Risky Business: Lessons for Mitigating Cyber Attacks From the International Insurance Law on Piracy

Scott J. Shackelford, JD, Ph.D.* & Scott Russell, JD**

ABSTRACT

Organizations of all sizes have increasingly been investigating the prospect of investing in cyber risk insurance to better manage the multifaceted cyber threat. But how useful is cyber risk insurance? Is international insurance law impacting the cyber risk insurance market? And what lessons can be taken from other analogies, such as the maritime piracy context? This article discusses the impact of cyber attacks on the private sector along with analyzing the benefits and drawbacks of relying on cyber risk insurance to enhance cybersecurity by drawing from the maritime insurance industry's response to piracy. We argue that firms must take a proactive stance to managing cyber attacks for their competitive wellbeing as well as to securing critical international infrastructure, but that stakeholders should learn from past experiences and begin by defining "cyber attacks" and international cybersecurity due diligence norms.

I. INTRODUCTION

A legal battle has been brewing since the 2011 cyber attacks on Sony pitting Zurich American Insurance Company ("Zurich") against Sony over the question of insurance coverage for a massive data breach involving more than 100 million lost consumer records and associated monitoring costs.[1] Zurich has

*Assistant Professor of Business Law and Ethics, Indiana University; Senior Fellow, Center for Applied Cybersecurity Research; W. Glenn Campbell and Rita Ricardo-Campbell National Fellow, Stanford University Hoover Institution.

argued that it should be absolved of any liability under its policy with Sony in the more than fifty punitive class-action lawsuits winding their way through legal systems in the U.S. and Canada, because, among other things, Sony was negligent for not encrypting consumer data prior to the breach.[2] Sony expected to spend nearly $180 million on breach-related costs, including litigation expenses, in 2011 alone,[3] though it had some success in getting some of the claims dismissed.[4] In February 2014, though, Zurich won a victory when a judge held that it did not have to defend Sony under the terms of the policy since the claim involved the actions of third parties (in this case, the hackers).[5]

Despite the substantial and growing costs of cyber attacks to many organizations, as the Sony episode exemplifies, many corporate boards of directors have failed to proactively manage their cyber risk exposure—indeed, many have failed to recognize that it even exists in the first place. "I don't think it's a topic that occupies a significant place in board considerations," argues Charles M. Elson, director of the University of Delaware's corporate governance center.[6] This conclusion is buttressed by the results of a 2010 report from Carnegie Mellon's CyLab, based on a survey that interviewed board members and senior executives at Fortune 1000 companies.[7] "*When asked to indicate their board's three top*

**Post-Graduate Fellow, Center for Applied Cybersecurity Research.

1.*See* Complaint, Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011 (N.Y. Sup. Ct. Jul. 20, 2011), *available at* https://iapps.courts.state.ny.us/fbem/DocumentDisplayServlet?documentId=tirVQewp3WujFno1EgNuTA==&.

2. *See* Jaikumar Vijayan, *Zurich Lawsuit Against Sony Highlights Cyber Insurance Shortcomings*, COMPUTERWORLD (July 26, 2011, 7:00 AM), http://www.computerworld.com/article/2509419/disaster-recovery/zurich-lawsuit-against-sony-highlights-cyber-insurance-shortcomings.html.

3. *See, e.g.*, *id.*

4. *See* Dara Kerr, *Sony PSN Hacking Lawsuit Dismissed by Judge*, CNET (Oct. 23, 2012, 5:54 PM), http://www.cnet.com/news/sony-psn-hacking-lawsuit-dismissed-by-judge/.

5. *See* Stewart Bishop, *Sony Units Denied Coverage for Suits Tied to Cyberattack*, LAW360 (Feb. 21, 2014, 4:36 PM), http://www.law360.com/articles/512263/sony-units-denied-coverage-for-suits-tied-to-cyberattack.

6. Chris Costanzo, *Is Your Company Prepared for Cyber Risk?*, BOARDMEMBER.COM (Feb. 24, 2011), https://archive.boardmember.com/Is-Your-Company-Prepared-for-Cyber-Risk.aspx.

