Viruses, Trojans and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz – Part I

By Roberta D. Anderson

Every organization is at cyber risk. Cyber threats are on the rise with unprecedented frequency, sophistication and scale, and they are pervasive across industries and geographical borders. It is abundantly clear that network security alone cannot entirely address the issue of cyber risk; no firewall is unbreachable, no security system impenetrable. Insurance can play a vital role in a company's overall strategy to address, mitigate and maximize protection against cyber risk, including data privacy risk. Aware of this fact, the SEC has advised that appropriate disclosures may include a "[d]escription of relevant insurance coverage" for cyber risks, providing yet another compelling reason for all public companies to carefully evaluate their insurance for cyber risks. In Part I of this four part article, the author examines the escalating threat and cost of cyber risk. Parts II and III will examine potential coverage for cyber and privacy-related risks under the general liability, property and other commonly purchased "traditional" insurance policies. Part IV will examine the types of coverages available under revolutionary new "cyber" insurance products.

We're not in e-Kansas anymore. And there's no denying that present day internet Oz, while extraordinary, is increasingly scary. Cyber attacks of various types continue to escalate across the globe. As aptly stated by one commentator: "Cybercrime is raging worldwide."[1] Reports of high profile cyber attacks make headlines almost every day. Recent headlines are filled with reports of sophisticated distributed denial-of-service ("DDoS") attacks against the largest U.S. banks, which disrupted transactions for hours at a time.[2] They also report some of the largest data breaches in history, which have affected the world's most sophisticated corporate giants.[3] And they report billions in intellectual property loss via cyber espionage.[4] Indeed, the director of the National Security Agency has stated that "[t]he ongoing cyber-thefts from the networks of public and private organizations, including Fortune 500 companies, represent the greatest transfer of wealth in human history."[5]

Roberta D. Anderson

The headlines confirm the reality: cyber attacks are on the rise with unprecedented frequency, sophistication and scale. They are pervasive across industries and geographical boundaries. And they represent "an ever-increasing threat."[6]

Even though no organization is immune from cyber risk,[7] it is uncertain that companies are sufficiently aware of the escalating onslaught.[8] Even companies that are sufficiently aware of the problem might not be sufficiently prepared. It is abundantly clear that network security alone cannot entirely address the issue; no firewall is unbreachable, no security system impenetrable. As noted by one observer: "[t]here is no fail-safe technology that is immune to hacking. Online security will evolve as hackers and security experts work continuously to outwit each other."[9] A recent survey conducted by global consulting firm Towers Watson notes "the growing awareness that the increasingly sophisticated cyber-attack capabilities of

Roberta D. Anderson is a partner in the Pittsburgh office of K&L Gates LLP, a law firm that regularly represents policyholders in insurance coverage disputes. The opinions expressed in this article are those of the author, and should not be construed as necessarily reflecting the views of her law firm, or the firm's clients, or as an endorsement by the law firm or the law firm's clients of any legal position described herein. Ms. Anderson can be reached at Roberta.Anderson@klgates.com.

hackers could require a more comprehensive protective net than a reliance on even the most capable IT staff."[10]

Insurance can play a vital role. Yet some companies may not be adequately considering the important role of insurance as part of their overall strategy to mitigate cyber risk. Although the demand for cyber insurance is increasing,[11] the recent Towers Watson survey notes "the sizable number of companies that do not have a liability policy in place," which "speaks to the need for more education and a better understanding of the long-lasting financial and reputational costs that companies face if they don't develop comprehensive risk strategies to thwart cyber-attacks."[12] A recent independent research survey sponsored by Zurich finds that "few organizations – less than 20 percent, according to survey respondents – have purchased security and privacy insurance specifically designed to cover exposures associated with information security and privacy-related issues."[13] On the other hand, risk managers and in-house counsel may not be aware if, and to what extent, the company *already* has coverage for cyber risks under its existing "traditional" insurance policies, many of which cover some form of cyber risk.

