CYBERSECURITY FUNDAMENTALS FOR SMALL BUSINESS OWNERS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Small businesses contribute significantly to the U.S. economy, comprising over 95 percent of all businesses in our country, producing about 50 percent of our Gross National Product (GNP), and creating about 50 percent of all of the new jobs. Small business owners face serious challenges in protecting their business information and the private information of their customers and employees. Often lacking sufficient resources to secure their information infrastructures effectively, small businesses are frequent targets of criminal attacks and hostile threats to systems.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently issued a new guide that tailors basic information on cybersecurity to the specific needs of small business owners to help them in planning for and managing secure information systems. NIST Interagency Report (NISTIR) 7621, *Small Business Information Security: The Fundamentals*, by Richard Kissel, presents three major areas that small businesses should address to provide security for their information, systems, and networks: **essential information security practices, highly recommended practices, and other planning considerations**. The major recommendations for each of these three areas are summarized in the following sections of this bulletin. The guide, which is available at http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf, provides more details on each of these actions and advises about steps to be taken for specific operating systems.

The best practices recommended by NIST focus on helping small businesses to avoid the costs of not protecting systems and information, and to protect the safety and security of information of their customers and their employees, as well as their sensitive business information.

Ten Essential Activities to Protect Small Business Information, Systems, and Networks

NIST recommends that small business organizations take the following actions to improve the effectiveness and security of their information systems:

- **Protect information, systems, and networks from damage by viruses, spyware, and other malicious code.**

Small businesses should install antivirus and antispyware software on every computer used in their business operations. The antivirus and antispyware software, which is readily available from commercial software vendors, should be updated regularly. Many vendors offer subscriptions to “security service” applications, which provide multiple

layers of protection, in addition to antivirus and antispyware protection. The software can be set to automatically check for updates and to carry out security scans at scheduled times, such as during the night. Business organizations should obtain copies of the antivirus software that is used by the business systems for the home systems of those employees who work at home.

- **Provide security for Internet connection.**

Business computers and networks that have broadband access to the Internet for 24 hours a day every day are exposed to continual hostile threats. Small businesses should install and keep operational a hardware firewall between their internal networks and the Internet. The firewall function may be provided by a wireless access point or router installed by the small business or by a router operated by the Internet Service Provider (ISP) of the small business. Home systems used by employees working at home should be protected by a hardware firewall between their systems and the Internet. Administrative passwords and default passwords provided with new software should be changed when the firewall is installed, and at regular intervals thereafter.

- **Install and activate software firewalls on all business systems.**

A software firewall should be installed and used on every operational computer system, and should be updated regularly. Software firewalls are needed to supplement the protection provided by hardware firewalls. Some operating systems include firewalls installed as part of the system. Software firewalls are available for purchase from vendors, and sometimes can be obtained free of cost. All systems, including employees' home systems, should be checked to assure that the software firewalls are installed and operational. More detailed information on software firewalls available for different operating systems is included in NISTIR 7621.

- **Patch all operating systems and applications.**

The vendors of major operating systems generally provide patches and updates to their products to correct discovered security problems and to improve functionality of the software. Patches should be applied to installed business systems regularly, and installed on all new systems and software. Details on the installation of patches are included in NISTIR 7621.

- **Make backup copies of important business data and information.**

Copies should be made of all data including word processing documents, electronic spreadsheets, databases, financial files, human resources files, accounts receivable and payable files, and other information used in or generated by the business. This will prevent loss of data when there are equipment failures, employee errors, or destruction of data by malicious code. An automatic backup should be done at least once a week, and stored on a separate hard disk on each business computer, off-line on a form of removable media, or in online storage. A full backup of all data should be made once a

month, and stored away from the business location. Regular backups and monthly backups, which can be made on external Universal Serial Bus (USB) hard drives, should be tested regularly to ensure that the data can be accessed and used.

- **Control physical access to business computers and network components.**

Unauthorized persons should not be allowed to access or to use any business computers, including laptops. Computers should not be available to access by cleaning crews or by unsupervised repair personnel. Employees working at their computers should position their displays so that they cannot be seen by people walking by an office or by unknown strangers who may walk into an office.