7. JODY R. WESTBY, GOVERNANCE OF ENTERPRISE SECURITY: CYLAB 2010 REPORT 6 (2010), *available at* ,http://www.fbiic.gov/public/2010/jul/cylab-

priorities, none of the respondents (0%) selected improving computer and data security, even though 56% of them selected improving risk management."[8] There is some evidence that attitudes are shifting with more firms considering data security as a major concern,[9] and looking to cyber risk insurance may help to mitigate this. But how useful is cyber risk insurance, and should nations view it as an important part of efforts to enhance private-sector cybersecurity?[10] Does it really protect at-risk companies, or is it true that "[t]here aren't many success stories where cyber insurance [has played] a significant role in reducing the costs of incidents"?[11] Ultimately, does cyber risk insurance make firms less proactive in enhancing cybersecurity, damaging the prospects for cyber peace? And what lessons can be learned from related contexts, such as international insurance law related to maritime piracy?

Despite the stakes, relatively little has been written on this vital topic.[12] This article seeks to begin to fill in that gap by first analyzing the rise of cyber risk insurance as an increasingly important tool allowing firms to mitigate their cyber risk exposure in Part II. In Part III, we turn to the analogy of maritime piracy, particularly looking at how courts have differentiated acts of piracy for insurance purposes and what lessons this teaches us for managing cyber attacks. We argue in the best case that cyber risk insurance could help

---

governance-2010.pdf.

8. *Id. at* 11; *see* Costanzo, *supra* note 6; *cf. 2010 Security 500: Tables*, SEC. MAG. (Nov. 1, 2010), http://www.securitymagazine.com/articles/2010-security-500-tables-1?v=preview (twenty percent and eighteen percent answering that cyber security and IT security, respectively, are one of their top areas of responsibility). *See generally* SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE 247 (2014).

9. *See, e.g.*, Catherine Dunn, *Cybersecurity Is Now No. 1 Concern for GCs*, CONN. L. TRIB., Aug. 27, 2012, at 16 (arguing that data security concerns are top of mind at many corporations).

10. *See generally* H. REPUBLICAN CYBERSECURITY TASK FORCE, 112TH CONG., RECOMMENDATIONS OF THE HOUSE REPUBLICAN CYBERSECURITY TASK FORCE 5, 8, 14 (2011) (discussing how cybersecurity is important to national security).

11. Vijayan, *supra note* 2 (quoting John Pescatore, an analyst with Gartner).

12. *Cf*. Lance Bonner, Note, *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*, 40 WASH. U. J.L. & POL'Y 257 (2012) (discussing cyber risk insurance but ignoring the international law dimension).

shield firms from the results of certain cyber attacks. In the worst case, it could merely shift costs and contribute to a more reactive focus, reinforcing an unsustainable status quo.[13]

II. THE RISE OF CYBER RISK INSURANCE

Some commentators have been arguing that insurance is a "key part of the [cybersecurity] solution" for years but it has only relatively recently begun to catch on.[14] The trouble and the reason behind this delay are concerns surrounding the accurate assessment of risk. As data and models have improved, though, cyber risk insurance policies are entering the mainstream. Even the U.S. government has considered encouraging firms to invest in them.[15] Part II begins by breaking down the U.S. cyber risk insurance market before moving on to discuss issues of cyber risk insurance-related moral hazard and due diligence obligations.

A. BREAKING DOWN THE CYBER RISK INSURANCE MARKET

Insurance companies have been experimenting in the cybersecurity arena for more than a decade; Zurich North America, for example, began offering "a reward for information leading to the conviction of" cyber terrorists in 2002.[16] Today, the major players in the cyber risk insurance industry include many market leaders. "Hiscox, a Lloyd's of London syndicate," for example, has begun offering policies for "telecommunications, media, and technology companies that cover[]" losses caused by cyber attacks.[17] By 2011 the cyber risk

---

13. For a more comprehensive look at the rise of cyber risk insurance, see Chapter 5 of SHACKELFORD, *supra note* 8. An earlier version of this research was published as Scott J. Shackelford, *Should Your Firm Invest in Cyber Risk Insurance?*, 55 BUS. HORIZONS 349 (2012).

14. SHACKELFORD, *supra note* 8, at 247 (quoting Google engineer and former technology director Chris Palmer, and citing to author's interview with Mr. Palmer).