A complete understanding of the company's insurance program is key to maximizing protection against cyber risk. This fact has the attention of the Securities and Exchange Commission. In the wake of "more frequent and severe cyber incidents," the SEC's Division of Corporation Finance has issued guidance on cybersecurity disclosures under the federal securities laws. The guidance advises that companies "should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents" and that "appropriate disclosures may include," among other things, a "[d]escription of relevant insurance coverage."[14] Since failure to make these disclosures may subject a company to enforcement actions and shareholder suits, the SEC's guidance provides yet another compelling reason for companies to carefully evaluate their insurance programs, evaluate what coverage already may be available and consider how gaps in coverage can be filled through specialty "cyber" risk policies.

Cyber Criminals Seize the Day – and the Data

2012 was dubbed "the year of the data breach."[15] Some of the world's most sophisticated corporate giants have fallen victim to some of the largest data breaches in history.[16] These breaches have affected the financial services sector, online gaming providers, the health care industry, marketing services firms, retailers, insurers, defense contractors, social networking sites, cloud storage providers, credit card processors – even sophisticated security firms.[17] Verizon's most recent *2013 Data Breach Investigations Report* remarks that "[p]erhaps more so than any other year, the large scale and diverse nature of data breaches and other network attacks took center stage" in the past year.[18] And virtually no major industry is immune from attack.[19]

The Privacy Rights Clearinghouse reports that, as of September 17, 2013, 613,483,424 records have been breached in 3,923 data breaches made public since 2005.[20] The organization notes that "the number … should be much larger" because it is "not a comprehensive compilation" and "[f]or many of the breaches listed, the number of records is unknown."[21]

The escalating cyber attacks are not limited to data breaches of course—they also include expensive DDoS attacks,[22] such as the recent attacks that targeted the financial services sector, and myriad other types of cyber threats, including attacks principally designed to destroy or corrupt data, cyber extortion and cyber espionage. A recent independent research study notes that "[c]yber risk comes in a bewildering variety of forms" including "malware and other viruses, administrative errors, incidents caused by data providers, malicious employee activity, attacks on Web applications, theft or loss of mobile devices, and internal hackers."[23]

The Ponemon Institute's[24] *2012 Cost of Cyber Crime Study* concludes that "companies expend considerable time and resources responding to a plethora of different types of attacks."[25] According to the recent study, "[c]yber attacks have become common occurrences" with the 56 organizations involved in its survey experiencing "102 [overall] successful attacks per week and 1.8 successful attacks per company per week."[26] The study notes that this represents an increase of 42 percent over the "successful attack experience" reflected in its prior study.[27] And the disturbing rise of cyber attacks over the past couple of years may be just the tip of the iceberg. In June 2013, the U.S. Department of the Treasury's Office of the Comptroller of the Currency hosted a call with more than 1,000 community bankers, and warned, as reported in the Wall Street Journal, that "cyber attacks overall, including on banks, increased 42% in 2012, ranging from malicious software or phishing attacks, to well publicized denial-of-service attacks."[28]

The problem of cyber risks is exacerbated, not only by increasingly sophisticated cyber criminals, malicious code and other types of malware[29] – which in the case of the recent DDoS attacks was described as "10 times as potent as the types of denial-of-service attacks hackers have

mounted in the past"[30] – but by the trend in outsourcing of data handling, processing and/or storage to third party vendors, including "cloud" providers. The Ponemon Institute's *2011 Cost of Data Breach Study*, published in March 2012, found that over 41 percent of U.S. data breaches are caused by third parties' errors, including "when protected data is in the hands of outsourcers, cloud providers and business partners."[31] The Ponemon Institute's recent *2013 Cost of Data Breach Study*, published in May 2012, indicate that third party errors also increase the average cost of a breach "by as much as $43 per record" according to the new 2013 study[32] – this is very significant considering that the average cost is $188 per record.[33]

The problem also is exacerbated by the reality of the modern business world, which is full of portable devices such as cell phones, laptops, iPads, USB drives, jump drives, media cards, tablets and other devices that facilitate the loss of sensitive information.[34] The Ponemon Institute's recent *2013 State of the Endpoint* study notes that "[o]ne of the top concerns is the proliferation of personally owned mobile devices in the workplace such as smart phones and iPads" and that "data-bearing devices pose a significant security risk to their organization's networks or enterprise systems because they are not secure."[35] Not only are these devices less secure (often unencrypted), but they are often lost or left unattended in unsecured locations. A Ponemon Institute study reports that business travelers lose more than 12,000 laptops per week in U.S. airports alone.[36] Another recent independent study emphasizes "[t]he sheer number of ways in which data can be lost, stolen, or misappropriated."[37]

