Security 101: Information Security Framework: Where to Begin?

By: Jim Mottola, Director of Forensic Investigations -Risk Mitigation Services, Sobel & Co.

Information security is principally about supporting a business by protecting critical and sensitive data as part of its processes. In my capacity as Special Agent in Charge of the United States Secret Service Newark Division, and in my current role as the Director of Forensic Investigations/Risk Mitigation Services at Sobel & Co., for most small to midsize business owners the biggest barrier to entry is often times just knowing the first step to take in protecting their greatest asset, information.

Unlike corporate and nonprofit organizations that operate specifically within the regulated environments of health care and financial services, government compliance may sometimes present a road map to protect consumer data. This is accomplished through the implementation of defined information security standards such as HIPAA and the Graham Leach Bliley Act (GBLA) as part of a risk management program. Under such a program, governance, risk and compliance result in an integrated comprehensive information security solution.

However, my experience demonstrates that most middle market businesses have resource limitations and are forced to contend with the residual risk inherent in operating in today's every changing environment, where criminal hackers exploit vulnerabilities in software, networks and people through a combination of social engineering and technological expertise. Given their limited resources, it is no wonder why business owners are so reluctant to expend precious financial funds at an cyber security incident that is difficult to predict the likelihood and quantify the business impact.

Now don't get me wrong. Through the analysis of their own customer data information security and telecommunication providers like McAfee and Verizon, have assisted all of us in making a semi-qualitative assessment of threats to specific industries and organizations based upon their size. However, while threat assessments are key, it is similar to my days in the Secret Service where even with the best intelligence supporting our mission it was often very difficult to determine what the "threat of the day" was and which vulnerability in our own processes were susceptible to exploitation.

To make the best informed decisions, we used a fundamental framework in which responsibilities for the formulation of the security plan were segregated by expertise, coordinated with appropriate oversight and integrated to support the office of the president.

This same comprehensive framework which I used in my governmental work also applies to a methodology to protect the business community. You may have heard me talk about a "Comprehensive Information Security Plan (CISP)." which is founded on participation from a consortium of attorneys, technologists, fraud examiners, physical security professionals and insurers.

This approach, which has been effective in the corporate and nonprofit world provides a thorough confidential, one-day assessment performed by a qualified team with specific expertise in the areas of Governance, Technology, Environmental Controls and Risk Management.

The professionals deliver a gap analysis of an organization's current state and a desired state of information security in order to help them make a more informed business decisions about where to spend their limited resources.

Clients who have gone through the CISP analysis process reinforce the belief that having qualified counsel, an information technologist, a physical security expert and an experienced insurance agent review their organizations entire information security program, all in one day, was invaluable. They note a confidence in making better decisions to protect their information and as a result, they believe to be more resilient in the face of a cybersecurity incident.

The one day assessment is intended to provide an organization with the details they need to begin to plan and develop a business case for making informed decisions about information security. It also focuses on organizational resilience based upon a multidisciplinary approach through the analysis of the businesses policies and procedures along with an engaged, open discussion with its key stake holders.