15. *See* WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 24 (2003), *available at* http://energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf.

16. Jon Swartz, *Firms' Hacking-Related Insurance Costs Soar*, USA TODAY (Feb. 9, 2003, 11:26 PM), http://usatoday30.usatoday.com/tech/news/computersecurity/2003-02-09-hacker_x.htm.

17. *Id.*; *see Safeonline Launches Internet Security Insurance*, HISCOX,

insurance market has boomed with an increasing number of firms looking to invest in coverage,[18] a trend that could be reinforced depending on regulatory developments such as the Securities and Exchange Commission (SEC) cyber attack disclosure guidelines.[19] Yet geography still plays a role in determining which insurance options are available to interested organizations. There are more policies available in the United States, for example, than other advanced markets, like Canada, which have smaller premium bases.[20] Though this status quo is changing, it will impact the extent to which this form of cyber risk mitigation is available to at-risk firms around the world, including in emerging markets that also experience cyber attacks.[21]

B. WEIGHING THE COSTS AND BENEFITS OF COVERAGE

As one 2008 survey explained, "cyber insurance is a concept that has a great deal of intellectual appeal, has seen a degree of implementation, but that isn't taking the enterprise world by storm."[22] However, these policies have become increasingly affordable.[23] This has kept firms like Brookeland

---

http://www.hiscox.com/news/press-releases/archive/2000/18-10-00.aspx (last visited Oct. 26, 2014).

18. *See, e.g.*, Nicole Perlroth, *Insurance Against Cyber Attacks Expected to Boom*, N.Y. TIMES (Dec. 23, 2011, 10:58 AM), http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom/?_php=true&_type=blogs&_r=0; Robert Lemos, *Should SMBs Invest in Cyber Risk Insurance?*, DARK READING (Sept. 9, 2010, 05:09 PM), http://www.darkreading.com/should-smbs-invest-in-cyber-risk-insurance/d/d-id/1134322?; Swartz, *supra* note 16.

19. *See* Perlroth, *supra* note 18.

20. Denis Drouin, *Cyber Risk Insurance: A Discourse and Preparatory Guide*, SANS INST. INFOSEC READING ROOM 5 (Feb. 9, 2004), http://www.sans.org/reading_room/whitepapers/legal/cyber-risk-insurance_1412.

21. *See generally Countries by Cyber-Attack*, INTELLECTUAL TAKEOUT, http://www.intellectualtakeout.org/library/chart-graph/countries-cyber-attack (last visited Oct. 8, 2014) (breaking down cybercrime between top twenty countries).

22. Robert Richardson, CSI COMPUTER CRIME & SECURITY SURVEY 11 (2008), *available at* http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.

23. *See generally Travelers Adds Cyber Protection Tailored to Small Businesses*, INS. JOURNAL (Jan. 22, 2014), http://www.insurancejournal.com/news/national/2013/01/22/278157.htm?print (discussing policies starting at $120). DHS summarized the current state of cyber risk insurance in 2012, noting that "[w]hile a sizable third-party market exists to cover losses suffered by a company's customers, first-party policies

Fresh Water Supply in East Texas, from which cybercriminals stole $35,000, afloat; because of its insurance policy, instead of going out of business, it only lost its $500 deductible.[24] Nevertheless, obstacles remain, including businesses needing to pass the equivalent of a cybersecurity audit.[25] If managers are not forthcoming, or do not have adequate safeguards in place, then insurance companies may decline coverage, and this is already happening in some markets.[26] And since cyber attacks can happen irregularly, the cost of protection may not always be worth it.[27]

C. DIFFICULTIES OF CALCULATING PREMIUMS AND ASSESSING DUE DILIGENCE OBLIGATIONS

Calculating cyber risk insurance premiums is no simple matter—there is little reliable data that is so critical, for example, to pricing healthcare and automobile insurance. Still, many firms are moving forward despite the relative newness of the problem and the relative lack of incentives for effective information sharing, which can result in skewed calculations.[28] Even after a policy is in place, though, insurance companies

---

that address direct harms to companies themselves remain expensive, rare, and largely unattractive." DHS, CYBERSECURITY INSURANCE WORKSHOP READOUT REPORT 1 (2012), http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf; *see also* Lemos, *supra* note 18.

