Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Gov't Must Integrate Insurance With Cybersecurity

Law360, New York (July 02, 2014, 11:22 AM ET) --

Cyber intrusions and attacks have increased dramatically over the last few years, exposing sensitive information, disrupting operations and imposing high costs on business and the economy. In an effort to encourage a stable, safe and resilient cyberspace, President Obama issued Executive Order 13636, which called for the establishment of a voluntary set of security standards for critical infrastructure industries. In response, in February 2014, the National Institute of Standards and Technology issued the first version of the "Framework for Improving Critical Infrastructure Cybersecurity."

Unfortunately, the topic of insurance is notably absent from the framework, and other governmental efforts to address cybersecurity similarly fail to sufficiently address the subject. Because insurance coverage is integral to an organization’s risk management strategy, the government’s cybersecurity initiatives should place stronger emphasis on cyber coverage.

J. Wylie Donald

NIST’s Cybersecurity Efforts

The NIST’s focus on cybersecurity precedes the recent issuance of President Obama's executive order and the framework. In 2011, the NIST published "Managing Information Security Risk, Special Publication 800-39," its "flagship" document, which was "intended to address only the management of information security-related risk derived from or associated with the operation and use of information systems or the environments in which those systems operate."[1] The NIST explained that the guidance was necessary because, in the past, “senior leaders/executives … had a very narrow view of information security either as a technical matter or in a stovepipe that was independent of organizational risk and the traditional management and life cycle processes.”[2] In sum, senior management needed to work with information technology professionals in order to sufficiently address cyber risk.

The guidance advises that “[r]isk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization.”[3] Specifically, an organization must engage in a “comprehensive process” that frames, assesses, responds to and continuously monitors risk.[4]

With regard to risk response, the guidance recognizes that an organization has five potential responses:

(1) acceptance, (2) avoidance, (3) mitigation, (4) transfer or (5) sharing.[5] A business may accept risk by choosing to use an unfiltered Internet connection. During the period of connectivity, the business may mitigate risk by searching for malware. Risk may be avoided by terminating an unfiltered connection. The guidance provides examples of how these responses may apply in practice. Unfortunately, however, the guidance fails to provide an example concerning risk transfer, which would have included a discussion of insurance coverage.

The guidance goes on to explain the concept of risk transfer, generally, as follows: "Risk transfer shifts the entire risk responsibility or liability from one organization to another organization (e.g., using insurance to transfer risk from particular organizations to insurance companies)."[6] The guidance also provides that "[r]isk sharing or risk transfer is the appropriate risk response when organizations desire and have the means to shift risk liability and responsibility to other organizations."[7] However, this general overview of the concept of risk transfer is the most substantive mention of the topic in the guidance.

The NIST has a vast library of cybersecurity-related publications.[8] While it is possible that insurance is occasionally mentioned, its significance is undoubtedly minuscule. This is evidenced by the 2014 Framework, the NIST's "voluntary how-to guide for organizations in the critical infrastructure community to enhance their cybersecurity."[9] Consonant with the prior treatment, the topic of risk transfer was given even less attention in the framework than in the guidance.

DHS' Cybersecurity Efforts

The NIST is not the only federal agency addressing cybersecurity. For example, in 2011 the U.S. Department of Homeland Security rolled out the "Blueprint for a Secure Cyber Future," a report "designed to protect [the nation's] most vital systems and assets and, over time, drive fundamental change in the way people and devices work together to secure cyberspace."[10] Subsequently, DHS collaborated with Carnegie Mellon University and, in 2014, issued the "Cyber Resilience Review Self-Assessment Package." The DHS website explains that "the CRR is a no-cost, voluntary, nontechnical assessment to evaluate an organization's operational resilience and cybersecurity practices. … The CRR assesses enterprise programs and practices across a range of 10 domains including risk management, incident management, service continuity and others."[11]

The CRR identifies five risk management goals: (1) develop a strategy for identifying, analyzing and mitigating risks, (2) identify risk tolerances and establish the focus of risk management activities, (3) identify risks, (4) analyze those risks and assign a disposition (i.e., risk response), and (5) mitigate and control the risks to assets and services.[12] The CRR sets forth the following options as dispositions: avoid, accept, monitor, research or defer, transfer, and mitigate or control. Notwithstanding the identification of the risk management "domain," like the guidance, risk transfer is mentioned only cursorily. The CRR simply explains as follows: "Risks that are to be transferred must demonstrate a clear and willing party (organization or person) able to accept the risk."[13] There is nothing else. In sum, like the guidance, the CRR ignores the importance of insurance with regard to risk management.

