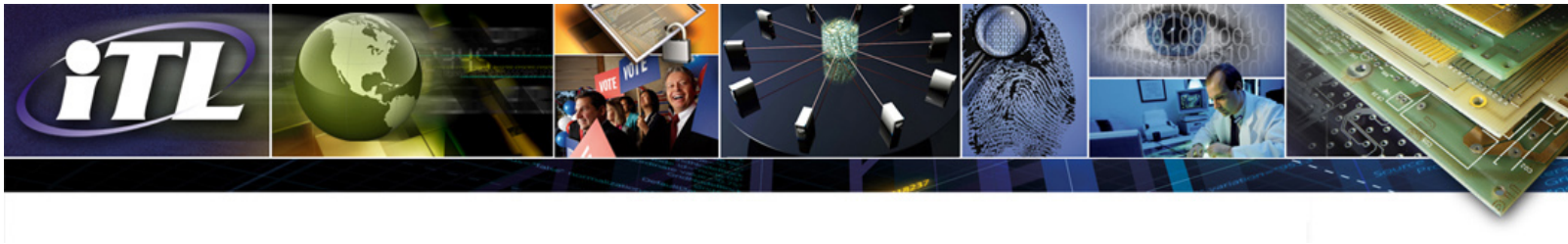

ITL BULLETIN FOR MAY 2014

SMALL AND MEDIUM-SIZE BUSINESS INFORMATION SECURITY OUTREACH PROGRAM

Richard Kissel, Kim Quill, and Chris Johnson, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Small and medium-size businesses (SMBs) represent 99.7 percent of all U.S. employers and are an important segment of the U.S. economy. These organizations, totaling more than 28.2 million, create over 60 percent of all new U.S. private sector jobs and produce over 47 percent of the country's Gross National Product (GNP).[1] SMBs are increasingly reliant on information technology as they store, process, and communicate information. Because information is one of the most valuable assets of an organization, the protection of this information is critical.

SMBs provide essential goods and services to the nation and therefore must be protected against increasing cyber threats. The security of an SMB is important to its customers, whose data it must protect, and to its partners within the supply chain, who have an expectation that their business affiliates have implemented effective information security safeguards. These business partners want to ensure that their systems are not put at risk by connecting to those of any other business.

Some SMBs, including those that provide products and services to critical infrastructure, may have agile and robust cybersecurity practices that allow them to rapidly adapt to a dynamic threat environment. However, many SMBs may be unable to apply the same level of rigor and resources (e.g., technology, people) to information security as larger and better resourced organizations and face significant challenges in securing their organization's information, systems, and networks. This reality, in conjunction with the crucial role that SMBs hold in the supply chain and the economy, make such SMBs an attractive target for cyber criminals looking to exploit common vulnerabilities.

ITL's SMB Information Security Outreach Program is designed to help small and medium-size businesses better protect the data of their customers, employees, and business partners by providing information on practical and cost-effective security practices for securing their information, systems, and networks. One of the main goals of the program is to increase cybersecurity awareness within the SMB community

[1] SBA *Small Business Advocate:* April 2014; SBA *Small Business GDP: Update 2002-2010,* January 2012.

and help them to better understand the threat environment and vulnerabilities so that SMBs can make sound, risk-based decisions regarding their cybersecurity investments.

As a component of this program, the National Institute of Standards and Technology (NIST), the Small Business Administration (SBA), and the Federal Bureau of Investigation (FBI) entered into a cosponsorship agreement to conduct a series of workshops on computer security for small businesses. These workshops help SMBs to better protect the data of their customers, employees, and business partners. Since the inception of the program in 2002, 118 half-day workshops have been conducted in 38 states, the District of Columbia, and Guam, reaching over 5000 businesses.

Through a series of workshop presentations and exercises, participants learn to:

- Identify and prioritize information;
- Evaluate the cost of potential loss/cost of protection of information;
- Determine the appropriate protections for information; and
- Implement policies, procedures, risk management, and best practices.