- **Secure wireless access points and networks.**

Small business owners who use wireless networking should set the wireless access point so that it does not broadcast its Service Set Identifier (SSID). When new devices are acquired, the administrative password that was on the device when it was purchased should be changed. Strong encryption should be used so that data being transmitted between the businesses' computers and the wireless access point cannot be easily intercepted and read by electronic eavesdroppers. The current recommended encryption is WiFi Protected Access 2 (WPA-2), which uses the Advanced Encryption Standard (AES) for secure encryption.

- **Train employees in basic security principles.**

Employees should be trained to use the sensitive business information properly and to protect the business' and its customer's information. Employees should receive training on the organization's information security policies, including the use of computers, networks and Internet connections, the limitations on personal use of telephones, printers, and other business resources, and any restrictions on processing business data at home. After receiving their training, employees should be requested to sign a statement indicating that they understand and will follow business policies, and that they understand the penalties for not following the policies. Security training for employees can be arranged through the local Small Business Development Center (SBDC), community college, technical college, or commercial training vendors.

- **Require individual accounts for each employee using business computers and business applications.**

A separate account should be established for each individual computer user, and strong passwords should be used. Passwords should be changed at least every three months. The employees' individual accounts should not have access to administrative accounts to avoid the installation and spread of unauthorized software or malicious code.

- **Limit access to data and information by employees, and limit the authority to install software.**

Access to all data and to all systems, including financial, personnel, inventory, and manufacturing, should not be provided to any one employee. Access to systems and data should be limited to the specific systems and information that employees need to do their jobs. One employee should not be allowed to both initiate and approve transactions, such as financial transactions.

Highly Recommended Practices for Small Businesses

The following practices are also very important and should be implemented immediately after the essential activities are put into effect.

.

- **Examine carefully email attachments and emails that request sensitive information.**

Email attachments should not be opened unless the email is expected and the sender is trusted since this is a means for distributing spyware or malicious code. The individual who may have sent the email should be called and asked if the mail is legitimate. If the sender's computer has been compromised by malicious code, the code can be installed on the computer of the person who opens the attachments that have been sent.

- **Examine carefully web links in email, instant messages, social media, and other communications.**

Connecting to links in email messages can lead to the installation of malicious software, viruses, or key stroke logging software on the user's computer. These links should be avoided unless the sender is trusted and the web link is known to be a legitimate one.

- **Avoid popup windows and other hacker tricks.**

Popup windows that request a response should be closed. Attackers frequently develop popup windows to try to trick the user into downloading and installing spyware or other malicious code. Employees should be trained not to bring into the office any USB drives that might be infected by hackers, and they should not plug them into the business computers.

- **Conduct online business and online banking securely.**

Online business, commerce, and banking should be conducted using a secure browser connection. This will normally be indicated by a small lock visible in the lower right corner of the web browser window. The web browser cache, temporary Internet files, cookies, and history associated with online commerce or banking sessions should be erased after the end of the sessions. This will prevent sensitive information from being stolen by a hacker or by a malware program, if the system has been compromised.

- **Engage in secure personnel practices when hiring employees.**

Comprehensive, nationwide background checks should be conducted before new employees are hired, and criminal background checks should be considered for all prospective new employees. Online background checks are quick, relatively inexpensive, and readily available. In addition, credit checks on prospective employees should be considered, and the references provided by prospective employees and their former employers should be contacted.

- **Adopt secure practices for web surfing.**

Users with administrative privileges should not surf the web to avoid the installation of malicious code. A guest account with limited privileges can be established for those employees who need web access, such as for educational purposes.

- **Limit the downloading of software from the Internet.**

Software should not be downloaded from any unknown web page. Only web pages from trusted business partners and services, such as operating system providers, should be downloaded. Freeware or shareware from a source on the web should be examined carefully. Though there may be no cost, this software often does not provide technical support.

