VENABLE® LLP

Cybersecurity Alert

March 17, 2014

Cybersecurity Assessments – Using the Tool Well

AUTHORS

Michael J. Baader
Jamie Barnett, Rear Admiral (Ret.)
David M. DeSalle
Anthony J. Rosso
Bobby N. Turnage, Jr.
Brian M. Zimmet
Jason R. Wool

RELATED INDUSTRIES

Cybersecurity

ARCHIVES

2014 2010 2006
2013 2009 2005
2012 2008 2004
2011 2007

Are you considering a cybersecurity assessment? If you heard Venable's presentation, "**New Cybersecurity Framework Released: What You Need to Know**," you might be.

The Framework places increased emphasis on organizational cybersecurity risk management. NIST states in the Framework that "organizations responsible for Critical Infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk." Sectors not considered to be Critical Infrastructure are likely subject to similar expectations. For instance, the SEC has indicated that "risk oversight is a core competence" of the boards of publicly held companies, and there can be little question today that cyber risk is an elemental component of many businesses' risk portfolios.

As a result, your organization should consider whether to perform reviews and assessments of your cybersecurity programs in the context of NIST's recommended risk management methodology. You may also want to determine your readiness to "adopt" the Framework or, because of current events and a growing awareness of increasingly sophisticated and widespread cybersecurity threats, perform vulnerability assessments or other penetration tests.

Why Consider an Assessment?

These assessments not only identify areas of improvement in any given cybersecurity program, but also confirm that other program components are successfully functioning as intended. These assessments can be extremely valuable in terms of risk management and could be used in litigation or enforcement actions to show that the cybersecurity program in question was "commercially reasonable" and managed in a reasonable manner. Additionally, corporate boards, as a matter of good corporate governance practice and fulfillment of their fiduciary duties, should consider obtaining periodic updates and assessments of their data security profile in light of the potential risks of IP loss, business interruption, harm to business reputation, and other adverse consequences arising from a data breach.

What Does My Organization Need to Know?

Evaluating your security program can help you identify areas where you can better protect your organization as well as your clients and customers, and there are some important considerations to keep in mind prior to embarking on such an endeavor.

- **First, consider engaging a third-party security consultant that specializes in cyber security.** The typical in-house IT department has many responsibilities related to the day-to-day operations of the business, whereas a third-party specialist makes it their business to know the latest and greatest threats as well as the most effective tools for defending against those threats. Bringing in a third-party specialist will both allow your IT department to continue focusing on the important work of keeping your business running and better ensure an objective analysis of organizational cyber risk.

- **Second, we urge you to consider having outside counsel retain your selected consultant, with draft reports being provided directly to the law firm.** This provides your lawyers with the ability to review draft findings and conclusions. Your organization likely will not know in advance what these third-party assessments will reveal, and having that information protected by attorney-client privilege could become very important, depending upon what is discovered in the assessment. Additionally, allowing your outside counsel the opportunity to provide input on the findings and conclusions in such a report while it is still in draft form enables them to ensure that a report does not contain speculative or inflammatory statements or conclusions that are not necessary but that could be harmful if ever disclosed.

Venable's **Cybersecurity Team** has considerable experience with these types of assessments and

has partnered with numerous IT consultant firms to provide both targeted and full-service cybersecurity reviews. Please feel free to contact us with any questions about protecting your organization while ensuring that its cyber risk is effectively and reasonably managed in light of the NIST Cybersecurity Framework.