Insurance Coverage Litigation
March-April 2014, Vol. 24 No. 2

The Unsatisfactory Insurance Aspect of the Federal Government's Cybersecurity Initiatives

By J. Wylie Donald and Jennifer Black Strutt

There has been a furor of activity by the federal government as it grapples with the cyber security threat. Guidance documents roll out, an executive order has been issued, and a Cybersecurity Framework has been set down. In all of this, insurance, the tool that is used in nearly all other circumstances where there is an exposure that threatens an organization's existence, gets short shrift or no shrift at all. The article examines the government's steps into cybersecurity and how insurance is addressed. It then offers some thoughts on what to do about it.

According to the National Institute of Standards and Technology (NIST), "[s]enior leaders/executives in modern organizations are faced with an almost intractable dilemma—that is, the information technologies needed for mission/business success may be the same technologies through which adversaries cause mission/business failure."[1] In today's vernacular, this describes the battlefield for cyber war.

With great fanfare, the Obama administration has mustered the nation's defenses against cyber attack.[2] Frustrated by a lack of achievement in the Congress, in 2013 President Obama, through Executive Order 13636,[3] called for the establishment of a voluntary set of security standards for critical infrastructure industries. This led to the release of the Cybersecurity Framework[4] one year later, which built on NIST work that had been released earlier.

One hesitates to criticize a project that has painstakingly sought to engage stakeholders across the nation. Yet, a uniform feature of the nation's commercial landscape is insurance coverage, to which the government's cyber initiatives give short shrift or no shrift at all. This should be fixed; fortunately, the NIST protocols provide a place to do so, and the place to start is NIST's 2011 publication, *Managing Information Security Risk*, NIST's "flagship document in the series of information security standards and guidelines."[5]

This article outlines the risk management practices recommended by the guidance and comments on those practices. It concludes that the government could do much better. Insurance is a fundamental part of an organization's risk response, and, notwithstanding the government's apparent lack of interest, prepared organizations must pursue their full set of risk management options—including insurance.

The Guidance: An Overview

The need for the guidance was paramount because, as the guidance itself observes, "[h]istorically, senior leaders/executives have 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."[6] The effect of this limited perspective was a lack of recognition "of how information security risk, like other organizational risks, affects the likelihood of organizations successfully carrying out their missions and business functions."[7] Thus, to address cyber risks, it was not enough to get the message only to the information technology professionals; if senior management was not engaged, the problem could not be solved.[8] Simply stated:

> The objective is to institutionalize risk management into the day-to-day operations of organizations as a priority and an integral part of how organizations conduct operations in cyberspace—recognizing that this is essential in order to successfully carry out missions in threat-laden operational environments.[9]

To assist all involved, the guidance lays out some risk management basics. First, one needs to understand risk management's scope. It is a comprehensive process that requires organizations to (1) frame risk, (2) assess risk, (3) respond to risk, and (4) monitor risk on an ongoing basis.[10] As defined in the guidance, "[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."[11]

Framing risk involves making explicit the risk perceptions that organizations routinely use in making both investment and operational decisions.[12] Organizations must figure out the assumptions and constraints that contribute to informing and establishing an organization's risk tolerance, which necessarily requires identifying the organization's priorities and recognizing the risk trade-offs. For example, conducting operations in the "cloud" may optimize software and hardware expenditure and avoid maintenance headaches (both priorities), but it necessarily means a loss of control (a trade-off).