- **Seek specialized expertise in information system security when it is needed.**

Sources of expertise in information security for small businesses include Small Business Development Centers (SBDCs), Service Corps of Retired Executives (SCORE), local Chambers of Commerce, Better Business Bureaus, and community and technical colleges. All potential service providers should be examined and reviewed for past performance and references.

- **Protect sensitive information when disposing of old computers and media.**

Small businesses should dispose of old business computers by removing and destroying the hard disks, electronic components, and connectors. Also old storage media that is obsolete and no longer usable, such as CDs, floppy disks, and USB drives, should be destroyed, and paper containing sensitive information should be shredded.

- **Protect information and systems from social engineering techniques.**

Social engineering is a personal or electronic attempt to obtain unauthorized information or access to systems or sensitive areas by attackers who manipulate people. The process is often conducted through telephone calls. Employees should be trained to be helpful, but to be vigilant when asked for information or special system access, and to authenticate callers by asking for identification information. All attempts by outsiders to obtain information or system access should be reported to management.

Planning Considerations

In addition to the operational procedures described above, small businesses should consider the following issues when planning and implementing their information systems:

- **Contingency and disaster recover planning.**

Plans should be developed for restoring business operations that might be interrupted by natural disasters and contingencies, such as floods, fires, tornados, power outages, sewer backups, or water damages. Since power outages are common, each computer and critical network component should be connected to an Uninterruptible Power Supply (UPS). An inventory should be made of all information used for operating the business. The information in the inventory should be prioritized for its importance to the business. Appendices A and B of the NIST small business guide include worksheet templates to help small businesses collect and evaluate this information.

- **Cost-avoidance considerations in information security.**

While there is a cost involved in protecting information, small businesses must consider the costs of not protecting information. For example, some states have enacted notification laws that require businesses, including small businesses, to notify, in a specified manner, all persons whose data might have been exposed in a security breach, such as a hacker incident, malicious code incident, or an unauthorized release of information. Appendix C of the guide contains a worksheet that can be used by small businesses to calculate the costs of not providing adequate protection to each data type used in the business, from the highest priority to the lowest priority, and for different information security incidents.

- **Business policies related to information security and other topics.**

Small businesses should develop and circulate written policies that identify acceptable practices and expectations for business operations. Some of the policies are related to human resources, and others are concerned with permitted employee practices for using business resources, such as telephones, computers, printers, fax machines, and Internet access. The range of potential policies is largely determined by the type of business and the degree of control and accountability desired by the business owner. Legal and regulatory requirements may also require that certain policies be put in place and enforced.

Policies for appropriate use of information, computers, and networks, and policies for Internet security should be formulated to convey the business management’s expectations to employees. These policies should identify the information and other resources that are essential to the operation of the business, and should describe how management expects the resources to be used and protected by all employees.

These policies should be communicated clearly to all employees, and all employees should sign a statement stating that they have read the policies, that they will follow the policies, and that they understand the possible penalties for violating the policies. This will help management to hold employees accountable for violation of the business policies. Penalties should be established for disregarding business policies, and all penalties should be enforced fairly and consistently for anyone who violates the policies of the business.

NIST Publications

NIST Interagency Report (NISTIR) 7621, *Small Business Information Security: The Fundamentals*, by Richard Kissel of NIST, is available on NIST's web page http://csrc.nist.gov/publications/PubsNISTIRs.html.

For information about other NIST security-related publications, including information about the use of firewalls, media sanitization, and encryption, see NIST's web page http://csrc.nist.gov/publications/index.html.

More Information

The term Small Enterprise (or Small Organization) is sometimes used for small businesses. A small enterprise or organization may also be a nonprofit organization. The size of a small business varies by type of business, but typically it is a business or organization with up to 500 employees (according to the U.S. Small Business Administration).

U.S. Small Business Administration
http://www.sba.gov/idc/groups/public/documents/sba_homepage/serv_sstd_tablepdf.pdf

White House Blog (information about cybersecurity awareness)
http://www.whitehouse.gov/blog/2009/10/26/cybersecurity-awareness-month-part-iv

Federal Trade Commission (for information on identity theft)
http://www.ftc.gov/bcp/edu/microsites/idtheft/

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.