action filed in April of 2009 against Federal Insurance Company provided some possible insight into the future of cyber risk insurance disputes.[144] However, the litigation was settled out of court pursuant to a confidential settlement agreement.[145]

IV. FEDERAL INTERVENTION

Considering the difficulties companies face protecting consumer personal data and insuring against loss or destruction of that data,[146] it is imperative that insurance coverage is considered in future

138. *Id.*

139. David Navetta, *Cyber Insurance: An Efficient Way To Manage Security And Privacy Risk In The Cloud?*, INFO. LAW GROUP (Feb. 1, 2012), http://www.infolawgroup.com/2012/02/articles/cloud-computing-1/cyber-insurance-an-efficient-way-to-manage-security-and-privacy-risk-in-the-cloud/.

140. McLeod, *supra* note 136.

141. VERIZON, *supra* note 56. *See also* Steve Brooks, Op-Ed., *Cyber Crimes And Data Breaches Are Not Just The Problems Of Big Companies*, PAC. COAST BUS. TIMES (Jan. 27, 2012), http://pacbiztimes.com/2012/01/27/oped-cyber-crimes-and-data-breaches-are-not-just-the-problems-of-big-companies/.

142. Brooks, *supra* note 141.

143. Godes, *supra* note 11.

144. Richard K. Traub, Robert M. Leff & Stuart A. Panensky, *Cybersecurity Coverage Litigation*, 2 DATA SEC. & PRIVACY LAW 14:40 (Ronald N. Weikers ed., 2012).

145. *Id.*

146. *See* discussion *supra* Parts III.A–B.

government action involving data breaches. The Sony data breach and other data breaches making recent headlines should provide a strong warning to both the business community and the government of the extent to which many entities remain at risk for lack of insurance against losses resulting from cyber risks. Considering the slow pace at which companies are retaining cyber risk insurance,[147] and in light of what is at stake,[148] federal and state governments should do their utmost to encourage widespread adoption through support of the private cyber insurance market.

Both the size of Sony as a corporate entity and the large expenses that have resulted from cyber attacks on its data network make it almost unbelievable that Sony failed to maintain any insurance that would cover its liability as a result of a data breach. As previously discussed, academics have observed and litigants have experienced firsthand the failure of CGL policies to cover cyber risk-related losses.[149] Cyber risks present too many unorthodox coverage scenarios for businesses to rely on their traditional CGL policies.[150] Although many businesses have been slow to realize this coverage gap, it is by no means a brand new revelation.[151] Considering the prominence of Sony, it is difficult to imagine Sony management was unaware of such a massive uncovered liability.

That Sony and other large corporate entities are at risk is disconcerting. It demonstrates that the current market incentives are not enough to convince even the most sophisticated businesses of the importance in insuring against cyber risk. However, the evidence that the majority of cyber attacks committed in 2010 were against small businesses is equally if not more troubling.[152] Consider what would happen to a small retail business that stores business information and client personal information such as credit card numbers on a computer. If the retail business was subsequently the target of a cyber attack, it could be liable to customers and would most likely need to expend a considerable amount of time and money responding to a

147. *See* discussion *supra* notes 132–42.
148. *See* discussion *supra* notes 23–30, 50–52.
149. *See* discussion *supra* Part III.A.
150. *Id.*
151. *See* discussion *supra* Parts III.A–B.
152. *See* discussion *supra* notes 140–42.

possible theft of its business identity. Arguably, large corporations like Sony can weather a few of these data breaches without insurance. Yet a small retail business could be crippled if not destroyed by just one attack.

There are a number of possible benefits in the state and federal facilitation of widespread cyber risk insurance adoption. First, insurers providing policies will most likely require better data security before providing businesses or organizations coverage.[153] This limits the amount of regulation and policing of private data security practices required at the national and state level.

As the proposed federal bills demonstrate, the current proposed framework for addressing data breaches and the electronic exposure of personal information would involve heavy agency regulation.[154] Agency regulation is one way to increase industry cyber security standards. However, regulations setting standards and policies will at best represent minimum requirements. The private insurance industry could instead foster best practices, as insurers require policyholders to minimize the risk they are insuring against.[155] Furthermore, considering the ever-changing landscape of cyber risks, it is probable that private entities are more capable of changing industry-wide standards and procedures to match new risks.

Aiding increased implementation of cyber risk insurance might also decrease the probability that government assistance will be needed if a major cyber security incident were to plague large institutions or affect widespread private entities. The more the private sector is able to internalize isolated as well as systematic data security failures, the less government interference is required.

Government has a few tools at its disposal to help facilitate widespread adoption of cyber risk insurance policies. First, the federal government could help insurers and policy seekers acquire cyber-security information. With increased information sharing, some of the uncertainties that are inherent in such a volatile risk area might

153. *See* discussion *supra* notes 130–31.

154. *See* discussion *supra* notes 88–100.

155. At least one observer has observed the prominent role private insurance can play over government regulation in strengthening cyber security. Schwartzel, *supra* note 100 (quoting senior counsel at the Center for Democracy and Technology in Washington, D.C.).

be eased. Greater ease in acquiring information would arguably decrease costs for insurers, which could be passed on to companies seeking protection and make insurance more accessible.

Second, federal and state governments could require government contractors and sub-contractors to maintain cyber risk insurance. Along with directly increasing the number of businesses with cyber risk insurance, this might indirectly influence more businesses in the private industry to follow their competitors' lead.

V. CONCLUSION

The federal government can play a valuable role in furthering cyber risk insurance adoption among businesses and organizations in the United States. Not only can the government help private entities protect themselves against mounting cyber risk, but encouraging the expansion of the cyber risk market will also help further the larger goal of increasing the effectiveness of cyber security policies and practices. Possible tools to achieve this goal include requiring government contractors and sub-contractors to have cyber risk insurance policies, as well as facilitating greater knowledge of cyber risks to ease the financial burden on the insurance industry.

Whether or not the federal government considers cyber insurance to be an important part of cyber security reform, it is clear that businesses and organizations must protect themselves from losses related to cyber risk. The 2011 Sony data breach is just one example of the devastating impact cyber attacks can have on businesses. Without adequate cyber risk protection, businesses are at high risk of disastrous loss.