Perhaps surprisingly, negligence, including employee and third party negligence, is about as likely to result in a data breach as a malicious attack (*e.g.*, misplacing a laptop or tablet or opening email attachments or clicking on links from an unknown source). In its most recent *2013 Cost of Data Breach Study*, the Ponemon Institute reports that 33 percent of the "root cause" of a data breach for United States companies is "human errors."[38] Importantly, however, malicious attacks, which are the "most costly,"[39] are increasing.

While data breaches, DDoS attacks and other types of cyber risks are increasing, state and international laws and regulations governing data security and privacy are proliferating.

Cyber Attack Costs Are on the Rise

As the incidence of cyber attacks escalates, the cost associated with attacks is also increasing. In data breach cases, for example, companies may incur substantial expenses relating to federal,[40] state[41] and international notification requirements alone.[42] In its most recent *2013 Cost of Data Breach Study*, the Ponemon Institute reports that U.S. organizations spend on average $565,020 on post-breach notification.[43]

Companies may face lawsuits seeking damages for invasion of privacy,[44] lost, corrupted or stolen data, loss of use of computers or systems, misappropriation of intellectual property or confidential business information, and other claims. Even if not ultimately successful, such lawsuits can be extremely costly to defend. Companies may also face governmental and regulatory investigations, fines and penalties, damage to brand and reputation, and other negative repercussions from a data breach, including those resulting from breaches of Payment Card Industry Data Security Standards.[45] In addition, companies may incur significant expenses associated with retaining forensics experts, assuaging and attempting to maintain customers and curtailing damage to reputation, including by providing credit monitoring services to affected individuals and retaining public relations consultants.

The Ponemon Institute's *2013 Cost of Data Breach Study* reports that U.S. organizations spend on average $1,412,548 overall in post-breach response costs.[46] The study also found that the average organizational cost of a data breach in 2012 was $188 per record for U.S. companies ($277 in the case of malicious attacks) and the average number of breached records was 28,765.[47] The average total organizational cost of a data breach is $5,403,644.[48] It is important to note that the study does "not include organizations that had data breaches in excess of 100,000 [records] because they are not representative of most data breaches and to include them in the study would skew the results."[49] Yet the incidents of large scale breaches are on the rise. The 2011 high profile attack on the Sony PlayStation Network alone was estimated to cost some $170 million.[50] This does not include potential compensation to claimants. Some experts say that the final tally could exceed $2 billion.[51]

Putting aside liability arising from potentially compromised personally identifiable information ("PII"), many companies have care, custody or control of third party company-confidential information, such as a third party's intellectual property, trade secrets, business plans, customer lists, market information and any other items of information not available to the general public. A data breach that compromises such information can subject a company to liability.

Even in cyber attack cases in which sensitive information is not actually or potentially compromised, a

company may face liability to third parties if its network becomes unavailable to users or serves as a conduit for the transmission of malware. In addition, a company can face significant media-related and other exposure because of employee use of Facebook and similar social sites and feeds (Twitter, LinkedIn, MySpace, etc.), posts to blogs, and personal emails.[52] Companies that provide services that support e-commerce, such as the services provided by internet service providers and software developers, may face liability arising out of, for example, the creation and implementation of software, and the provision of services.

A company also may experience substantial business interruption and related losses if online systems or websites are disabled by – or disabled in order to address – cyber attack. These losses may be in addition to those incurred to repair damage to or replace a company's computers, networks, and data, as well as the costs to update and fix any flaws in its security systems.[53]

In addition, cyber industrial espionage, including through Advanced Persistent Threats ("APTs"), costs U.S. companies billions.[54] These examples of cyber threats are far from exhaustive. The Ponemon Institute's *2012 Cyber Crime Study* found that "the average annualized cost of cyber crime for 56 organizations in [its] study is $8.9 million per year, with a range of $1.4 million to $46 million."[55] This number is up from the $8.4 million average annualized cost reflected in the 2011 survey.[56]

It is clear that attacks and associated costs are on the rise. And insurance can play an important role in mitigating the problem.