During the workshops, participants examine the business case for security – how cybersecurity operates in support of sound management, customer service, legal, and economic practices. In this light, cybersecurity represents an investment, and the workshop focuses on helping SMBs make informed investment decisions by examining the types of information they possess (e.g., personally identifiable information, intellectual property); determining the degree of protection that the information requires with respect to confidentiality, integrity, and availability; and evaluating the potential cost of information loss versus the cost of protection. Equipped with this knowledge, SMBs can evaluate and select from a wide range of products and services designed to meet their needs.

By understanding the information that they possess and the protection that it requires, SMBs are able to identify practical and cost-effective security measures that they can implement. Such measures may include the development of security policies that describe the information that an organization holds and how it must be protected (e.g., acceptable use, training) and the development of procedures that describe roles, responsibilities, and processes for effectively implementing security policies. Workshop participants are given the opportunity to explore risk assessment processes, allowing them to learn how to identify threats, vulnerabilities, and associated risks, and how to make informed risk management decisions based on organizational risk tolerance.

The final workshop activity focuses on presenting a set of information security best practices — fundamental activities that an SMB should consider performing on an ongoing basis to better protect its information, systems, and networks.

The security best practices described in the workshop presentation and materials are explored in greater detail in the NIST Interagency Report (NISTIR) 7621*, Small Business Information Security: The Fundamentals*. This report complements the workshop materials and presents essential actions, recommended practices, and other steps that small businesses should take to protect their information, systems, and networks. NISTIR 7621 helps SMBs to identify, assess, plan, and implement a basic risk-based information security program. The appendices of NISTIR 7621 contain templates that can be used to identify and prioritize an organization's information types and protection requirements, and to estimate the financial impact of information disclosure, loss, or modification.

In addition to the workshops and NISTIR, SMBs can explore the security best practices described in the *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (the Framework). In February 2014, in response to *Executive Order 13636*, NIST published a voluntary Framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. The Framework is a flexible tool that can be used by SMBs to better understand and manage cybersecurity risk. Using the Framework, an SMB can compare its current cybersecurity activities with the practices outlined in the Framework, determine the extent to which they are successfully applying these practices, and establish a practical, prioritized, and cost-effective approach for managing cybersecurity risk.

The security practices presented in the Framework are aligned with the Framework's five high-level functions: *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*. The activities described in the *Identify* function focus on helping an organization to better understand its systems, assets, data, and capabilities, and through this understanding, to more effectively manage its cybersecurity risk. Equipped with this understanding, SMBs can develop and implement practical and cost-effective safeguards based on the activities described in the Framework's *Protect* function.

While an SMB may have protective measures in place, such measures are not infallible, and it is still necessary to be able to detect cybersecurity events in a timely manner. The Framework's *Detect* function focuses on implementing capabilities that enable the discovery of anomalies and events (e.g., ongoing monitoring of the organizations information systems and assets). When such an event is detected, it is important that organizational response and recovery mechanisms be in place in advance of the incident. The Framework *Respond* and *Recovery* functions describe the activities that can help an SMB better prepare to respond to and recover from an incident and help minimize any disruption to the organization's business or mission.

The workshops, publications, webinars, and videos provided through ITL's SMB Information Security Outreach Program are designed to provide an overview of the threat and vulnerability landscape and to identify practical tools and techniques for implementing high-value security practices. By implementing these security practices, SMBs are better able to meet their business commitments and protect the information that their customers, business partners, and employees have entrusted to them.

Additional Resources

The NIST Small Business Corner website contains useful information regarding upcoming and past workshops; a library of presentations, videos, publications, and exercises; FAQs, and contact information for the program. Learn more about the small business information security outreach program at: http://csrc.nist.gov/groups/SMA/sbc

The NIST Cybersecurity Framework website contains links to Executive Order 13636; the Cybersecurity Framework; news releases; archived documents; and information related to upcoming and past workshops and events. Learn more about the Cybersecurity Framework at: http://www.nist.gov/cyberframework

Additional information about NIST's information security programs, standards, guidelines, and related publications is available from the Computer Security Resource Center at: http://csrc.nist.gov

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov