DRAFT NISTIR 7621
Revision 1

Small Business Information Security: The Fundamentals

Richard Kissel
Hyunjeong Moon

This publication is available free of charge

National Institute of Standards and Technology
U.S. Department of Commerce

DRAFT NISTIR 7621
Revision 1

Small Business Information Security: The Fundamentals

Richard Kissel
Hyunjeong Moon
Computer Security Division
Information Technology Laboratory

This publication is available free of charge

December 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

National Institute of Standards and Technology Interagency Report 7621 Revision 1
32 pages (December 2014)

This publication is available free of charge

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *December 15, 2014* through *February 9, 2015*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: smallbizsecurity@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

NIST, as a partner with the Small Business Administration and the Federal Bureau of Investigation in an information security awareness outreach to the small business community, developed this NISTIR as a reference guideline for small businesses. This document is intended to present the fundamentals of a small business information security program in non-technical language.

Keywords

small business information security; cybersecurity fundamentals

Acknowledgements

The authors, Richard Kissel and Hyunjeong Moon, wish to thank their colleagues and reviewers who contributed greatly to the document's development.

Table of Contents

Overview 1

1 Introduction 2

2 The "absolutely necessary" cybersecurity actions that a small business should take to protect its information, systems, and networks. 4

2.1 Manage Risk. 4

2.2 Protect information/systems/networks from damage by viruses, spyware, and other malicious code. 4

2.3 Protect your Internet connection. 5

2.4 Install and activate software firewalls on all your business systems. 6

2.5 Patch your operating systems and applications. 6

2.6 Make backup copies of important business data/information. 7

2.7 Control physical access to your computers and network components. 9

2.8 Secure your wireless access point and networks. 9

2.9 Train your employees in basic security principles. 9

2.10 Require all individual user accounts for each employee on business computers and for business applications. 10

2.11 Limit employee access to data and information, and limit authority to install software. 11

3 Highly Recommended Cybersecurity Practices 12

3.1 Be careful with email attachments and emails requesting sensitive information. 12

3.2 Be careful with web links in email, instant messages, social media, or other means. 12

3.3 Watch for harmful popup windows and other hacker tricks. 12

3.4 Do online business or banking more securely. 13

3.5 Exercise due diligence in hiring employees. 14

3.6 Be careful when surfing the Web. 14

3.7 Be concerned when downloading software from the Internet. 14

3.8 Get help with information security when you need it. 15

3.9 Dispose those old computers and media safely. 15

3.10 Protect against Social Engineering. 16

3.11 Perform An Asset Inventory (and identify sensitive business information). 16

3.12 Implement Encryption To Protect Your Business Information. 16

4 More Advanced Cybersecurity Practices 18

4.1 Plan for Contingency and Disaster Recovery. 18

4.2 Identify Cost-Avoidance considerations in information security. 19

4.3 Create Business policies related to information security. 19

Appendix A— Identifying and prioritizing your organization's information types 21

Appendix B— Identifying the protection needed by your organization's priority information types 22

Appendix C— Estimated costs from bad things happening to your important business information 23

Appendix D— NIST Framework for Improving Critical Infrastructure Cybersecurity 24

Overview

For some small businesses, the security of their information, systems, and networks might not be a high priority, but for their customers, employees, and trading partners it is very important. The term Small Enterprise (or Small Organization) is sometimes used for this same category of business or organization. A small enterprise/organization may also be a nonprofit organization. The size of a small business varies by type of business, but typically is a business or organization with up to 500 employees.[1]

In the United States, the number of small businesses totals to over 99 % of all businesses. The small business community produces around 46 % of our nation's private-sector output and creates around 63 % of all new jobs in our country.[2] Small businesses, therefore, are a very important part of our nation's economy. They are a significant part of our nation's critical economic and cyber infrastructure.

Larger businesses in the United States have been actively pursuing information security with significant resources including technology, people, and budgets for some years now. As a result, they have become a more difficult target for hackers and cyber criminals. What we are seeing is that the hackers and cyber criminals are now focusing more of their unwanted attention on less secure businesses.

Therefore, it is important that each small business improve the cybersecurity of its information, systems, and networks.