(Endnotes)

1. Kevin Robinson-Avila, Cyber attacks on the rise worldwide, ABQJournal (Dec. 17, 2012), *available at* http://www.abqjournal.com/main/2012/12/17/biz/cyber-attacks-on-the-rise-worldwide.html (last visited July 5, 2013).
2. *See* Robert Vamosi, *Twenty-Six Banks Identified in Latest Malware Threat*, Mocana (Oct. 18, 2012), *available at* https://mocana.com/blog/2012/10/18/twenty-six-banks-identified-in-latest-malware-threat/ (last visited July 5, 2013).
3. *See* Michael P. Voelker, After "*Year of the Data Breach,*" *Carriers Increase Capacity, Competition for Cyber Risks*, Property Casualty 360 (Feb. 2, 2012), available at http://www.propertycasualty360.com/2012/02/02/after-year-of-the-data-breach-carriers-increase-ca (last visited July 5, 2013).
4. James Holley and Jeff Spivey, *Prevention Is Over: Assume Your Intellectual Property Is Under Attack*, Wall St. J. (May 27, 2013), *available at* http://blogs.wsj.com/cio/2013/05/27/prevention-is-over-assume-your-intellectual-property-is-under-attack/ (last visited July 5, 2013).
5. *An introduction by General Alexander*, The Next Wave, Vol. 19, No. 4 (2012), *available at* http://www.nsa.gov/research/tnw/tnw194/article2.shtml (last visited July 11, 2013).
6. PwC State of Cybercrime Survey, at 1 (June 2013), *available at* http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-state-of-cybercrime.jhtml (last visited July 11, 2013) (hereinafter "State of Cybercrime Survey").
7. *See Here a Hack, There a Hack, Everywhere a Cyber Attack*, All Things D (Feb. 4, 2013), *available at* http://allthingsd.com/20130204/here-a-hack-there-a-hack-everywhere-a-cyber-attack/ (last visited July 5, 2013) ("It's quickly becoming clear – and the recent batch of attacks has only reinforced it – that pretty much every company under the sun is at risk."); Richard S. Betterley, The Betterley Report, *Cyber/Privacy Insurance Market Survey*, at 7-8 (June 2013), *available at* http://www.irmi.com/products/store/betterley-report.aspx (last visited July 11, 2013) (hereinafter "The Betterley Report") ("there are organizations that have breaches and know it and there are organizations that have breaches and don't know it – yet").
8. *See The Cloud Darkens*, N.Y. Times (June 29, 2011), *available at* www.nytimes.com/2011/06/30/opinion/30thu1.html (last visited July 5, 2013) (opining that "[c]ompanies and the government are unprepared").
9. *Id.*; *see also* Darren Caesar, *Cyber liability insurance: Don't run a business without it*, Network World (July 2, 2010), *available at* http://www.networkworld.com/news/tech/2010/070210-tech-update-1.html?page=3 (last visited July 5, 2013) ("Providing adequate protection against not only rapidly evolving criminal strategies, but also human error or omission is virtually impossible.").
10. 2013 Towers Watson Risk and Finance Manager Survey, at 2 (Apr. 2013), *available at* http://www.towerswatson.com/en/Insights/IC-Types/Survey-Research-Results/2013/04/2013-Risk-and-Finance-Manager-Survey (last visited July 5, 2013) (hereinafter "Risk and Finance Manager Survey").
11. *See* Ponemon Institute, *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age*, at 4 (August 2013), *available at* http://www.ponemon.org/blog/managing-cyber-security-as-a-business-risk-cyber-insurance-in-the-digital-age (last visited Sept. 18, 2013) (hereinafter "Cyber Insurance in the Digital Age") ("Currently, less than one-third of respondents (31 percent) in this study say their organization has a cyber security insurance policy. However, among those companies that do not have a policy 57 percent of respondents say they plan to purchase one in the future."); *Benchmarking Trends: More Companies Purchasing Cyber Insurance*, Marsh (Mar. 14, 2013), *available at* http://usa.marsh.com/NewsInsights/MarshRiskManagementResearch/ID/29870/Benchmarking-Trends-More-Companies-Purchasing-Cyber-Insurance.aspx (last visited July 5, 2013) ("The number of clients of Marsh's FINPRO Practice purchasing cyber insurance increased 33% from 2011 to 2012").
12. Risk and Finance Manager Survey, *supra* note 10, at 3; see also Ty Sagalow, *A Case For Cyber Insurance*, Insurance Thought Leadership (September 22, 2013), *available at* http://www.insurancethoughtleadership.com/articles/a-

