Bloomberg BNA

Privacy and Security Law Report®

Cybersecurity Insurance to Mitigate Cyber-Risks and SEC Disclosure Obligations

BY EDWARD R. MCNICHOLAS

Long a concern of information security specialists, the potential for material economic losses from internet-based intrusion has finally struck a chord in the investment community. Reports of a serious, nearly decade long, external penetration into information intended for only the most senior executives at Nortel Networks Ltd. has been one of the few public examples in which a company's overall value has been compromised. In response to this risk for publicly traded companies, the Securities and Exchange Commission has issued informal guidance (''SEC Guidance'' or ''Guidance'') outlining cybersecurity disclosure obligations, requiring registrants to disclose their vulnerabilities and cyber-incidents and their cybersecurity plans, including what form of insurance, if any, they have.[1]

As the Guidance notes, cybersecurity insurance may serve to mitigate financial risks and limit a company's disclosure obligations by incentivizing companies to comply with best practices and reducing the harm of potential attacks. Comprehensive cybersecurity insurance can minimize the fallout from an actual cyber-incident and can serve to decrease the likelihood of a potential attack. That being said, it seems that only a fraction of companies have insurance to cover losses arising from a cyber-attack. Indeed, many rely upon more general policies, whose coverage over cybersecurity incidents seems to be, at best, unclear. For instance, Sony Corp. of America's insurer, Zurich American Insurance Co., filed suit against Sony alleging that its policy only covered property damages and other tangible losses, not the harm caused from a cyber-attack.[2]

President Obama's Executive Order 13636 (Feb. 12, 2013) has now mandated the development of a national ''Cybersecurity Framework'' and programs to encourage voluntary adoption of the framework, directed the Secretary of Homeland Security to designate those critical infrastructure companies at greatest risk, and created a framework for increased threat information sharing with critical infrastructure companies.[3] In light of these significant changes in the cybersecurity landscape, more companies are looking for insurance products that mitigate their risk and thereby enable them to assure investors that this risk is being appropriately managed.

Cyber-Incidents Raise Awareness in the Investment Community

Adm. Mike Mullen, chairman of the Joint Chiefs of Staff, stated that the United States faces two existential threats. One is nuclear weapons, and the other is cybersecurity.[4] Cybersecurity, however, is not only a national security concern; it is also a financial concern. Companies worldwide lose an estimated $1 trillion per year due to cyber-attacks and data losses.[5] These losses are

Edward R. McNicholas is a partner in Sidley Austin LLP's Washington office and a global coordinator of its Privacy, Data Security, and Information Law practice. The views expressed herein are those of the author personally and do not necessarily reflect the views of any governmental or private entity, client, or association. This article is published for informational purposes only and is not legal advice.

[1] SEC Div. of Corp. Fin., *CF Disclosure Guidance: Topic No. 2* (Oct. 13, 2011) [hereinafter SEC Guidance], *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (10 PVLR 1495, 10/17/11).

[2] First Amended Complaint, *Zurich American Ins. Co. v. Sony Corp. of Am.*, No. 651982 (N.Y. Sup. Ct. Sept. 27, 2011) (10 PVLR 1058, 7/25/11).

[3] Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11738 (Feb. 19, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (12 PVLR 257, 2/18/13).

[4] *See* Karen Parrish, *Mullen Offers 40-Year Perspective on Social, Military Issues*, Am. Forces Press Serv. (Sept. 20, 2011).

[5] McAfee Inc. & Science Applications Int'l Corp., *Underground Economies: Intellectual Capital and Sensitive Corpo-*

not merely breaches of controls over personal information, but also the theft of next-generation designs, bidding strategies, customer lists, and algorithms. A quarter of organizations have suffered a data breach or loss in the last year, averaging more than $1.2 million per incident.[6] According to the Office of the National Counterintelligence Executive, many of the threats come from foreign, perhaps state-supported, economic espionage in securing data pertaining to communications technology, military equipment, civilian and dual-use technologies, health care and pharmaceuticals, agriculture technology, energy and natural resources, and macroeconomic trends and forecasts.[7] In addition, non-state actors threaten to disrupt business operations to fulfill political activist objectives or procure sensitive data for third parties.[8]

The omnipresent threat of cyber-attacks has caused ripples of concern in the financial community. With major corporations like Google Inc., Saudi Arabian Oil Co., and RSA suffering major data breaches in the last few years, investors understand that cybersecurity vulnerabilities translate into palpable financial risks. As Sen. John D. Rockefeller IV (D-W.Va.) and former Secretary of Homeland Security Michael Chertoff recently noted, ‘‘Cybercriminals are stealing American ideas, research, formulas, source code, negotiation plans, designs and blueprints on a massive scale.’’[9] In May 2011, Rockefeller along with four other senators wrote to the SEC to request that it ‘‘develop and publish interpretive guidance clarifying existing disclosure requirements pertaining to information security risk, including material information security breaches involving intellectual property or trade secrets.’’[10] The SEC's response was its first official statement on cybersecurity disclosure. The commissioner stated that existing regulations could require disclosures of actual cyber-attacks and vulnerabilities.[11]

SEC Guidance on Disclosure of Cybersecurity Threats and Incidents

On Oct. 13, 2011, the SEC Division of Corporation Finance issued guidance on disclosure obligations for cybersecurity risks and incidents.[12] While not a binding regulation, the Guidance highlighted existing disclosure obligations, treating cyberthreats as akin to other serious business risks. The Guidance, however, significantly alters the landscape for companies by creating an expectation of disclosure of cybersecurity incidents, and the specter of public and/or private enforcement for failure to disclose risks that materially harm corporate value.