This NIST Interagency Report (NISTIR) will assist small business management in understanding how to provide basic security for their information, systems, and networks.

In addition to this NISTIR, NIST has fostered the creation of the *Framework for Improving Critical Infrastructure Cybersecurity*[3]. This Cybersecurity Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. For more information, see Appendix D—.

Revision 1 of this publication reflects changes in technology and a reorganization of the information needed by small businesses to implement a reasonably effective cybersecurity program.

---

[1] U.S. Small Business Administration, *Table of Small Business Size Standards*, July 14, 2014. https://www.sba.gov/sites/default/files/Size_Standards_Table.pdf (accessed November 20, 2014).

[2] U.S. Small Business Administration, Office of Advocacy, *Frequently Asked Questions*, March 2014. https://www.sba.gov/sites/default/files/FAQ_March_2014_0.pdf (accessed November 20, 2014).

[3] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (accessed November 20, 2014).

1 Introduction

Why should a small business be interested in, or concerned with, information security?

The customers of small businesses have an expectation that their sensitive information will be respected and given adequate and appropriate protection. The employees of a small business also have an expectation that their sensitive personal information will be appropriately protected.

And, in addition to these two groups, current and/or potential business partners also have their expectations of the status of information security in a small business. These business partners want assurance that their information, systems, and networks are not put "at risk" when they connect to and do business with a small business. They expect an appropriate level of security in an actual or potential business partner—similar to the level of security that they have implemented in their own systems and networks.

Some of the information used in your business needs special protection for one or more of the following:

- **confidentiality**, to ensure that only those who need access to that information to do their jobs actually have access to it;
- **integrity**, to ensure that the information has not been tampered with or deleted by those who should not have had access to it; and
- **availability**, to ensure that the information is available when it is needed by those who conduct the organization's business.

Such information might be sensitive employee or customer information, confidential business research or plans, or financial information. Some of these information categories (e.g., health, privacy, and certain types of financial information) have special, more restrictive regulatory requirements for information security protection. Failure to properly protect such information, based on the required protections, can easily result in significant fines and penalties from the regulatory agencies involved.

Just as there is a cost involved in protecting information (for hardware, software, or management controls such as policies & procedures, etc), there is also a cost involved in not protecting information. Those engaged in risk management for a small business are also concerned with cost-avoidance—in this case, avoiding the costs of not protecting sensitive business information.

When we consider cost-avoidance, we need to be aware of those costs that aren't immediately obvious. Among such costs are the notification laws that many states have passed which require any business, including small businesses, to notify, in a specified manner, all persons whose data might have been exposed in a security breach (hacker incident, malicious code incident, an employee doing an unauthorized release of information, etc). The average estimated cost for these notifications and associated security breach costs is well over $130 per person. If you have 1000 customers whose data was/or ***might have been*** compromised in an incident, then your expected minimum cost would be $130,000, per incident. Prevention of identity theft is a goal of these laws and regulations. This should provide motivation to implement adequate security to

prevent such incidents. Of course, if there is such an incident then some customers will lose their trust in the affected business and take their business elsewhere. This is another cost that isn't immediately obvious, but which is included in the above per-person cost.

Considering viruses and other malicious code (programs), the severity and impact of current virus/Trojan/Malware attacks are becoming much greater. [4] It is unthinkable to operate a computer without protection from these harmful programs. Many, if not most, of these viruses or malicious code programs are used by organized crime to steal information from computers and make money by selling or illegally using that information for such purposes as identity theft.

It is not possible for any business to implement a perfect information security program, but it is possible (and reasonable) to implement sufficient security for information, systems, and networks that malicious individuals will go elsewhere to find an easier target. Additional information may be found on NIST's Computer Security Resource Center, http://csrc.nist.gov.

[4] Symantec Corporation, *Internet Security Threat Report 2014*, 2013 Trends vol. 19 (April 2014), p.24-40. http://www.symantec.com/security_response/publications/threatreport.jsp (accessed November 20, 2014).

2 The "absolutely necessary" cybersecurity actions that a small business should take to protect its information, systems, and networks.

