COSMOS
Navigate the Compliance Universe

CEP Magazine - July 2018

Three things are certain: death, taxes, and cyber breaches

by Megan M. Moloney

Megan M. Moloney (moloneymegan@gmail.com) is a Senior Strategy, Risk, and Compliance Manager at the Federal Bureau of Investigation in Washington DC.

Cyber incidents are no longer the purview of security and information technology professionals alone. Compliance officers, risk managers, and the full range of C-suite executives ignore this topic at their own risk. An important first step for senior executives is to establish and participate in cross-functional cybersecurity governance structures that span all verticals of the organization, including traditional outliers of compliance, risk management, human resources, and communications. This ensures that all entities within your business are actively contemplating their potential exposure and cyber security responsibilities. Once such structures are in place, members must assess the cyber security posture of the business, including but not limited to its readiness for and response to cyber incidents. A fundamental piece of preparing for and responding to a cyberbreach is effective communication with the government.

Let's be honest. Over the past decade, there has been a tangible boardroom reluctance to share details about cyber security threats and intrusions with the government. This is understandable, because there are real concerns regarding legal and regulatory risk, privacy, and reputational damage. But this reluctance has also been and continues to be detrimental to the collective security of the country and businesses operating within it.

In 2013, Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (PPD-21), identified 16 critical infrastructure sectors "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[1],[2] In the time since, there has been tremendous coordination between the government and these sectors, but the increasing number of attacks on non-critical infrastructure demonstrates the need for this cooperation to expand to other industries. In 2016, Presidential Policy Directive 41, United States Cyber Incident Coordination (PPD-41), set forth that "significant cyber incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors," without singling out any industries.[3] Meaningful coordination between the government and private sector entities of all flavors will not only improve preparedness and response, but may also, ultimately, save lives.

Government communications take many different forms. The ideal communication plan for your organization should be tailored to the size, industry, and known risks of the entity in question. That said, the general steps below apply to virtually all organizations and, if taken, will improve your positioning before, during, and after a significant cyber incident.

Use a common cyber security language

One of the key challenges of communicating effectively with the government is finding a common language — an Esperanto of cyber security. Historically, private sector industries and organizations employed different cyber security terminology, but over the past decade, private sector and government entities have coordinated

extensively to develop a common language. Two key translation mechanisms that serve this purpose are the Office of the Director of National Intelligence (ODNI) Cyber Threat Framework and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The ODNI Cyber Threat Framework not only aims to create consistent categorization and characterization of cyber threats, but also seeks to identify overarching trends. The NIST Cybersecurity Framework was originally developed under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," and was designed to provide a framework for voluntary use by critical infrastructure owners and operators.

The Cybersecurity Enhancement Act of 2014 (CEA) statutorily cemented NIST's role by requiring NIST to identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks."[4] Familiarity with each of these documents will greatly advance the ability to speak across industries and sectors about the common threats we face.