Having established the risk framework, the organization must closely assess its risks and activities. In that assessment, the threats and vulnerabilities facing the organization are identified, and the resulting harms and impacts on the organization analyzed. A critical part of that analysis is a determination of the likelihood and extent of any impact.[13]

Once risk assessment is complete, the organization must develop, evaluate, select, and then implement among alternative courses of action.[14] The choices facing an organization are simple: It can accept, avoid, mitigate, share, or transfer a risk.[15]

Finally, the organization must monitor all of the above: verifying threats and vulnerabilities, determining effectiveness of responses, and identifying changes within the organization or externally that affect its ability to protect itself from cyber risk.[16]

To implement these ideas, the guidance breaks down an organization into three "tiers" with effective communications between them: (1) the organization level, (2) the mission/business process level, and (3) the information system level.[17] Tier 1 implements the "risk framing" concept described previously, which in turn determines the assessment and response outcomes. An example may make this concrete. As stated in the guidance,

> Tier 1 provides a prioritization of missions/business functions which in turn drives investment strategies and funding decisions, thus, affecting the development of enterprise architecture (including embedded information security architecture) at Tier 2 and the allocations and deployment of management, operational, and technical security controls at Tier 3.[18]

The guidance suggests locating the quirkily named "risk executive (function)"—a single individual or office or group that provides the needed "comprehensive, organization-wide approach to risk management"—in Tier 1.[19] The risk executive (function) serves to facilitate communications among the tiers and also to provide oversight of the risk management activities of Tiers 2 and 3.[20]

Among other things, the risk executive (function) works with senior management to "[e]stablish risk management roles and responsibilities."[21] It also strives to "[d]evelop and implement an organization-wide *risk management strategy* that guides and informs organizational risk decisions (including how risk is framed, assessed, responded to, and monitored over time)," as well as to perform numerous technical roles.[22]

Chapter 3 of the guidance describes in more detail the risk framing, assessment, response, and monitoring elements. Germane to this discussion is the analysis of risk response. As noted above, an organization facing a particular risk has five potential responses: acceptance, avoidance, mitigation, transfer, or sharing.[23] The guidance provides a simple example of how these ideas might apply in practice. In an emergency situation, an organization might accept risk by using an unfiltered connection to the Internet.[24] When the emergency has passed, risk is avoided by terminating the connection. During the period of connection, risk is mitigated by actively searching for malware and monitoring system operations. In the long-term, risk is mitigated by anticipating the need for an emergency connection and developing appropriate controls beforehand. Absent from the example is any discussion of risk transfer; had it done so, it could have included the procurement of an insurance policy addressed to the cause of the emergency or to recovering from cyber harms.

A subsequent paragraph addresses risk transfer: "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)."[25]

A partial risk transfer is the concept of risk sharing, which "shifts a portion of risk responsibility or liability to other organizations (usually organizations that are more qualified to address the risk)."[26] Risk 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."[27] Notwithstanding, other than in that single paragraph, there are no references to insurance in the guidance.

Why Is Insurance Missing from the Guidance?

There are probably at least three reasons for the lack of any substantive information concerning insurance in the guidance. First, as the guidance acknowledges, "self-initiated transfers of risk by public sector organizations (as typified by purchasing insurance) are generally not possible."[28] Because the guidance is focused on governmental activities—as evidenced by the references (over 75 percent of which relate to government topics)[29] and the authors (not one of which is an insurance company or risk management group)[30]—it is understandable that insurance is not paramount in the discussion.

Second, a caveat in the guidance warns users that the guidance is not the end of the discussion: "[T]he risk management guidance described herein is complementary to and should be used as part of a more comprehensive Enterprise Risk Management (ERM) program."[31] In the private sector, it may be axiomatic that an ERM program includes cyber insurance.

Last, there is (in our view) a substantial 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."[32] We would submit that this fails to appreciate how insurance is implemented and its effect. Further, it is inconsistent with the risk framing concept established as central to a cyber risk program. These ideas are discussed further below.