Of the government's initiatives, DHS' "National Protection and Programs Directorate" arguably paid the most attention to cyberinsurance. The NPPD assembled a workshop and two roundtable discussions attended by a diverse group of individuals from the private and public sectors, for the purpose of discussing cybersecurity insurance.[14] The most recent roundtable included participants from insurance companies, information technology experts and risk managers, all of whom focused on the following question: "How do cost and benefit considerations inform the identification of not only an organization’s top cyber risks but also appropriate risk management investments to address them?”[15]

In an effort to answer this question, three representatives from health care organizations were asked to describe a cyber incident they experienced, explain how the organization managed the incident and provide the lessons learned from that experience.[16] The discussion was supposed to cover cyberinsurance from a practical standpoint, but unfortunately, these representatives did not possess the insurance-related experience necessary to enable a truly meaningful discussion on the topic. One organization, which was described as a “‘highly federated and distributed international enterprise that include[d] 260 operating companies located in some 60 countries,”[17] had not invested in cybersecurity insurance.[18] The representatives from the other organizations had little more involvement with cyber coverage. One representative viewed cybersecurity insurance as appropriate for “catastrophic” situations, and another representative had never submitted a claim for cyber coverage and “was dubious about the level of reimbursement his organization would receive in the event of a breach.”[19]

In the end, participants generally agreed that cybersecurity professionals and insurers “would benefit from a sustained dialogue,” but other than recommending further conversation on advancing “the cybersecurity insurance market’s ability to cover cyber-related critical infrastructure loss,” further talking points were not suggested.[20]

Benefits of Insurance

Insurance is commonly understood as providing a method of recovery for loss. To be certain, an indemnity payment is an ascertainable benefit to an organization that has suffered a loss. But cyberinsurance provides another, far-reaching benefit that seems to be overlooked in this arena: Insurance may increase an organization’s cyber preparedness, thereby minimizing the risk potential.

Specifically, insurance companies engage clients heavily during the underwriting process, typically using extensive questionnaires and speaking directly with clients to understand vulnerabilities and the adequacy of risk management controls. If an insurer is dissatisfied with a client’s systems and operations, the client must make corrections or coverage will not be issued. In essence, the involvement of insurance companies at the outset may improve an organization’s security program by requiring improvements that are necessary to reduce the risk of cyber attack.

Why is Insurance Missing from Government Dialogue?

Despite the participation of multiple departments of government and various personnel from the public and private sectors (including insurance professionals), there is a lack of clarity in terms of the role of insurance with regard to cybersecurity risk management. Why is insurance missing from the discussion?

First, when the focus is on governmental activities, it is understandable that insurance is not a prominent part of the discussion. As the guidance acknowledges, “self-initiated transfers of risk by public-sector organizations (as typified by purchasing insurance) are generally not possible.”[21]

Another reason may be a bias against insurance. The guidance states: “It is important to note that risk transfer reduces neither the likelihood of harmful events occurring nor the consequences in terms of harm to organizational operations and assets, individuals, other organizations or the nation.”[22] However, this position conflicts with the risk-framing concept and fails to appreciate the benefits that result from the underwriting process discussed above.

Last, there may be a perception that insurance increases the opportunity for “moral hazard” (i.e., because a particular risk is insured, an organization may take fewer steps to secure itself against the risk). But this argument also disregards the underwriting process and ignores the fact that moral hazard may be controlled, as seen with other lines of coverage.

