ITL BULLETIN FOR MARCH 2017

FUNDAMENTALS OF SMALL BUSINESS INFORMATION SECURITY

Celia Paulsen, Larry Feldman,[1] and Greg Witte,[1] Editors
Applied Cybersecurity Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

Small businesses are an important part of our nation's economy. According to the Small Business Administration (SBA), these businesses produce approximately 46 percent of our nation's private sector output and create 63 percent of all new jobs in the country. Small businesses are more innovative, agile, and productive than ever, thanks to the capabilities delivered by information technology (IT), but the IT security challenge for small businesses looms larger than ever. An information security incident can be detrimental to the business, its customers, employees, business partners, and many others. It is vitally important that small business leaders understand and manage risks to their information, systems, and networks.

To address this need, NIST published NIST Interagency Report 7621 Revision 1 (NISTIR 7621r1), Small Business Information Security: The Fundamentals. The document provides guidance on how small businesses can provide basic security for their information, systems, and networks. It presents the fundamentals of a small business information security program in nontechnical language.

The NISTIR uses the Framework for Improving Critical Infrastructure Cybersecurity[2](CSF) to help organize the discussion of cybersecurity risk management processes and procedures and to ease the transition from cybersecurity fundamentals to more advanced cybersecurity risk management as described in the CSF. Since the CSF has proven useful to a variety of audiences, CSF's functional approach provides a logical way to present and organize information and cybersecurity best practices.

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.
[2] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Revision 1 reflects changes in technology since the original NISTIR 7621 was published. NISTIR 7621r1 reorganizes the procedures that small business leaders need to implement a cybersecurity program that will help protect information and manage cybersecurity risk.

Information Security and Cybersecurity Fundamentals

NISTIR 7621r1 provides a basic overview of information security, cybersecurity, and their main objectives: confidentiality, integrity, and availability. It describes how cybersecurity works in conjunction with a variety of other security-related components, such as physical security, personnel security, contingency planning and disaster recovery, operational security, and privacy. The publication emphasizes the importance of all these components; lacking any one of them diminishes the effectiveness of the others. For example, good physical security measures mean little if personnel security is poor.

The guidance further describes why small business leaders should provide information security. Small businesses often don't understand why they would be targeted, but they may have money or information that can be valuable to a criminal; an organization's computers may be compromised and used to launch an attack on somebody else (i.e., as part of a botnet); or the business may provide inside access to more high-profile targets through its products, services, or supply chain role.

In addition, small businesses often see information security as too difficult or that it requires too many resources to achieve. Because small businesses typically have fewer resources to invest in information security when compared to larger businesses, cyber criminals may view them as soft targets.

There is no easy, one-time solution to information security – it takes time and careful consideration with all relevant stakeholders. However, when viewed as part of the business's strategy and regular processes, information security doesn't have to be intimidating. It is not possible for any business to be completely secure. Nevertheless, it is possible—and reasonable—to implement a program that balances security with the needs and capabilities of a business. This publication aims to help small businesses develop a basic, risk-based program to understand and protect their business information.

Understanding and Managing Your Risks

Risk is a function of threats, vulnerabilities, the likelihood of a harmful event, and the potential impact such an event would have. Each business has a unique risk profile and differing risk appetites. It is unreasonable to expect a business to eliminate all risk. Understanding risk is key to focusing a business's information security protection, detection, and response efforts.

The goal of an information security program should be to provide for informed, risk-based decision making. NISTIR 7621r1 describes the following simple steps for creating a risk-based information security program:

- Identify what information your business stores and uses;
- Determine the value of that information;
- Develop an inventory of technology that interacts with that information; and
- Understand the threats and vulnerabilities which may impact that information.

Using these steps, the business can prioritize and focus their information security efforts. In support of these steps, NISTIR 7621r1 provides a set of three useful worksheets. A table shows how a business can prioritize their information security efforts based on the value of the information their business stores or uses (or "impact") and the potential likelihood of an attack. The publication directs small businesses to focus first on implementing tools and practices which aid in protecting from and detecting an event impacting their most sensitive information, then to develop a schedule for adding further protections to less sensitive, but still important information. The publication emphasizes that information security risk management is not a one-time process, but is a continual, ongoing set of activities.

Safeguarding Your Information

The publication further describes tools and practices useful in protecting information, organized in alignment with the CSF's five Functions - *Identify, Protect, Detect, Respond,* and *Recover*. The CSF has proven a valuable resource, providing a simple, common language for helping organizations to identify, assess, and manage cybersecurity risks. For the reader's convenience, NISTIR 7621r1 contains reference information about the CSF in one of its appendices.

NISTIR 7621r1 lists a small number of basic tools and practices for each of the CSF's five functions. The tools and practices listed are applicable to most small businesses, are relatively easily implemented, and can provide a foundation for more advanced information security practices as needed. As part of this foundation, the publication provides example information security policy and procedure statements.

Working Safety and Securely

In addition to the programmatic (planned) steps listed in alignment with the CSF, NISTIR 7621r1 contains a last section focused on everyday activities leaders and their employees can do to help keep their business safe and secure. Many incidents can be prevented by practicing safe and secure business habits. While adversaries are becoming more sophisticated, most criminals still use well-known and easily avoidable methods. Each employee should be trained to follow basic practices such as:

- Pay attention to the people you work with and around;
- Be careful of email attachments and web links;
- Use separate personal and business computers, mobile devices, and accounts;

- Do not connect personal or untrusted storage devices or hardware into your computer, mobile device, or network;
- Be careful downloading software;
- Do not give out personal or business information;
- Watch for harmful pop-ups;
- Use strong passwords; and
- Conduct online business more securely.

Conclusion

NISTIR 7621 Revision 1 provides guidance to help small businesses set up a basic information security program. The publication describes how an information security program can be implemented, discusses key actions small businesses can take to protect their information, and identifies key practices directed towards users, which can be implemented to protect a system and information.

The guidance emphasizes the importance of a risk management approach to information security. The comprehensive coverage of information security fundamentals, written using plain, nontechnical language, makes these guidelines useful for protecting small business systems and information. The worksheets in the publication help small businesses to conduct a risk analysis, and the examples of information security policy and procedure statements help them set up a lasting information security program. Because the document is aligned with the CSF, it provides a stepping stone for small businesses to develop or incorporate more advanced cybersecurity practices as needed.

For more information on ways in which ITL helps small businesses to enhance their cybersecurity, see the ITL Director Charles Romine's recent testimony on small business cybersecurity at https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-115-SY15-WState-CRomine-20170214.pdf.

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