These practices must be done to provide basic information security for your information, computers, and networks.

These practices will help your organization to **identify** and understand the value of your information and systems, **protect** those resources, **detect** possible incidents that could compromise them, and help your organization to **respond** to and **recover** from possible cybersecurity events. See Appendix D— for more detailed descriptions of these Cybersecurity Framework functions.

2.1 Manage Risk.

*Cybersecurity Framework (CF) Function(s): **Identify**, **Protect***

Risk Management is the process of identifying the risks that your business is exposed to and then managing that risk by implementing protective measures to limit the identified risks.

The action of Risk Assessment is engaged to identify the risks that your business is exposed to. Included in Risk Assessment is identifying the threats to your business and identifying the vulnerabilities that your business has to each of those threats.

Since most small business owners/managers are not cybersecurity professionals, this set of actions should be provided by a cybersecurity contracting firm (preferably one which specializes in small business risk assessment). It would be wise to have them conduct a penetration test of your systems and networks. This is a testing process which seeks out vulnerabilities in your hardware or software. Perhaps this could be arranged for through your local SCORE[5] chapter's cybersecurity professionals.

It is good risk management practice to arrange for an annual independent IT security review to verify the effectiveness of your IT security program. The annual IT security review should be done by an auditing business different from the business providing your cybersecurity services. In the event that you have a cybersecurity incident, this may support your due diligence in protecting your sensitive business information.

2.2 Protect information/systems/networks from damage by viruses, spyware, and other malicious code.

*CF Function(s): **Protect***

Malicious code is code (computer programs) written to do bad things to your data and/or computer (including smart phones, tablets, and other mobile devices). Bad things can be: "find and delete sensitive data;" "find and copy sensitive data – and send it to cyber criminals who

[5] Originally known as the Service Corps of Retired Executives, it is now simply referred to as SCORE.

will sell it or use it to make money; record all keystrokes made on the computer (including account numbers, passwords, answers to secret questions, etc) and report that information to a 'command center' somewhere on the Internet; encrypt your sensitive data and demand money for you to get it back; reformat your hard drive; and other actions that might significantly harm your business. There are a growing number of smartphone and tablet apps which contain malicious code.

Install, use (in "real-time" mode, if available), and regularly update anti-virus and anti-spyware software on every computer used in your business.

Many commercial software vendors provide adequate protection at a reasonable price or for free. An Internet search for anti-virus and anti-spyware products will show many of these organizations. Most vendors now offer subscriptions to "security service" applications, which provide multiple layers of protection (in addition to anti-virus and anti-spyware protection).

You should be able to set the anti-virus software to automatically check for updates at some scheduled time during the night (12:00 midnight, for example) and then set it to do a scan soon afterwards (12:30 am, for example). Schedule the anti-spyware software to check for updates at 2:30 am and to do a full system scan at 3:00 am. This assumes that you have an always-on, high-speed connection to the Internet. Regardless of the actual scheduled times for the above updates and scans, schedule them so that only one activity is taking place at any given time.

It is a good idea to obtain copies of your business anti-virus software for your and your employees' home computers. Most people do some business work at home, so it is important to protect their home systems, too.

For case studies of real small businesses that have been victims of cybercrime, go to: http://krebsonsecurity.com/category/smallbizvictims/

2.3 Protect your Internet connection.

*CF Function(s): **Protect***

Most businesses have broadband (high-speed) access to the Internet. It is important to keep in mind that this type of Internet access is always "on." Therefore, your computer—or any network your computer is attached to—is exposed to threats from the Internet on a 24 hours-a-day, 7 days-a-week basis.

For broadband Internet access, it is critical to install and keep operational a hardware firewall between your internal network and the Internet. This may be a function of a wireless access point/router, or it may be a function of a router provided by the Internet Service Provider (ISP) of the small business. There are many hardware vendors that provide firewall wireless access points/routers, firewall routers, and separate firewall devices.

Since employees will do some business work at home, ensure that all employees' home systems are protected by a hardware firewall between their system(s) and the Internet.