The Framework and the Department of Homeland Security's Efforts

For whatever reason, the guidance's discussion and analysis of the transfer option is less than robust, and it has not improved. Less than three years after the promulgation of the guidance, NIST issued the Cybersecurity Framework. On February 12, 2014, the White House announced:

> Today the Obama Administration is announcing the launch of the Cybersecurity Framework, which is the result of a year-long private-sector led effort to develop a voluntary how-to guide for organizations in the critical infrastructure community to enhance their cybersecurity. The Framework is a key deliverable from the Executive Order on "Improving Critical Infrastructure Cybersecurity" that President Obama announced in the 2013 State of the Union.[33]

The framework was in the making for over a year. Under the auspices of NIST, workshops were set up across the country.[34] Based on the perspectives shared at those meetings, as well as submissions from government and industry, a preliminary framework[35] was drafted. Then, after a 45-day public comment period, the final version was released. The framework "enables organizations—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the *principles and best practices of risk management* to improving the security and resilience of critical infrastructure."[36] But notwithstanding this exhortation, the guidance's acknowledgement that risk transfer is an "appropriate risk response" and even a filed comment critical of the draft framework's omission of any discussion of insurance, the final version remained silent on the topic. Nor have other government papers filled the void.

Contemporaneously with the issuance of the framework, the Department of Homeland Security (DHS) issued *Cyber Resilience Review (CRR); Self-Assessment Package*, which again ignores the valuable role played by insurance.[37] The *Cyber Resilience Review* is the result of a collaboration between DHS and Carnegie Mellon University. As explained on the DHS webpage, "the CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices … The CRR assesses enterprise programs and practices across a range of ten domains *including risk management*, incident management, service continuity, and others."[38]

In the risk management domain, five goals are identified: (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, and (5) mitigate and control the risks to assets and services.[39] "Assign a disposition" is the 2014 equivalent to the 2011 guidance's "response." Somewhat different options are available as "dispositions": avoid, accept, monitor, research or defer, transfer, and mitigate or control. Once again, "transfer" is an alternative, but all that is stated is: "Risks that are to be transferred must demonstrate a clear and willing party (organization or person) able to accept the risk."[40] This is not particularly helpful.

To date, the federal government's most significant focus on cyber insurance may result from DHS's National Protection and Programs Directorate (NPPD), which convened a workshop and two roundtable discussions among private and public sector stakeholders for the purpose of examining the current state of the cybersecurity insurance market.[41] During the most recent roundtable, insurance carriers, risk managers, and information technology/cyber experts (among others) focused on "a fundamental yet unanswered question that had arisen over the course of the prior discussions: 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?"[42]

Specifically, the NPPD asked three representatives from health care organizations to describe an actual cyber incident they experienced, how their organizations managed the incident, and lessons learned.[43] The presentations were supposed to address, in part, what role cybersecurity insurance plays in the organization's cyber risk management strategy.[44] Unfortunately, the three representatives "were somewhat ambivalent about the role of cybersecurity insurance within their organizations' cyber risk management strategies."[45] In fact, one representative saw cybersecurity insurance as a way to address only "catastrophic" situations, while another representative had never submitted a claim under its cyber policy and "was dubious about the level of reimbursement his organization would receive in the event of a breach."[46] The third organization, which was described as a "'highly federated and distributed international enterprise' that include[d] 260 operating companies located in some 60 countries,"[47] had not even invested in cybersecurity insurance, and its representative believed that resources were better spent on risk mitigation rather than risk transfer options.[48]

The participants at the NPPD Cyber Insurance Roundtable generally agreed that cybersecurity professionals and insurers "would benefit from a sustained dialogue,"[49] but there did not appear to be a consensus in terms of the role that insurance should play regarding cybersecurity. One insurer actually cautioned that cyber insurance "should not be considered an incentive that will somehow encourage critical infrastructure owners to use the Cybersecurity Framework called for in Executive Order 13636."[50] According to that insurer, carriers will assess the impact of the framework on cyber loss, and based on those experiences, carriers may incorporate into their policies the framework's elements that result in better cybersecurity outcomes.[51]

In sum, the result of these governmental initiatives is a lack of clarity in terms of the appropriate application of cyber insurance to ERM and cybersecurity.