The disclosures recommended by the Guidance are robust. First, consistent with Item 503(c) of Regulation S-K, cybersecurity threats and incidents must be disclosed if they ‘‘are among the most significant factors that make an investment in the company speculative or risky.’’[13] At the least, it would seem that companies must determine cybersecurity risks by examining their vulnerabilities and risk experience, taking into account the frequency of prior incidents and the probability and potential harm of future incidents. The 503(c) obligations require companies to ‘‘adequately describe the nature of the material risk and specify how each risk affects the registrant,’’ avoiding generic descriptions and boilerplate language.[14] The Guidance in particular highlights that companies should describe any outsourced operations that pose unique risks, past security incidents, and potentially undetected threats. And this disclosure must be candid. Referring to an actual material cybersecurity incident as a mere ‘‘risk’’ or ‘‘threat’’ could well constitute a violation of a company's disclosure obligations. Instead, specific material incidents must be disclosed, along with their known and potential costs and the broader consequences on company operations. Without providing a road map for potential hackers and saboteurs, ‘‘registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant.’’[15]

Second, consistent with Item 303 of Regulation S-K and Item 5 of Form 20-F, registrants are required to address cybersecurity risks and incidents in the Management's Discussion and Analysis (MD&A) if they ‘‘represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.’’[16] In the case of an actual, material cyber-attack, the company must describe the stolen information, its effect on operations, liquidity, and financial conditions. If the attack caused a change in reported financial information, projected operating results, or financial conditions, the company must disclose it. If the attack caused a material increase in cybersecurity expenses, this too must be reported.

The Guidance highlights also other areas of disclosure. Consistent with Item 101 of Regulation S-K, if a cyber-incident or vulnerability materially affects a registrant's ‘‘products, services, relationships with customers or suppliers, or competitive conditions,’’ the company is required to disclose this in its ‘‘Description of Business.’’[17] The company is required to describe the incident and its potential impact on each of its reportable segments. In a ‘‘Legal Proceedings’’ disclosure, consistent with Item 103 of Regulation S-K, companies are required to provide the details of material litigation involving cyber-incidents. Consistent with Accounting

rate Data Now the Latest Cybercrime Currency 5 (2011) [hereinafter McAfee & SAIC] (noting that companies lost more than an estimated $1 trillion in 2008).

[6] *Id.* at 15.

[7] Office of the Nat'l Counterintelligence Exec., *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011* 9–10 (Oct. 2011).

[8] *See* McAfee & SAIC, *supra* note 5.

[9] Jay Rockefeller & Michael Chertoff, *A New Line of Defense in Cybersecurity, With Help From the SEC*, Wash. Post, Nov. 17, 2011.

[10] Letter from Sen. John D. Rockefeller IV et al., to Mary Schapiro, Chairman, SEC (May 11, 2011), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-8gtgsb (10 PVLR 736, 5/16/11).

[11] Letter from Mary Schapiro, Chairman, SEC, to Sen. John D. Rockefeller IV (June 6, 2011), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-8hp4dn (10 PVLR 874, 6/13/11).

[12] SEC Guidance, *supra* note 1.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

   ISSN 1538-3423

Standards Codification (ACS) 350-40, the Guidance recommends reporting costs to prevent cyber-attacks in so far as they are related to internal software use. The Guidance also recommends considering ACS 605-50 in reporting expenses associated with outreaching to customers and providing them with incentives to maintain business relations in the event of a cyber-incident. Finally, to the extent that a cyber-attack poses a material risk to a registrant's ability to record, process, summarize, and report information, the company must consider whether it is deficient in disclosure controls and procedures rendering it ineffective in making required disclosures.

Google was one of the first companies to disclose a cyber-attack. In a Form 8-K, Google stated that it ''detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google.''[18] Google disclosed that it and at least twenty other companies were the subject of the attack and identified that the ''primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists.''[19] Security upgrades were undertaken in response to the attack, and Google recommended specific security steps to its customers.

The SEC Guidance stresses that adequate detail be provided regarding such threats and actual incidents and their consequences upon the operations of the company and its financial condition. For instance, following a 2012 hack of an e-commerce company's servers (involving the theft of 24 million customer names and emails), SEC disagreed with the company's initial view that the hack was not significant enough to be disclosed, and then asked the company to ''expand [the cybersecurity] risk factor to disclose that you have experienced cyber attacks and breaches'' and ''to describe [risks of] third-party technology and systems.''[20] Likewise, several other registrants, such as Google, have been asked to expand cybersecurity disclosures.[21]

Cybersecurity Insurance as a Mitigating Factor

Insurance, however, can play a significant role as a mitigating factor affecting companies' disclosure obligations. As the Guidance's calculation of risk for Item 503(c) of Regulation S-K makes clear, the less the probability of future harm and likelihood of cyber-incidents, the less there is to disclose. Considerations that feed into this calculation include the strength of technical solutions to combat cyber-incidents, company policies and employee practices regarding use and disclosure of data, a cybersecurity plan that clearly outlines how employees should respond to cyber-incidents, and the speed with which solutions to data breaches and security incidents can be implemented.