24. *See The Case for Cybersecurity Insurance, Part II*, KREBS ON SECURITY (July 14, 2010, 10:22 AM), http://krebsonsecurity.com/2010/07/the-case-for-cybersecurity-insurance-part-ii/.

25. *See, e.g.*, Brooke Yates & Katie Varholak, *Cyber Risk Insurance – Navigating the Application Process*, SHERMAN & HOWARD (June 6, 2013), http://shermanhoward.com/publications/cyberriskinsurance-navigatingtheapplicationprocess/.

26. *See generally* Mark Ward, *Energy Firm Cyber-Defense Is 'Too Weak', Insurers Say*, BBC NEWS (Feb. 27, 2014), http://www.bbc.com/news/technology-26358042.

27. *See generally* Denise Dubie, *Corporate Security Spending Not in Line with Real-World Requirements*, NETWORK WORLD (May 5, 2003, 1:00 AM), http://www.networkworld.com/news/2003/0505nemertes.html (arguing that most large companies do not spend enough of their IT budgets on upgrading security infrastructure); Riva Richmond, *How to Determine if Cyber Insurance Coverage is Right for You*, ENTREPRENEUR (July 5, 2012), http://www.entrepreneur.com/article/223921 (discussing factors that go into the decision whether to purchase cyber insurance).

28. *See* Lawrence A. Gordon et al., *A Framework for Using Insurance for Cyber-Risk Management*, 46 COMM. ACM, Mar. 2003, at 81, 82; *see also* DHS, *supra* note 23, at 1. *See generally* SHACKELFORD, *supra* note 8, at 251.

may worry about companies' behavior when insulated from risk, e.g., moral hazard (consider the Sony example above). This issue may be at least partly addressed through incentive programs such as offering premium reductions for firms that avoid certain bad behaviors,[29] analogous to a safe driving discount. Among others, AIG currently provides discounts to firms that utilize secure hardware and software packages.[30]

Given that cyber attacks are a global issue, it is essential that the role of international law be analyzed if cyber risk insurance is to be a component of mitigating threats. However, there is a relatively paucity of applicable regulations.[31] As a result, we have decided to draw an analogy to international maritime law, specifically piracy, to assess the lessons that may be learned.

III. APPLYING LESSONS LEARNED FROM THE MARITIME PIRACY CONTEXT

Analogies between cyberspace and international maritime law are not new.[32] Cyberspace, like the high seas, may be considered as an international arena that confounds traditional notions of territorial sovereignty.[33] Both feature layered jurisdictions, with the oceans comprised of territorial seas and exclusive economic zones, and cyberspace conceptualized as both an extension of national territory and a "global networked commons."[34] Indeed, both of these regions of the "global

29. *See* Gordon et al., *supra* note 28, at 83; DHS, *supra* note 23, at 40. *See generally* SHACKELFORD, *supra* note 8, at 251.

30. Gordon et al., *supra* note 28, at 83. *See generally* SHACKELFORD, *supra* note 8, at 251.

31. Most contemporary examples include European Union laws and private sector trade association initiatives. *See, e.g.*, EUR. NETWORK & INFO. SEC. AGENCY, INCENTIVES AND BARRIERS OF THE CYBER RISK INSURANCE MARKET IN EUROPE 30 (2012).

32. *See* Jeremy Rabkin & Ariel Rabkin, *Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea*, 14 CHI. J. INT'L L. 197, 202 (2013).

33. *See* SHACKELFORD, *supra* note 8, at 282–83; *cf.* MILTON MUELLER & BEN WAGNER, INTERNET GOVERNANCE FORUM, FINDING A FORMULA FOR BRAZIL: REPRESENTATION AND LEGITIMACY IN INTERNET GOVERNANCE 9–10 (2014), http://www.internetgovernance.org/wordpress/wpcontent/uploads/MiltonBenWPdraft_Final.pdf (stating that censorship is one of the many ways nations exercise control over cyberspace).

34. Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010),

commons" are experiencing increasing regulation by national governments keen to exploit offshore resources, regulate e-commerce, control restive populations, and mitigate cyber attacks.[35] Similarities between piracy and cybercrime range from problems of enforcement and extradition,[36] to the modern trend of active defense.[37] These similarities are best seen in the failure to establish an international definition of either "piracy" or "cyber attack."[38]

This Part begins by discussing the difficulties of defining "piracy" under international law before moving on to briefly discuss the rise of maritime piracy insurance and what lessons may be applied to overcome challenges in the field of cyber risk insurance.

A. DEFINING "PIRACY" UNDER INTERNATIONAL LAW

Despite a long history of international efforts aimed at regulating piracy, there is no overarching body of international piracy law, illustrated by the fact that agreements like the UN Convention on the Law of the Sea (UNCLOS) merely create frameworks from which nations may choose to enforce domestic piracy laws when it suits their interests.[39] This is further complicated by the unique definition given to piracy for

---

http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

35. The notion of the global commons posits that there are limits to national sovereignty in certain issue areas, and that these fields should be "open to use for community access and public use and closed to exclusive appropriation or individual use . . . ." *See* CHRISTOPHER C. JOYNER, GOVERNING THE FROZEN COMMONS: THE ANTARCTIC REGIME AND ENVIRONMENTAL PROTECTION 222 (1998).

36. *See* Jennifer J. Rho, Comment, *Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable Under the Alien Tort Statute*, 7 CHI. J. INT'L L. 695, 709–12 (2007).

37. *See* Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. INT'L. L. 103, 103–05 (2014).

38. *See* SHACKELFORD, *supra* note 8, at xxxii. Though definitions vary, according to the U.S. National Academy of Sciences, cyber attacks refer to "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks." NAT'L RESEARCH COUNCIL OF THE NAT'L ACADEMIES, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009); *see also infra* notes 41–45 and accompanying text.

39. *See* Lucas Bento, *Toward an International Law of Piracy Sui Generis: How the Dual Nature of Maritime Piracy Law Enables Piracy to Flourish*, 29 BERKELEY J. INT'L L. 399, 415 (2011).

insurance purposes, wherein courts distinguish piracy from acts at sea that may be politically motivated, despite being otherwise piratical.[40] The international community should learn from the history of maritime piracy in defining what actions constitute cybercrimes, setting standards for due diligence, and determining what responsibilities nations have to mitigate cybercrime within their jurisdictions.

Piracy, despite being an international crime, has long had an ambiguous definition in international law.[41] Even with the adoption of UNCLOS, the definition of piracy fosters ambiguity by requiring the act be for "private ends" without clarifying how this determination is to be made, and by necessitating the act be illegal without demanding that states enact domestic anti-piracy laws.[42] International treaties that address piracy are also muddied by the divergence between monist states, like France, and dualist states, like the United States.[43] Monist states adopt the international definition inherently, whereas dualist states sometimes require domestic legislation to enact the relevant portions of a treaty, and thereby insulate themselves from developments in international law.[44] The situation is further complicated by the existence of no less than six potential sources defining piracy.[45]

B. THE RISE OF MARITIME PIRACY INSURANCE

Among the varied national and international laws criminalizing piracy, insurance law is a distinct category with unique rules. Although insurance companies have long crafted

---

40. *Id.* at 432.

41. The UN Convention on the Law of the Sea defines "piracy" in part as "any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft . . . ." United Nations Convention on the Law of the Sea art. 101, Dec. 10, 1982, 1833 U.N.T.S. 3; *see also Piracy and Armed Robbery Against Ships*, INT'L MAR. ORG., http://www.imo.org/OurWork/Security/PiracyArmedRobbery/Pages/Default.aspx (last visited Sept. 2, 2014) (showing that the definition of "piracy" under the UN Convention on the Law of the Sea is ambiguous).

42. *See* Bento, *supra* note 39, at 416.

43. *Id* at 413.

44. *Id*. The distinction between self-executing and non-self-executing treaties under international law is ably explored in the U.S. context by Oona A. Hathaway et al., *The Treaty Power: Its History, Scope and Limits*, 98 CORNELL L. REV. 239 (2013).