Insurance Should Play a Pivotal Role Regarding Cybersecurity

Every cyber insurance program of which we are aware requires a prospective insured to report on its systems and operations to the insurer in the policy application. Areas where the insurer is dissatisfied must be corrected, or coverage will not be issued. In other words, by requiring improvement in an organization's cyber preparedness, an insurance company necessarily reduces the likelihood of harmful events occurring and may, through those improvements, reduce the harmful consequences of a successful cyber attack.

Undoubtedly, some will assert that insurance increases the opportunity for moral hazard to apply, thus increasing the likelihood of a harmful event. That is, because the risk is insured, the insured organization will take fewer steps to ensure the insured risk does not materialize. While that is possible, it assumes that moral hazard cannot be avoided or mitigated. The trillions of dollars in insured risks throughout the world in a wide variety of areas demonstrate that moral hazard is a controllable feature.

Moreover, it is important to recognize that an organization's prioritization of business functions "drives investment strategy and funding decisions."[52] In other words, central to how an organization addresses cyber risk are the dollars available. Indeed, "one aspect of the total impact to organizations is the cost of recovery from a loss of confidentiality, integrity, or availability."[53] Necessarily, opportunities to make more dollars available to support the organization's priorities—such as the purchase of insurance—must be carefully considered in establishing an organization's cyber response.

Last, it must be recognized that an unavoidable part of every insurance risk transfer is risk acceptance. This comes in the forms of deductibles and policy limits; that is, losses below a certain value, as well as those above a certain value, are retained by the insured. But it also includes the very terms and conditions of the insurance contract, which determine whether the materializing risk is covered. Exclusions limiting coverage for risks are the simplest example of this, but one must acknowledge that definitions, reporting obligations, insuring agreements, and a whole host of other terms can also work contractually to limit the actual transfer of risk. Thus, implicit in every decision to insure a risk is also a decision to accept some portion of that risk.

All of these features of insurance matter in preparing an organization's response to cyber attacks (and other cyber problems).

Conclusion

Almost 10 years ago, one of the authors was a member of the Maryland CIO Roundtable. He was the only lawyer in a group of chief information officers. At the time, cyber liability insurance was much less accepted than it is today (and even today, its market penetration is not as pronounced as many think it should be). Members were pressed as to why their firms did not purchase cyber liability insurance. The answer was simple: Their job was passwords, firewalls, anti-intrusion software; insurance was the job of the chief financial officer (CFO). And when CFOs were asked outside the roundtable, their answer was equally simple: The information technology department has never asked for insurance. This same schism is apparent in the framework. Insurance is simply omitted.

To be fair, insurance is not rejected by the government's initiatives, but at best it is hidden in jargon as a "response" or a "disposition." This should be changed. The guidance posits a reality where insurance should be fundamental.

> 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.[54]

This statement, when stripped of jargon, makes clear that even organizations that prepare for cyber attacks will not be 100 percent successful. In the non-cyber world, where there are losses that are likely to occur, that would mean insurance must be brought into the game. In the cyber world, at least as described by the government, insurance is largely ignored.

The government's cyber initiatives expressly preserve the importance of an organization's own risk management program. As the framework itself states, it "complements, and does not replace, an organization's risk management process and cybersecurity program."[55] Organizational leaders and specifically those in an organization's risk executive (function) should keep this at the forefront of their planning and ensure that the risk protection utilized to address the manifold other risks facing the organization—insurance—is also brought to bear in connection with the cyber risk. As Michelle Kerr and Joel Berg observed in a recent issue of *Risk & Insurance*: "In every industry and at every company size, cyber risk is a foundation-level exposure that every business must confront—one that must be viewed with the same gravity as a company's property, liability or workers' comp risks."[56] All of those risks are dealt with through insurance; cyber risk deserves no less.

Keywords: litigation, insurance, coverage, cybersecurity, cyber threat, cyber liability, NIST, Framework, ERM

J. Wylie Donald is a partner in the Wilmington, Delaware, office of McCarter & English, and Jennifer Black Strutt is an associate in the firm's Stamford, Connecticut, office.