[18] Google Inc., *SEC Form 8-K*, Comm'n File No. 0-50726 (Jan. 12, 2010).

[19] *Id.*

[20] Letter from William H. Thompson, Accounting Branch Chief, SEC, to Shelly Reynolds, Vice President and Worldwide Controller, Amazon.com, Inc. (Apr. 18, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1018724/000000000012019757/filename1.pdf.

[21] *See* Linda Sandler, *SEC Guidance on Cyber-Disclosure Becomes Rule for Google*, Bloomberg, Aug. 29, 2012, http://www.bloomberg.com/news/2012-08-29/sec-guidance-on-cyber-disclosure-becomes-rule-for-google.html.

Insurance, however, is certainly of material importance to this risk calculus. The SEC Guidance indeed stresses that a company must disclose a ''[d]escription of relevant insurance coverage.''[22] Comprehensive cybersecurity insurance can reduce a company's cybersecurity vulnerabilities, thereby mitigating its disclosure obligations. But it matters a great deal what type of coverage such insurance provides.

Most commercial insurance policies are limited to harms that arise from damage to tangible property and, therefore, do not cover cyber-incidents. Depending upon the size of a company, the company's business sector, the sensitivity of the company's data, and the type of security threats faced by the company, the type of insurance necessary for adequate coverage varies widely.

Cybersecurity insurance generally breaks down into two categories. First-party coverage can include the damages directly associated with intellectual property theft, data loss and destruction, hacking, and denial-of-service attacks, including the immediate technical and forensic expenses associated with detecting the breach and its source. Third-party coverage can include public relations services to coordinate outreach to affected customers and mitigate fallout in the broader community, legal expenses arising from lawsuits brought by customers or third-party businesses, credit-monitoring and fraud-resolution services for the affected individuals and companies, and the associated penalties and fines imposed by domestic and international regulations.[23]

Cybersecurity insurance can thus play a significant positive role in incentivizing companies to adopt best practices, thereby reducing vulnerabilities before coverage begins. To be eligible, prudent insurers require sufficient documentation or audits demonstrating that technology solutions have been implemented to combat cyberthreats, including such fundamental components as a robust firewall, encryption of highly-sensitive data, and strong password protections for access to company servers and email accounts.

Significantly, insurance policies can also offer discounts to those who are better secured. And there is an emerging role for consultants in helping to prepare companies for cybersecurity insurance reviews and rating. As such, companies are incentivized to reduce cybersecurity vulnerabilities to achieve immediate cost savings.

The benefits to publicly traded companies from a robust cybersecurity insurance policy are two-fold. First, cybersecurity insurance coverage reduces the potential harm to companies by reducing the risks associated with the financial fallout from cyber-attacks. In addition to the decrease in financial vulnerability, there is an immediate concomitant increase in security derived from compliance with best practices, which evolve through an interaction between insurance policies, ever-changing cyberthreats, and company practices and technology solutions. The reduced financial vulnerability and increased security produce a second benefit in the form of reduced disclosure obligations. Under Item

[22] SEC Guidance, *supra* note 1.

[23] *See, e.g.*, Nicole Perlroth, *Insurance Against Cyber Attacks Expected to Boom*, N.Y. Times, Dec. 23, 2011; J.D. Harrison, *Cyber Security Insurance: What Small Businesses Need to Know*, Wash. Post, Dec. 28, 2011.

503(c)'s risk formula, insurance reduces the potential harm of a cybersecurity incident, while at the same time compliance with best practices reduces the probability of attack. In the end, the financial risk of a cybersecurity incident is reduced, meaning that the obligation to disclose material cybersecurity threats is mitigated.

Where Government Is Headed

As the president's executive order demonstrated, the SEC Guidance was merely a first step in the direction of greater disclosures of cyber-incidents and risks. Over 50 cybersecurity legislative proposals have been made in Congress in the past few sessions.[24] And multiple cybersecurity bills remain active on Capitol Hill despite the general legislative morass.

The bottom line is that companies operating in the modern globally networked economy will have to disclose more about their cybersecurity plans, incidents, and threats. Accordingly, it is essential for companies to engage in a detailed assessment of their cybersecurity risks and to develop plans to respond to cybersecurity incidents in a manner that complies with all of their legal obligations. Cybersecurity insurance is one component of an effective cybersecurity system that companies will have to disclose to reduce their risk, ensure stability, and increase investor confidence.

[24] The Constitution Project, *Recommendations for the Implementation of a Comprehensive and Constitutional Cybersecurity Policy* 23 (Jan. 27, 2012).

ISSN 1538-3423