For these devices, the administrative password must be changed upon installation and regularly thereafter. It is a good idea to change the administrator's name as well. The default values are easily guessed, and, if not changed, may allow hackers to control your device and thus, to monitor or record your communications and data via the Internet.

2.4 Install and activate software firewalls on all your business systems.

CF Function(s): ***Protect, Detect***

Install, use, and regularly update a software firewall on each computer system used in your small business.

If you use the Microsoft Windows operating system, it probably has a firewall included.[6] You have to ensure that the firewall is operating.

It is important to note that you should only be using a current and vendor-supported version of whatever operating system you choose to use.

When using any commercial operating system, ensure that you review the operating manuals to discover if your system has a firewall included and how it is enabled and configured.

There are commercial software firewalls that you can purchase at a reasonable price or for free that you can use with your Windows systems or with other operating systems. Again, Internet searches and using online and trade magazine reviews and references can assist in selecting a good solution.

Again, since employees do some business work at home, ensure that employee's home systems have firewalls installed and operational on them, and that they are regularly updated.

It is necessary to have software firewalls on each computer even if you have a hardware firewall protecting your network. If your hardware firewall is compromised by a hacker or by malicious code of some kind, you don't want the intruder or malicious program to have unlimited access to your computers and the information on those computers.

2.5 Patch your operating systems and applications.

CF Function(s): ***Protect***

All operating system vendors provide patches and updates to their supported products to correct security problems and to improve functionality. Microsoft provides monthly patches on the second Tuesday of each month. From time to time, Microsoft will issue an "off schedule" patch to respond to a particularly serious threat. To update any supported version of Windows, go to "Start" and select "Windows Update" or "Microsoft Update." Follow the prompts to select and install the recommended patches. Other operating system vendors have similar functionality.

---

[6] See Microsoft's *Safety & Security Center* for more information and downloads: http://www.microsoft.com/security/default.aspx (accessed November 20, 2014).

Ensure that you know how to update and patch any operating system you select. When you purchase new computers, update them immediately. Do the same when installing new software.

To update Windows 7:

- click **Start**, then **All Programs**, then **Windows Update**;
- click **Change Settings** in the left pane;
- under **Important Settings**, select the option you want;
- under **Recommended Updates**, choose "Include recommended updates when downloading, installing, or notifying me about updates";
- click **OK**.

To update Windows 8:

- display the charms list by sliding across the top of the screen to the right edge;
- choose **Settings**, then **Control Panel**, then **System and Security**;
- in **Windows Update**, turn **Automatic Updating** "On" and select **Install Updates Automatically**;
- if you want to check for available updates, select **Check for Updates**;
- if you want to see what updates have been installed, select **Update History**.

It is important to note that you should only be using a current and vendor-supported version of whatever operating system you choose to use. Vendors **do not have to provide security updates** for unsupported products. For example, Microsoft ended support for Windows XP on April 8, 2014.[7]

Office productivity products such as Microsoft Office also need to be patched and updated on a regular basis. For Microsoft software, the patch/update process is similar to that of the Microsoft Windows operating systems. Other software products also need to be updated regularly.

2.6 Make backup copies of important business data/information.

*CF Function(s): **Respond, Recover***

Back up your data on each computer used in your business. Your data includes (but is not limited to) word processing documents, electronic spreadsheets, databases, financial files, human resources files, accounts receivable/payable files, and other information used in or generated by your business.

It is necessary to back up your data because computers die, hard disks fail, employees make mistakes, and malicious programs can destroy data on computers. Without data backups, you can

[7] Microsoft Corporation, *Windows lifecycle fact sheet* (April 2014), http://windows.microsoft.com/en-us/windows/lifecycle (accessed November 20, 2014).

easily get into a situation where you have to recreate your business data from paper copies and other manual files.

Do this automatically if possible. Many security software suites offer automated backup functions that will do this on a regular schedule for you. Back up only your data, not the applications themselves. **Automatic data backups should be done at least once a week**, and stored on a separate hard disk on your computer, on some form of removable media (e.g., external hard drive), or online storage (e.g., a cloud service provider). The storage device should have enough capacity to hold data for 52 weekly backups, so its size should be about 52 times the amount of data that you have, plus 30 % or so. Remember, this should be done on each of your business computers. It is important to periodically test your backed up data to ensure that you can read it reliably. There are "plug and play" products which, when connected to your computer, will automatically search for files and back them up to a removable media, such as an external USB hard disk.

