From: Norman Marks
Sent: Monday, January 16, 2017 11:47:53 AM
To: cyberframework
Subject: Blog post about the NIST Cyber Framework

Please see my comments here: [Blog]

[From Blog]

Perhaps the most important cyberrisk framework is that published by the U.S. National Institute of Standards and Technology (NIST). Recently, NIST shared for comment a proposed update to their framework.

Here are some key excerpts from the executive summary:

- Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.
- The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.
- 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.
- The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks — different threats, different vulnerabilities, different risk tolerances — and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

Later, the authors say this:
"Enterprise risk management is the consideration of all risks to achieving a given business objective. Ensuring cybersecurity is factored into enterprise risk consideration is integral to achieving business objectives. This includes the positive effects of cybersecurity as well as the negative effects should cybersecurity be subverted."
There's a good amount of material to like.

- The framework is risk-based and talks about, in my words, investing in cybersecurity commensurate with the level of risk.
- When it talks about risk, it is to the achievement of business objectives. They don't talk about protecting information assets, but rather drive to what is important to the success of the business.
- It uses a maturity model (although it doesn't describe it as such) as a useful way to assess the effectiveness of the cyber program.
- It makes the point that those responsible for the cyber program need to be at an appropriate level within the organization.
- It emphasizes that the management of cyberrisk needs to be integrated within the broader enterprise risk management activity.

However, there are some few areas where I would have liked to have seen more discussion.

- Appendix B is a list of objectives for the cyber program. However, in my opinion it is over-simplified and probably incomplete. For example, I do not see anything about protecting the organization from the effects of social engineering.
- While detection is emphasized, the need for *timely* detection is not mentioned.
- The framework mentions the need for continuous improvement and that cyberrisk is dynamic. However, the sea is constantly rising and defenses have to adapt at least as fast as the risk changes. Investment needs to be in resources that enable threats to be monitored and defenses upgraded continuously.
- The task of assessing the likelihood of a breach is hardly covered at all. There is general acceptance of the fact that a breach is almost inevitable, so the emphasis perhaps should be on the likelihood of different degrees of impact. Past experience may not be a good indicator, as prior breaches may not have been detected — leaving management with the unjustified belief that the incidence of breach is lower than it really is.

- The framework suggests that the organization should have an inventory of all assets or points on the network. However, with the extended supply chain plus the Internet of Things plus the fact that employees and other individuals are hacked as entry points, the problem is far more severe than is presented. I am not persuaded that an inventory can ever be considered complete.
- While the framework talks about integration with the enterprise risk management program, it is important to note that cyber may be one of several risks that might affect the achievement of one or more business objectives. Decisions about acceptable levels of risk to an objective should consider all these risks, not just one. In other words, cyber and other risks to an objective may appear to be at an acceptable level individually, but the aggregate effect may be intolerable and require action.
- The framework references the ISO 31000:2009 global risk management standard (curiously not the COSO ERM Integrated Framework) but defines "risk" in its own way. It also uses the term "risk tolerance" in its own way, inconsistent with that of COSO or ISO. (It is essentially the same as COSO's risk appetite).

A framework is simply that, a framework that any organization can build out to suit its situation and needs.
I encourage everybody to consider the document, respond with suggestions for improvement, and perhaps use it to assess and then upgrade your organization's cyber program.

Your comments?

[End Blog]

I would be happy to expand on them if needed.

Thanks
Norman

Norman D. Marks, CPA, CRMA
Author, Evangelist and Mentor for Better Run Business
OCEG Fellow, Honorary Fellow of the Institute of Risk Management