case-for-cyberinsurance#axzz2fdtcMcFC (last visited Sept. 22, 2013) ("Despite the increased attention to cyber incidents, most reports indicate only a minority of companies currently purchase cyber-insurance. According to the 'Chubb 2012 Public Company Risk Survey: Cyber,' 65% of public companies surveyed do not purchase cyber insurance, yet 63% of decision-makers are concerned about cyber risk. In a recent Zurich survey of 152 organizations, only 19% of those surveyed have bought cyber insurance despite the fact that 76% of companies surveyed expressed concern about their information security and privacy.").

13. Harvard Business Review Analytic Services, *Meeting the Cyber Risk Challenge*, at 8 (2013), *available at* http://www.computerweekly.com/blogs/public-sector/Meeting%20the%20Cyber%20Risk%20Challenge%20-%20Harvard%20Business%20Review%20-%20Zurich%20Insurance%20group.pdf (last visited July 5, 2013) (hereinafter "Meeting the Cyber Risk Challenge").
14. SEC Division of Corporation Finance, Cybersecurity, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (last visited July 5, 2013). What the SEC offers as "guidance" now might soon become law. Activists and public officials are pressing the SEC to elevate its guidance to companies on the disclosure of actual breaches. In an April 9 letter to the SEC Chairman, Senate Commerce Chairman Jay Rockefeller urged the SEC to step up the requirements on its guidance for companies to disclose information about their ability to defend against attacks on their networks. The letter states in part:

    Investors deserve to know whether companies are effectively addressing their cyber security risks — just as investors should know whether companies are managing their financial and operational risks … Formal guidance from the SEC on this issue will be a strong signal to the market that companies need to take their cyber security efforts seriously.

    The April 9, 2013 letter is available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51 (last visited Sept. 18, 2013).
15. *See* Todd McLees, *2012 Deemed the Year of the Data Breach*, PKWARE (Dec. 6, 2012), *available at* http://www.pkware.com/Blog/2012-deemed-the-year-of-the-data-breach (last visited July 5, 2013).
16. The Identity Theft Resource Center® defines a data breach as "an event in which an individual name plus Social Security Number ("SSN"), driver's license number, medical record or a financial record/credit/debit card is *potentially* put at risk – either in electronic or paper format." *See* http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml#breaches (last visited July 5, 2013) (original emphasis).
17. *See* Ellen Messmer, *The Worst Data Breaches of 2013 (So Far)*, CIO (Apr. 9, 2013), *available at* http://www.cio.com/slideshow/detail/94870 (last visited July 5, 2013); Zack Whittaker, 2012: *Looking back at the major hacks, leaks and data breaches*, ZDNet (Dec. 17, 2012), *available at* http://www.zdnet.com/2012-looking-back-at-the-major-hacks-leaks-and-data-breaches_p3-7000008854/ (last visited July 5, 2013); Shara Tibken, *SecurID Clients Get Jitters*, Wall St. J. (June 8, 2011), *available at* http://online.wsj.com/article/SB10001424052702304906004576371952388757620.html (last visited July 5, 2013).
18. Verizon, *2013 Data Breach Investigations Report*, at 1 (2013), *available at* http://www.verizonenterprise.com/DBIR/2013/ (last visited Sept. 17, 2013).
19. *See* Cass W. Christenson, *Insurance Coverage Regarding Data Privacy, Cloud Computing, and Other Emerging Cyber Risks*, at 1, *available at* 2011 WL 601376, at *1 (Feb. 2011) (Thomson Reuters/Aspatore February 2011) ("virtually every major industry is affected by data breaches").
20. http://www.privacyrights.org/data-breach#CP (last visited Sept. 18, 2013).
21. https://www.privacyrights.org/data-breach-FAQ (last visited Sept. 18, 2013).
22. As with the case with data breaches, DDoS attacks occur off the front page "on a daily basis." Jelena Mirkovic et al., *Understanding Denial of Service*, Ch. 2.5 (Aug. 12, 2005), *available at* http://www.informit.com/articles/article.aspx?p=386163&seqNum=5 (last visited July 5, 2013).
23. Meeting the Cyber Risk Challenge, *supra* note 13, at 1.
24. The Ponemon Institute is a prominent research institute. As described on its website, the "Ponemon Institute conducts independent research on privacy, data protection and information security policy." http://www.ponemon.org/ (last visited July 5, 2013).
25. Ponemon Institute, *2012 Cost of Cyber Crime Study: United States*, at 28 (October 2012), *available at* http://www.ponemon.org/news-2/44 (last visited July 5, 2013) (hereinafter "2012 Cost of Cyber Crime Study").
26. *Id*. at 1.
27. *Id*.; *see also* Ponemon Institute, *Second Annual Cost of Cyber Crime Study*, at 1 (August 2011) (the company experienced "72 successful attacks per week and more than one successful attack per company per week"), *available at* http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf (last visited July 5, 2013) (hereinafter "Second Annual Cost of Cyber Crime Study").
28. Michael R. Crittenden, *A Call to Arms for Banks, Regulators Intensify Push for Firms to Better Protect Against Cyberattacks*, Wall St. J. (June 14, 2013), *available at* http://online.wsj.com/article/SB10001424127887324049504578545701557015878.html?mod=ITP_businessandfinance_0 (last visited July 10, 2013).
29. Malware has been defined as:

    Programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior. Examples include various forms of adware, dialers, hijackware, slag code (logic bombs), spyware, Trojan horses, viruses, web bugs, and worms.

    US-CERT's Control System Security Center, *An Undirected Attack Against Critical Infrastructure*, Case Study Series: Vol 1.2 (Sept. 2005), available at http://ics-cert.us-cert.gov/sites/default/files/undirected_attack0905.pdf (last visited July 5, 2013).

30. Siobhan Gorman, *Iran Renews Internet Attacks on U.S. Banks*, Wall St. J. (Oct. 17, 2012) ("These latest attacks, which investigators say are at least 10 times as potent as the types of denial-of-service attacks hackers have mounted in the past, have disrupted service at even the largest U.S. banks. The highly sophisticated computer attack is using a new cyberweapon called 'itsoknoproblembro[.]'"), *available at* http://online.wsj.com/article/.SB10000872396390444592704578063063201649282.html (last visited July 5, 2013).
31. *See* Ponemon Institute, *2011 Global Cost of Data Breach Study*, at 6 (March 2012), *available at* http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-global.en-us.pdf (last visited Aug. 29, 2013) (hereinafter "2011 Global Cost of Data Breach Study"); *see also* State of Cybercrime Survey, *supra* note 6, at 5 ("Not all companies recognize that supply chain vendors and business partners such as joint ventures, strategic partnerships, and franchisees can have lower – even nonexistent – cybersecurity policies and practices, a situation that can increase cybercrime risks across any entity that partner or supplier touches.").
32. Ponemon Institute, *2013 Cost of Data Breach Study: Global Analysis*, at 12 (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 (last visited July 5, 2013) (hereinafter "2013 Cost of Data Breach Study").
33. *Id.*
34. *See* Kevin P. Kalinich, J.D., AON Network Risk Insurance 2012 Update, *Privacy and Security Exposures and Solutions*, at 4 ("The dramatic increase in use of mobile devices by company employees presents new security threats to corporate networks. Data breaches caused by smartphones are becoming more common than lost or stolen laptops. Though companies have learned to protect their employees' laptops through the use of full-disk encryption, mobile devices are softer targets because they are smaller, making them more vulnerable to loss or theft. And because they are generally turned 'on,' they are constantly vulnerable."), *available at* http://www.aon.com/risk-services/network-security-privacy.jsp (last visited Aug. 4, 2013).
35. Ponemon Institute, *2013 State of the Endpoint*, at 1 (December 2012); *available at* http://www.ponemon.org/blog/2013-state-of-the-endpoint (last visited July 5, 2013); *see also* Office of the National Counterintelligence Executive, Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, at 6 (October 2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (last visited July 11, 2013) (hereinafter "ONCIX Report to Congress") ("[T]he number of devices such as smartphones and laptops in operation worldwide that can connect to the Internet and other networks is expected to increase from about 12.5 billion in 2010 to 25 billion in 2015. This will cause a proliferation in the number of operating systems and endpoints that malicious actors such as foreign intelligence services or corrupt insiders can exploit to obtain sensitive information.").