It is important to **make a full backup of each computer once a month** and store it away from your office location in a protected place. If something happens to your office (fire, flood, tornado, theft, etc) then your data is safe in another location and you can restore your business operations using your backup data and replacement computers and other necessary hardware and software. As you test your individual computer backups to ensure they can be read, it is equally important that you test your monthly backups to ensure that you can read them. If you don't test your backups, you have no grounds for confidence that you will be able to use them in the event of a disaster or contingency.

If you choose to do this monthly backup manually, an easy way is to purchase a form of removable media, such as an external USB hard drive (at least 1 terabyte (TB) capacity). On the hard drive, create a separate folder for each of your computers, and create two folders in each computer folder—one for each odd numbered month and one for each even numbered month. Bring the external disk into your office on the day that you do your monthly backup. Then, complete the following steps: connect the external disk to your first computer and make your backup by copying your data into the appropriate designated folder; immediately do a test restore of a file or folder into a separate folder on your computer that has been set up for this test (to ensure that you can read the restored file or folder). Repeat this process for each of your business computers and, at the end of the process, disconnect the external drive. At the end of the day, take the backup hard drive to the location where you store your monthly backups. At the end of the year, label and store the hard disk in a safe place, and purchase another one for use in the next year.

It is very important to do a monthly backup for each computer used in your business.

Storing data in the "Cloud" is also a possibility. Do your due diligence when selecting a Cloud Service Provider. It is recommended that you encrypt all data prior to storing it in the Cloud. The

Cloud Security Alliance (CSA) provides information and guidance for using the Cloud safely. See Domain 11 "Encryption and Key Management" for additional advice on encryption.[8]

2.7 Control physical access to your computers and network components.

CF Function(s): ***Protect, Detect***

Do not allow unauthorized persons to have physical access to or to use of any of your business computers. This includes locking up laptops when they are not in use. It is a good idea to position each computer's display (or use a privacy screen) so that people walking by cannot see the information on the screen.

Controlling access to your systems and networks also involves being fully aware of anyone who has access to the systems or networks. This includes cleaning crews who come into the office space at night to clean the trash and office space. Criminals often attempt to get jobs on cleaning crews for the purpose of breaking into computers for the sensitive information that they expect to find there. Controlling access also includes being careful about having computer or network repair personnel working unsupervised on systems or devices. It is easy for them to steal privacy/sensitive information and walk out the door with it without anyone noticing anything unusual.

No one should be able to walk into your office space without being challenged by an employee. This can be done in a pleasant, cordial manner, but it must be done to identify those who do not have a legitimate reason for being in your offices. "How may I help you?" is a pleasant way to challenge an unknown individual.

2.8 Secure your wireless access point and networks.

CF Function(s): ***Protect***

If you use wireless networking, it is a good idea to set the wireless access point so that it does not broadcast its Service Set Identifier (SSID). Also, it is critical to change the administrative password that was on the device when you received it. It is important to use strong encryption so that your data being transmitted between your 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), using the Advanced Encryption Standard (AES) for secure encryption. See your owner's manual for directions on how to make the above changes. Note that WEP (Wired-Equivalent Privacy) is not considered secure; **do not use WEP for encrypting your wireless traffic**.

2.9 Train your employees in basic security principles.

CF Function(s): ***Protect***

---

[8] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing v3.0* (2011), p.129. https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/ (accessed November 20, 2014).

Employees who use any computer programs containing sensitive information should be told about that information and must be taught how to properly use and protect that information. On the first day that your new employees start work, they need to be taught what your information security policies are and what they are expected to do to protect your sensitive business information. They need to be taught what your policies require for their use of your computers, networks, and Internet connections.

In addition, teach them your expectations concerning limited personal use of telephones, printers, and any other business owned or provided resources. After this training, they should be requested to sign a statement that they understand these business policies, that they will follow your policies, and that they understand the penalties for not following your policies. (You will need clearly spelled-out penalties for violation of business policies.)