45. ALFRED P. RUBIN, THE LAW OF PIRACY 1 (1988).

specific policies to cover piracy, coverage requires in-depth analysis of whether specific acts are "piratical, war-like, terrorist, malicious, or merely violent."[46] Due to provisions like "war-risks exclusion" clauses, conduct that might appear to be piracy under an international law definition will not be considered such by an insurer if it is exempted by a "free of capture and seizure clause," or otherwise distinguishable from the insurer's definition of piracy.[47] The absence of an internationally consensual definition of piracy has historically resulted in seemingly inequitable results for the insured, as the ambiguity in definition allowed for courts to interject national policy into international adjudication.[48] Similar debates are happening now in the cybersecurity context, as is discussed below.[49]

For instance, in the 1909 English case of *Republic of Bolivia v. Indemnity Mutual Marine Insurance Co.*, the Court of Appeal of England and Wales upheld a lower court's determination that an insurance policy, which specifically covered losses from piracy, was not bound by the international law defining piracy.[50] The case involved a Bolivian cargo ship that was supplying Bolivian troops to aid in a dispute over the Brazil-Bolivia border, whereas the "pirates" in question were Brazilian nationals. Justice Pickford, writing for the lower court, openly acknowledged that the act might have fallen under the definition of piracy under prevailing international law.[51] In addressing the definition of "piracy," however, he chose to apply "the meaning that would be given to it by ordinary persons, rather than the meaning to which it may be

---

46. Richard Williams, *The Effect of Maritime Violence on Contracts of Carriage by Sea*, 10 J. INT'L MAR. L. 343, 344 (2004).

47. *See generally* Christopher M. Douse, *Combatting Risk on the High Sea: An Analysis of the Effects of Modern Piratical Acts on the Maritime Insurance Industry*, 35 TUL. MAR. L.J. 267, 278–281 (2010) (discussing how maritime insurers use free of capture and seizure clauses to limit piracy from coverage).

48. *See generally id.* at 281–85 (introducing cases showing how English courts have used national policy to determine whether piracy is within the scope of coverage).

49. *See infra* notes 61–67 and accompanying text.

50. [1909] 1 K.B. 785 (Eng.).

51. *Id.* at 791–92 (Vaughan Williams L.J.) ("Such an act may be piracy by international law, but it is not, I think, piracy within the meaning of a policy of insurance; because, as I have already said, I think you have to attach to piracy a popular or business meaning, and I do not think, therefore, that this was a loss by piracy." (quoting Pickford, J.)).

extended by writers on international law."[52] Categorized as such, the Brazilian assailants were held not to be pirates, and damages caused by their actions were therefore not covered by the English insurance policy.[53] The court effectively utilized the weak international standards regarding the definition of piracy to further domestic public policy.

In the more recent case of the Somali Pirates, insurance companies have sought other means to manage risk.[54] The English insurer Lloyd's of London, in response to the substantial increase in potential costs from pirate capture and ransom, classified the entire Gulf of Aden as a "war risk zone," raising premiums for individual voyages from $500 to up to $150,000 per ship per voyage.[55] In the United States, the situation was avoided entirely. Although U.S. hull insurance policies exclude losses due to piracy, these losses are then covered by the Maritime War Risk Insurance Program.[56] This program allows the Secretary of Transportation to provide insurance to shipping vessels when insurance cannot be obtained on reasonable terms in the U.S. market (a public option for insuring against piracy, as it were).[57] This, in combination with active U.S. naval patrols throughout the Horn of Africa, has allowed U.S. maritime insurers to avoid paying ransom for any act of piracy.[58] It should be noted, however, that neither of these cases adequately addressed the problems of piracy. The British insurers solved the problem by reclassifying the attacks as war risks rather than piracy and substantially increasing the insurance premiums on all vessels.[59] In the United States, the insurance costs associated with piracy were effectively paid by state subsidy.[60] However, it

52. *Id.* at 790.

53. *Id.* at 786.

54. *See* Zack Phillips, *Marine Insurers Transfer Piracy Risk to War Cover: Surge in Attacks Prompts Move by London Market*, BUS. INS. (Mar. 29, 2009, 6:00 AM), http://www.businessinsurance.com/article/20090329/ISSUE01/100027383&template=printart.

55. *See* LAUREN PLOCH ET AL., CONG. RESEARCH SERV., R40528, PIRACY OFF THE HORN OF AFRICA 13 (2011), *available at* http://www.fas.org/sgp/crs/row/R40528.pdf.