36. *See Airport Insecurity: The Case of Missing & Lost Laptops*, Ponemon Institute LLC, at 3 (June 2008).
37. Meeting the Cyber Risk Challenge, *supra* note 13, at 4.
38. 2013 Cost of Data Breach Study, *supra* note 32, at 12; *see also* Richard S. Betterley, *Cyber Insurance 3.0: Risks, Rewards and Future Outlook*, at 2 (2013), *available at* http://www.experian.com/innovation/business-resources/cyber-insurance-report-risks-rewards-and-future-outlook.jsp (last visited July 11, 2013) (hereinafter "Cyber Insurance 3.0") ("Data loss can occur because of hackers, but many losses are a result of human error – such as posting or forwarding the wrong file, improperly disposing of private information, or clicking on a link."); Cyber Insurance in the Digital Age, *supra* note 11, at 3 ("the most common data breaches are due to negligence or mistakes that resulted in the loss of business confidential information"); Ponemon Institute, *Third Annual Benchmark Study on Patient Privacy & Data Security*, at 2 (December 2012), *available at* http://www.ponemon.org/library/third-annual-patient-privacy-data-security-study (last visited July 5, 2013) ("[t]he primary cause of breaches in th[e] study is a lost or stolen computing device …followed by employee mistakes or unintentional actions … and third-party snafus.").
    In its 2011 Cost of Data Breach Study published in March 2012, the Ponemon Institute reported that employee negligence was the root cause of 39 percent of breaches involving U.S. companies, while malicious attacks accounted for 37 percent of breaches. *See* 2011 Global Cost of Data Breach Study, *supra* note 31, at 6. The number has been steadily increasing.
39. Malicious attacks are increasing as the root cause of most breaches. In its 2013 Cost of Data Breach Study, a reported 41 percent of breaches involving U.S. companies are caused by malicious attack, while 33 percent are caused by negligence and 26 percent by "system glitch." *See* 2013 Cost of Data Breach Study, *supra* note 32, at 7. This is up from 37 percent reported in the prior study. *See* 2011 Global Cost of Data Breach Study, *supra* note 31, at 6.
40. For example, the Health Information Technology for Economic and Clinical Health ("HITECH") Act includes a national breach notification requirement and extends the Health Insurance Portability and Accountability Act ("HIPAA") to business associates. In addition to current laws, additional legislation has been introduced. For example, the Senate Judiciary Committee has referred to committee the Data Breach Notification Act of 2013, which is "[a] bill to require certain entities that collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information, and for other purposes." The text of the bill is available at http://www.govtrack.us/congress/bills/112/s3333/text (last visited July 5, 2013). This bill was reintroduced as S. 1193 on June 20, 2013.
41. In addition to numerous federal statutes and regulations, forty six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. *See* National Conference of State Legislatures, "State Security Breach Notification Laws" (updated Aug. 20, 2012), *available at* http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last visited July 5, 2013). Additional legislation is pending in various state legislatures. *See* National Conference of

State Legislatures, "2012 Security Breach Legislation" (updated Dec. 13, 2012), *available at* http://www.ncsl.org/issues-research/telecom/security-breach-legislation-2012.aspx (last visited July 5, 2013).