[1] Nat'l Inst. of Standards & Tech., Special Publication 800-39, *Managing Information Security Risk*, at H-1 (Mar. 2011) [Hereinafter NIST 800-39].
[2] As useful a definition as any is one put out by NIST: "Cyber Attack—An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information." NIST 800-39, at B-3. Cyberspace is "the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." NIST 800-39, at B-3.
[3] Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).
[4] Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0) (Feb. 12, 2014).
[5] NIST 800-39, at 4.
[6] NIST 800-39, at 2.

[7] NIST 800-39, at 2.

[8] NIST 800-39, at 14 ("To be effective, organization-wide risk management programs require the strong commitment, direct involvement, and ongoing support from senior leaders/executives.").

[9] NIST 800-39, at 14.

[10] NIST 800-39, at 6.

[11] NIST 800-39, at 6.

[12] NIST 800-39, at 6.

[13] NIST 800-39, at 7.

[14] NIST 800-39, at 7.

[15] NIST 800-39, at 7.

[16] NIST 800-39, at 7.

[17] NIST 800-39, at 9.

[18] NIST 800-39, at 9.

[19] NIST 800-39, at 12–14.

[20] NIST 800-39, at 14.

[21] NIST 800-39, at 14.

[22] NIST 800-39, at 12–13.

[23] NIST 800-39, at 42.

[24] NIST 800-39, at 42.

[25] NIST 800-39, at 43.

[26] NIST 800-39, at 43.

[27] NIST 800-39, at 43 (emphasis added).

[28] NIST 800-39, at 43.

[29] NIST 800-39, app. A.

[30] NIST 800-39, at v.

[31] NIST 800-39, at 3.

[32] NIST 800-39, at 43.

[33] Press Release, The White House, Launch of the Cybersecurity Framework (Feb. 12, 2014).

[34] *See* Nat'l Inst. of Standards & Tech., Cybersecurity Framework—Workshops and Events.

[35] Nat'l Inst. of Standards & Tech., *Improving Critical Infrastructure Cybersecurity, Executive Order 13636: Preliminary Cybersecurity Framework* (Oct. 22, 2013).

[36] Press Release, *supra* note 33 (emphasis added).

[37] Dep't of Homeland Sec., *Cyber Resilience Review (CRR); Self-Assessment Package* (Feb. 2014) [Hereinafter CRR].

[38] Dep't of Homeland Sec., Cyber Resilience Review (CRR) (webpage) (emphasis added).

[39] CRR, at 26.

[40] CRR, at 94.

[41] *See* Dep't of Homeland Sec., Cybersecurity Insurance.

[42] Nat'l Prot. & Programs Directorate, Dep't of Homeland Sec., *Cyber Insurance Workshop Readout Report, Health Care & Cyber Risk Management: Cost/Benefit Approaches* 2 (Feb. 2014) [Hereinafter Readout Report].

[43] Readout Report, at 2. 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 3. Notwithstanding, they also hailed from only the health care industry. Readout Report, at 2. That is a limited perspective, and likely much could be gained if any future dialogue concerning cyber insurance involved chief information security officers or risk management equivalents from diverse sectors other than health care.
[44] Readout Report, at 2.
[45] Readout Report, at 4.
[46] Readout Report, at 4.
[47] Readout Report, at 30.
[48] Readout Report, at 4.
[49] Readout Report, at 4.
[50] Readout Report, at 41.
[51] Readout Report, at 41.
[52] NIST 800-39, at 9.
[53] Nat'l Inst. of Standards & Tech., Special Publication 800-30 Rev. 1, *Guide for Conducting Risk Assessments*, at J-1 (Sept. 2012).
[54] NIST 800-39, at H-4 (emphasis added).
[55] Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* 4 (Version 1.0) (Feb. 12, 2014).
[56] Michelle Kerr & Joel Berg, "Cyber: The New CAT," *Risk & Ins.*, Apr. 7, 2014.