Conclusion

Historically, the absence of cyber coverage from an organization’s insurance program may have been inadvertent rather than intentional. A communication breakdown between information technology personnel who focused on the technical aspects of cybersecurity, and the senior management who oversaw the purchase of insurance, may have contributed to the sparse demand for cyber coverage in the insurance marketplace. Without the demand, and given scant actuarial data, insurers previously may have been ambivalent about issuing this line of coverage. This is undergoing change.

We believe the government’s initiatives are successfully bringing the topic of cybersecurity to the forefront of business operations by bridging the information gap between information technology and senior management. However, the initiatives do not go far enough. The guidance acknowledges that:

Agile defense assumes that a small percentage of threats from purposeful cyber attacks will be successful by compromising organizational information systems through the supply chain, by defeating the initial safeguards and countermeasures (i.e., security controls) implemented by organizations, or by exploiting previously unidentified vulnerabilities for which protections are not in place.[23]

Despite an organization’s best efforts to avoid cyber loss, the risk is as real as any property or liability risk. As a result, cyber coverage should be included in an organization’s insurance program, and the topic deserves more prominent focus by the government. Additionally, the insurance industry should take an active role in the development and implementation of cybersecurity standards, as it did over a century ago when fire insurance organizations first released a set of sprinkler installation rules, which led to the creation of our modern fire safety codes and standards.[24]

—By J. Wylie Donald and Jennifer B. Strutt, McCarter & English LLP

J. Wylie Donald is a partner in McCarter & English's Wilmington, Delaware, office, where he is a member of the firm's insurance coverage and cybersecurity and data practice groups.

Jennifer Strutt is an associate in McCarter & English's Stamford, Connecticut, office, where she is a member of the firm's insurance coverage practice group.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] National Institute of Standards & Technology, Special Publication 800-39, Managing Information Security Risk, at vii (Mar. 2011), http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf (hereinafter “NIST 800-39”).

[2] NIST 800-39 at 2.

[3] NIST 800-39 at 6.

[4] NIST 800-39 at 6.

[5] NIST 800-39 at 42.

[6] NIST 800-39 at 43.

[7] NIST 800-39 at 43.

[8] See NIST website, http://www.nist.gov/publication-portal.cfm (topic: Cybersecurity).

[9] Press Release, The White House, Launch of the Cybersecurity Framework (Feb. 12, 2014), http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework.

[10] Department of Homeland Security, Blueprint For A Secure Cyber Future, at iii (November 2011), http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

[11] DHS website: http://www.us-cert.gov/ccubedvp/self-service-crr.

[12] DHS, Cyber Resilience Review; Self-Assessment Package, at 26 (February 2014), http://www.us-cert.gov/sites/default/files/c3vp/csc-crr-self-assessment-package.pdf (hereinafter "CRR").

[13] CRR at 94.

[14] See DHS website: http://www.dhs.gov/publication/cybersecurity-insurance.

[15] National Protection & Programs Directorate DHS, Cyberinsurance Roundtable Readout Report, Health Care & Cyber Risk Management: Cost/Benefit Approaches, at 2 (February 2014), http://www.dhs.gov/sites/default/files/publications/Cyber%20Insurance%20Use%20Case%20Readout%20Report.pdf (hereinafter "Readout Report").

[16] Readout Report at two. The NPPD reported that the three representatives "hailed from a variety of organizations" and that "each presented very different cyber risk management use cases." Readout Report at three. However, only the health care industry was represented. See Readout Report at two. Any future discussions should involve chief information security officers or risk management equivalents from diverse sectors.

[17] Readout Report at 30.

[18] Readout Report at 4.

[19] Readout Report at 4.

[20] Readout Report at 4.

[21] NIST 800-39 at 43.

[22] NIST 800-39 at 43.

[23] NIST 800-39 at H-4 (emphasis added).

[24] National Fire Protection Association, History Of The NFPA Codes & Standards-Making System, http://www.nfpa.org/~/media/Files/Codes%20and%20standards/Standards%20development%20process/HistoryNFPACodesStandards.pdf.