Set up and teach "rules of behavior" which describe how to handle and protect customer data and other business data. This may include not taking business data home or rules about doing business work on home computers.

Having your employees trained in the fundamentals of information, system, and network security is one of the most effective investments you can make to better secure your business information, systems, and networks. You want to develop a "culture of security" in your employees and in your business.

It would be helpful to make your employees aware of the cybersecurity issues arising from allowing children or grandchildren to use their home computers. This is especially true if children or grandchildren are using the computers unsupervised.

Typical providers of such security training could be your local Small Business Development Center (SBDC), SCORE Chapter, community college, technical college, or commercial training vendors.

2.10 Require all individual user accounts for each employee on business computers and for business applications.

CF Function(s): ***Protect***

Set up a separate account for each individual and require that good passwords be used for each account. Good passwords consist of a random sequence of letters (upper case and lower case), numbers, and special characters—and are at least 12 characters long.

To better protect systems and information, ensure that all employees use computer accounts which do not have administrative privileges. This will hinder any attempt—automated or not—to install unauthorized software. If an employee uses a computer with an administrative user account, then any malicious code that they activate (deliberately or by deception) will be able to install itself on their computer—since the malicious code will have the same administrative rights as the user account has.

Without individual accounts for each user, you may find it difficult to hold anyone accountable for data loss or unauthorized data manipulation.

Passwords that stay the same, will, over time, be shared and become common knowledge to an individual user's coworkers. Therefore, **passwords should be changed at least every 3 months**.

2.11 Limit employee access to data and information, and limit authority to install software.

CF Function(s): ***Protect***

Use good business practices to protect your information. Do not provide access to all data to any single employee. Do not provide access to all systems (financial, personnel, inventory, manufacturing, etc) to any single employee. For all employees, provide access to only those systems and only to the specific information that they need to do their jobs.

Do not allow a single individual to both initiate and approve a transaction (financial or otherwise).

The unfortunate truth is that insiders—those who work in a business—are the source of most security incidents in the business. The reason is that they are already known, trusted, and have been given access to important business information and systems. So, when they perform harmful actions (deliberately or otherwise), the business information, systems, and networks—and the business itself—suffer harm.

3 Highly Recommended Cybersecurity Practices

These practices are very important and should be completed immediately after those in Section 2.

3.1 Be careful with email attachments and emails requesting sensitive information.

CF Function(s): ***Protect, Detect***

For business or personal email, do not open email attachments unless you are expecting the email with the attachment and you trust the sender.

One of the more common means of distributing spyware or malicious code is via email attachments. Usually these threats are attached to emails that pretend to be from someone you know, but the "from" address has been altered and it only appears to be a legitimate message from a person you know.

It is always a good idea to call the individual who "sent" the email and ask them if they sent it and ask them what the attachment is about. Sometimes, a person's computer is compromised and malicious code becomes installed on it. Then, the malicious code uses the computer to send emails in the name of the owner of the computer to everyone in the computer owner's email address book. The emails appear to be from the person, but instead are sent by the computer when activated by the malicious code. Those emails typically have copies of the malicious code (with a deceptive file name) as attachments to the email and will attempt to install the malicious code on the computer of anyone who receives the email and opens the attachment.

Beware of emails which ask for sensitive personal or financial information—regardless of who the email appears to be from. No responsible business will ask for sensitive information to be provided in an email.

3.2 Be careful with web links in email, instant messages, social media, or other means.

CF Function(s): ***Protect, Detect***

For business or personal email, do not click on links in email messages. Some scams are in the form of embedded links in emails. Once a recipient clicks on the link, malicious software (e.g., viruses or key stroke logging software) is installed on the user's computer. It is not a good idea to click on links in a Facebook or other social media page.

Don't do it unless you know what the web link connects to and you trust the person who sent the email to you. It is a good idea to call the individual prior to clicking on a link and ask if they sent the email and what the link is for. Always hold the mouse pointer over the link and look at the bottom of the browser window to ensure that the actual link (displayed there) matches the link description in the message (the mouse pointer changes from an arrow to a tiny hand when placed over an active link).