56. *See id.*

57. *Id.* at 40–41.

58. *See id.* at 13 (stating that actions by owners to protect their ships and cargo constitute a third factor contributing to this result).

59. *See supra* note 55 and accompanying text.

60. *See supra* note 56 and accompanying text.

seems unlikely that the U.S. government would be similarly inclined to reimburse firms hit by cyber attacks through direct subsidies or public insurance coverage.

C. LESSONS FOR CYBER RISK INSURANCE

The parallels between insuring against maritime piracy and cyber attacks are abundant. In both cases, losses may be motivated by a multitude of reasons ranging from pecuniary gain to furthering social causes to geopolitics.[61] For instance, the 2009 cyber attacks on Lockheed Martin resulted in substantial financial losses both in the form of trade secrets and in a damaged public image.[62] Analysis of the attack has led some observers to speculate that it was perpetrated by, or at least connected with, the Chinese government.[63] Categorizing such an attack as merely a cybercrime would fail to address the potential geopolitical element of the incident, whereas categorizing it as cyber espionage may preclude insurance coverage, analogous to the "war-risks exclusion," given that, among other problems, spying is not illegal under international law.[64] Nor is there a consensual definition of "trade secrets."[65] This ambiguity is exacerbated by the ease with which cyber attacks can be masked or obfuscated across platforms and jurisdictions.[66] Cybercriminals may mount attacks that appear to have originated within foreign governments, while state sponsorship of cyber attacks using non-state actors further

61. *See* SHACKELFORD, *supra* note 8, at 6–18 (discussing the four main categories of cyber attacks: cyber war and espionage (roughly corresponding to geopolitics), cyber crime (pecuniary gain), and cyber terrorism (social causes)).

62. *See, e.g.*, Siobhan Gorman, August Cole, & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, WALL ST. J. (Apr. 21, 2009, 12:01 AM), http://online.wsj.com/article/SB124027491029837401.html.

63. *See id*.

64. *See* SHACKELFORD, *supra* note 8, at 7–11.

65. *See* Scott J. Shackelford et al., *Using BITs to Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets through Bilateral Investment Treaties*, 52 AM. BUS. L.J. 1, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2324619.

66. An example is Mandiant's 2013 report on China's cyber espionage activities. *See* Dan Mcwhorter, *Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators*, M-UNITION (Feb. 18, 2013), https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/; *cf.* Jeffrey Carr, *Mandiant APT1 Report Has Critical Analytical Flaws*, DIGITAL DAO (Feb. 19, 2013, 4:14 AM), http://jeffreycarr.blogspot.com/2013/02/mandiant-apt1-report-has-critical.html.

complicates the picture. Similarly, hacktivist groups like Anonymous and the Lizard Squad often have social or pseudo-terrorist motivations, and may also be outside the intended bounds of cyber risk insurance policies. Difficulty in attribution is nothing new,[67] but with the added element of insurance coverage, the result for businesses will likely be increases in costs and litigation.

Beyond mere classification of the attack, there is the issue of what property is covered. Under maritime insurance policies, a typical distinction would be made between coverage of the hull (the body of the ship) and coverage of the goods being shipped.[68] This dichotomy has parallels with cyber risk insurance. Cybercriminals may wish to steal data, which may be analogized with the loss of goods, whereas cyber terrorists (and sometimes governments) may wish to damage or destroy critical infrastructure, which is akin to the hull itself. Yet again because of the attribution problem and the associated difficulties of establishing intent, it will be difficult for both insured organizations and insurance companies to prove who exactly was going after what and to what end.

Most importantly, maritime piracy teaches us that the best means of combating piracy internationally is to address the problem at its sources, which are the nations where such activity is allowed to flourish.[69] The recent reemergence of piracy in the Indian Ocean is a direct result of the destabilization of nations in East Africa that has allowed piracy to go domestically unprosecuted.[70] The collapse of the Somali government in 1991 provided a safe haven for piracy, and it is only through domestic enforcement mechanisms that the problem will be effectively stamped out.[71] Regarding cybersecurity, it has been shown that nations with broadband

---

67. For more on this topic, see generally SHACKELFORD, *supra* note 8, ch. 3 & 6.

68. *See* Douse, *supra* note 47, at 278–80 (comparing the coverage of hull policies and cargo-related policies).