42. For an excellent discussion regarding federal, state, private and international laws and regulations, *see* Peter R. Taffae & M. Damien Magnuson, *What Every Insurance Professional Should Know about Network Security and Privacy Liability*, IRMI White Paper (2012), *available at* https://www.irmi.com/.forms/ssl/contactus.aspx?action=privacy (last visited July 5, 2013).
43. 2013 Cost of Data Breach Study, *supra* note 32, at 16.
44. Although the United States does not have a universal privacy law, a number of different laws respond to different situations and types of data, such as health care data (HIPAA), financial data (Gramm-Leach-Bliley Act), credit information (Fair Credit Reporting Act), and unauthorized access (Computer Fraud and Abuse Act).
45. Current standards can be viewed at https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html. (last visited July 5, 2013). New standards are scheduled to come into effect in November 2013.
46. 2013 Cost of Data Breach Study, *supra* note 32, at 16-17.
47. *Id.* at 1-2. This is slightly down from $194 per record in 2011 (and $214 per record in 2010). *See* 2011 Global Cost of Data Breach Study, *supra* note 31, at 2. The average number of breached records likewise has decreased slightly from 28,349 for U.S. companies. *See id.* at 5.
48. 2013 Cost of Data Breach Study, *supra* note 32, at 5. Other studies indicate that this number is considerably higher. *See, e.g.*, Cyber Insurance in the Digital Age, *supra* note 11, at 4 ("The average financial impact of these security exploits and data breaches experienced by companies represented in this research is $9.4 million.").
49. 2013 Cost of Data Breach Study, *supra* note 32, at 1.
50. See Paul Tassi, Sony Pegs PSN Attack Costs at $170 Million, $3.1B Total Loss for 2011, Forbes - Business (May 23, 2011), *available at* http://blogs.forbes.com/insertcoin/2011/05/23/sony-pegs-psn-attack-costs-at-170-million/ (last visited July 10, 2013).
51. Liana B. Baker & Jim Finkle, *Sony's insurers to help foot bill for data breach: Experts say the final tally could exceed $2 billion, Reuters, available at* http://www.msnbc.msn.com/id/42923992/ns/technology_and_science-games/ (last visited July 10, 2013).
52. *See* Advisen Special Report, *Online Social Networking: A Brave New World of Liability*, at 1 (Mar. 2010), *available at* https://www.advisen.com/downloads/SocialNetworking.pdf (last visited July 11, 2013) ("Millions of people across the world now participate on social network websites such as Facebook, LinkedIn and Twitter. … But social network sites also can be liability minefields, exposing companies to risks as diverse as copyright infringement, consumer fraud and discrimination. Employers also can be held liable for the unsupervised activities of their employees on social network sites.").
53. The Ponemon Institute has identified the following "four general cost activities" associated with "external consequences or costs associated with the aftermath of successful [cyber] attacks," including costs associated with lost information, business interruption, damage to equipment, and loss of customers:
    - Cost of information loss or theft: Loss or theft of sensitive and confidential information as a result of a cyber attack. Such information includes trade secrets, intellectual properties (including source code), customer information and employee records. This cost category also includes the cost of data breach notification in the event that personal information is wrongfully acquired.
    - Cost of business disruption: The economic impact of downtime or unplanned outages that prevent the organization from meeting its data processing requirements.
    - Cost of equipment damage: The cost to remediate equipment and other IT assets as a result of cyber attacks to information resources and critical infrastructure.
    - Lost revenue: The loss of customers (churn) and other stakeholders because of system delays or shutdowns as a result of a cyber attack[.]

    2012 Cost of Cyber Crime Study, *supra* note *25*, at 24. These are in addition to "five internal cost activity centers," which include costs associated with detecting, investigating and mitigating attacks, and repairing system damage in the wake of an attack. *See id.* at 23-24.
54. *See* McAfee Report, The Economic Impact of Cybercrime and Cyber Espionage, Center for Strategic and International Studies, at 3 (July 2013) ("the cost of cybercrime and cyber espionage to the global economy is probably measured in the hundreds of billions of dollars"); ONCIX Report to Congress, *supra* note 35, at 24 (losses to U.S. organizations resulting from economic espionage range between $2 - $400 billion per year). Prior ONCIX reports are available at http://www.ncix.gov/publications/reports/fecie_all/ (last visited July 11, 2013).
55. 2012 Cost of Cyber Crime Study, *supra* note 25, at 1.
56. Second Annual Cost of Cyber Crime Study, *supra* note 27, at 4.