GOOD HARBOR
SECURITY RISK MANAGEMENT, LLC

Developing a Framework to Improve Critical Infrastructure Cybersecurity

Submitted by: Good Harbor Security Risk Management- Jacob Olcott, Emilian Papadopoulos, Jacob Gilden, Will Howerton

Across industries and sectors, corporate executives are struggling to properly manage cybersecurity risk within their companies, including owners and operators of critical infrastructure. In providing strategic advice to corporate clients, Good Harbor Security Risk Management has found that while executive recognition about cyber risk is growing, executives face significant challenges in implementing cyber risk governance structures and hiring employees who can properly manage enterprise-wide cyber risk programs. As NIST begins to craft the Cybersecurity Framework it must consider the organizational and human capital challenges that all firms face when addressing cybersecurity challenges. NIST should avoid prescribing or recommending a single cybersecurity management structure, focusing instead on the importance of corporate-wide strategic and governance frameworks that executives can employ to properly mitigate cyber risks to their organizations.

Good Harbor works with senior corporate executives to develop strategic cybersecurity programs that mitigate organizational risk. We work with large and medium-sized companies across all sectors of the economy. In the course of our work, we have found that organizations that develop an enterprise-wide cyber risk governance program with clearly defined roles and responsibilities for executives and personnel across the company are, generally speaking, better positioned to manage and mitigate cyber risk than those who place complete responsibility and authority for cybersecurity within one individual. Unfortunately, many companies believe that addressing cyber risk simply involves designating one key individual with cyber risk management responsibility. Organizations commonly place a Chief Information Security Officer (CISO) in charge of managing cybersecurity risk across the enterprise. The CISO reports directly to a Chief Information Officer (CIO) or Chief Technology Officer (CTO), who is typically a senior executive within the company. We have found that this corporate structure, by itself, is inadequate to properly address cyber risk.

Good Harbor has found in its experience advising executives in multiple industries that shifting to an executive cybersecurity council-based reporting model for CISOs is more likely to lead to a cybersecurity risk management program that reflects the true cybersecurity challenges to businesses including potential legal, operational, and

financial harm. By including the General Counsel, Chief Financial Officer, and other executives along with the CIO in an executive council format, companies can build organization-wide cyber risk management program that focuses on addressing the company's most significant, material risks.

Managing material cyber risks, rather than meeting compliance mandates, should be the goal of any corporate cybersecurity program. While organizations have legal responsibilities to secure certain types of information (personal, financial, or health information), there is other valuable information within a company's networks that also requires protection. Business secrets and intellectual property tend to constitute the most important assets held by any company but can be ignored when a company focuses its security resources only on building a legal compliance program. By including other executives in a corporate-wide cyber risk management program, CISOs are likely to obtain valuable perspective when scoping their information security program. This more holistic view of enterprise business risk will allow the CISO to better align technical measures, policy, and practices in order to address the greatest risks cybersecurity presents to the firm.

We believe internal and external oversight of cybersecurity risk management from corporate boards and investors is a critical component of an enterprise-wide governance model. Boards of Directors have the basic role of safeguarding shareowners and ensuring that the company is operating with proper oversight. In the context of cybersecurity, Boards must be prepared to act pursuant to this role to ensure that companies properly manage cyber risk and protect their most critical assets, which are ultimately the lifeblood of any company and the basis for value creation for shareowners. Boards also play an important crisis management role, overseeing the implementation of plans to respond to potentially serious cybersecurity incidents. Boards should receive regular updates from the cyber risk council and individuals responsible for managing cyber risk in order to properly perform their duties.

Investors, like corporate boards, also play a critical role in overseeing proper cybersecurity risk management, but from outside the corporation. The Securities and Exchange Commission Guidance on Cybersecurity issued in October 2011 makes clear that public companies have an option to disclose cyber incidents that have a material impact on company operations. Investors must begin to request and properly value these disclosures and introduce cyber risk into their decision-making during their investment diligence process and when they are invested in a firm. Investors should

request information from senior management in order to properly ensure that the company is diligently mitigating cyber risks to the organization.

This organizational-wide approach toward managing cyber risk requires a shift in staffing cyber risk management programs within companies. Traditionally, technical experts have staffed cybersecurity programs almost exclusively, including the CISO position. But cyber risk management not only requires technical solution implementation, but also finding strategic methods of transferring, mitigating, or accepting business risks associated with information technology. We are finding that companies are adding more business-focused strategic managers to augment their cybersecurity teams. The companies that are best positioned to manage cyber risk employ strategic risk management or business professionals to either assist or oversee the CISO, helping to integrate cybersecurity across the enterprise. These risk managers provide a strategic vision for cybersecurity across the company and help create a culture of cybersecurity.

To successfully manage cybersecurity risks, organizations need talented cybersecurity professionals. Good Harbor has found that a lack of available qualified technical cybersecurity professionals is currently one of the greatest inhibiting factors companies face as they look to implement cybersecurity risk management programs. The current dearth of individuals who can properly implement technical security programs in large organizations is a serious issue not only for private industry, but for government agencies as well. Education programs in technical cybersecurity at the undergraduate and graduate level have failed to keep pace with public and private sector workforce demand. Moreover, additional specialized cybersecurity training is often needed for certain organizations, such as in industries reliant on industrial control systems.

In addition to the lack of adequate technical training, business students are currently entering the workforce without adequate comprehension of cybersecurity enterprise risk management. There are currently few business school graduates with a deep enough understanding of cyber risk to staff a position in charge of implementing a strategic cybersecurity risk management program, let alone to understand the cyber threats that businesses they will eventually run are likely to face. Corporate boards, executives, and investors are likely to continue to misunderstand the importance of sound corporate cybersecurity practices and risk management without proper education within business-related fields.

As government and private industry work to build common understandings of what

enterprise-wide cybersecurity risk management should entail, governance and management structures must be included, and traditional approaches to managing the problem must be challenged. Simply adopting a list of technical measures and standards will be insufficient to properly manage the increasingly dangerous cyber threats that businesses face. Without the right governance structures to address enterprise risk management, companies will struggle to adequately protect their information and networks.

Thank you for the opportunity to provide these comments to the Cybersecurity Framework.