69. *See* PLOCH ET AL., *supra* note 55, at 41 ("Ultimately, piracy is a problem that starts ashore and requires an international solution ashore. We made this clear at the offset of our efforts. We cannot guarantee safety in this vast region. Our role in preventing some of these attacks is only one part of the solution to preventing further attacks." (quoting *Combating Piracy on the High Seas: Hearing Before the H. Comm. on Armed Serv.*, 115th Cong. 8 (2009) (statement of William E. Gortney, Commander, U.S. Naval Forces Cent. Command))).

70. *See id.* at 4.

71. *Id.* at 41–42.

Internet connections and weak governance have increased risk of becoming havens for cybercrime.[72] Incentives and information sharing mechanisms are required to overcome this situation.[73]

Although insurance may incentivize best practices and provide effective risk management, cyber risk insurance is ultimately only a method of cost shifting. Private entities would benefit from proactively implementing measures to deter and prevent cybercrime, and the international community should endeavor to create meaningful enforcement mechanisms to police nations harboring cybercriminals. By defining robust international standards of private and public due diligence, the international community can effectively mitigate cyber attacks.[74]

IV. CONCLUSION

Although the cyber risk insurance market still has to surmount difficulties with accurately assessing and quantifying risk along with a lack of information sharing,[75] it is growing in size, sophistication, and importance, and is becoming better able to meet the risk mitigation needs of organizations of all sizes.[76] However, there is a potential dilemma that some firms would rely on cyber risk insurance to put off enhancing their cybersecurity, as could have been partly behind Sony's woes, which is why policies should be set up to "reward" firms that

72. *See* Marthie Grobler & Joey Jansen van Vuuren, *Broadband Broadens Scope for Cyber Crime in Africa*, *in* INFO. SEC. SOUTH AFRICA CONF. PROC. (Hein S. Venter et al. eds., 2010), *available at* http://icsa.cs.up.ac.za/issa/2010/Proceedings/Full/28_Paper.pdf; *Cybercriminals in Developing Nations Targeted*, BBC NEWS TECHNOLOGY (July 20, 2012), http://www.bbc.co.uk/news/technology-18930953; Tamasin Ford, *Ivory Coast Cracks Down on Cyber Crime*, BBC NEWS BUSINESS (Jan. 16, 2014), http://www.bbc.co.uk/news/business-25735305.

73. As an example of such information sharing, see *Oman's CERT Designated as Regional Cyber Security Centre in the Arab World*, E.OMAN (Dec. 15, 2012), http://www.ita.gov.om/ITAPortal/MediaCenter/NewsDetail.aspx?NID=476.

74. *See* Andreas Zimmermann, *International Law and 'Cyber Space*,' 3 ESIL REFLECTIONS, no. 1, Jan. 10, 2014, at 5–6, *available at* http://www.esil-sedi.eu/sites/default/files/ESIL%20Reflections%20-%20Andreas%20Zimmermann_0.pdf.

75. *See* DHS, *supra* note 23, at 6.

76. *See id.* at 6–8.

make proactive cybersecurity investments.[77] Firms can and must do more to mitigate their cyber enterprise risks,[78] while insurance companies and policymakers should learn from the piracy context and begin to work on defining "cyber attacks" for insurance purposes, assisting nations in securing their networks and prosecuting criminals, and establishing due diligence standards. Ultimately, just as maritime shippers would hire private security forces[79] and avoid routes known to harbor pirates,[80] so must firms take every precaution to ensure that their infrastructure and processes are formulated to promote cybersecurity for their consumers and investors alike.

---

77. *Cf. id.* at 5 (stating that cybersecurity insurance may incentivize firms to make proactive cybersecurity investments).

78. *See generally* SHACKELFORD, *supra* note 8, ch. 3 (further discussing technical best practices).

79. *See US Firm to Fight Somali Pirates*, BBC NEWS (Nov. 25, 2005, 8:49 PM), http://news.bbc.co.uk/2/hi/africa/4471536.stm.

80. *See* John W. Miller, *Piracy Cause Changes in Routes*, *Insurance*, WALL ST. J., Apr. 9, 2009, at A10.