3.3 Watch for harmful popup windows and other hacker tricks.

*CF Function(s): **Protect, Detect***

When connected to and using the Internet, do not respond to popup windows requesting that you to click “ok” for anything.

If a window pops up on your screen informing you that you have a virus or spyware and suggesting that you download an anti-virus or anti-spyware program to take care of it, close the popup window by selecting the X in the upper right corner of the popup window. Do not respond to popup windows informing you that you have to have a new codec, driver, or special program for something in the web page you are visiting. Close the popup window by selecting the X in the upper right corner of the popup window.

Some of these popup windows are actually trying to trick you into clicking on “OK” to download and install spyware or other malicious code onto your computer. Be aware that some of these popup windows are programmed to interpret any mouse click anywhere on the window as an “OK” and act accordingly. For such unexpected popup windows, a safe way to close the window is to reboot your computer. (first close any open applications, documents, etc)

Hackers are known to scatter infected USB drives with provocative labels in public places where their target business’s employees hang out, knowing that curious individuals will pick them up and take them back to their office system to “see what’s on them.” What is on them is generally malicious code which attempts to install a spy program or remote control program on the computer. Teach your employees to not bring USB drives into the office and plug them into your business computers (or to take them home and plug into their home systems). It is a good idea to disable the “AutoRun” feature for the USB ports (and optical drives like CD and DVD drives) on your business computers to help prevent such malicious programs from installing on your systems.

3.4 Do online business or banking more securely.

*CF Function(s): **Protect***

Online business/commerce/banking should only be done using a secure browser connection. This will normally be indicated by a small lock visible in the lower right corner of your web browser window.

After any online commerce or banking session, erase your web browser cache, temporary internet files, cookies, and history so that if your system is compromised, that information will not be on your system to be stolen by the individual hacker or malware program. The steps for erasing this data in Microsoft Internet Explorer and Mozilla Firefox are described below.

For Microsoft Internet Explorer, version 10.0 (steps for other versions may vary slightly):

- select **Tools**, then **Safety**, and click **Delete Browsing History**;
- select those items you want to erase (e.g., temporary files, history, cookies, saved passwords and web form information) and click **Go** to erase them.

For Mozilla Firefox, version 32.0 (steps for other versions may vary slightly):

- select **Tools**, then near the bottom of the popup window click **Options**;
- select the **Privacy** tab, select **Remove Individual Cookies**, then select **Remove All Cookies** to erase your session information;
- it is a good idea to check the box **Tell Sites that I don't want to be tracked;**
- under **History**, select **Never remember history**.

If you do online business banking, the safest way to do this is to have a dedicated computer which is used ONLY for online banking. Do not use it for Internet searches. Do not use it for email. Use it only for online banking for the business.

3.5 Exercise due diligence in hiring employees.

*CF Function(s): **Protect***

When hiring a new employee, conduct a comprehensive background check before making a job offer.

You should consider doing criminal background checks on all prospective new employees. Online background checks are quick and relatively inexpensive. Do a full, nationwide, background check. This should also include a sexual offender check. In some areas, the local police department provides a computer for requesting a background check. In some areas, this service is free to you. If possible, it is a good idea to do a credit check on prospective employees. This is especially true if they will be handling your business funds. And, do the rest of your homework—call their references and former employers.

If there are specific educational requirements for the job that they have applied for, call the schools they attended and verify their actual degree(s), date(s) of graduation, and GPA(s).

In considering doing background checks of potential employees, it is also an excellent idea for you to do a background check of yourself. Many people become aware that they are victims of identity theft only after they do a background check on themselves and find arrest records and unusual previous addresses where they never lived (some people become aware only after they are pulled over for a routine traffic stop and then arrested because the officer is notified of an outstanding arrest warrant for them).

3.6 Be careful when surfing the Web.

*CF Function(s): **Protect***

No one should surf the Web using a user account with administrative privileges.

If you do surf the Web using an administrative user account, then any malicious code that you happen across on the Internet may be able to install itself on your computer–since the malicious code will have the same administrative rights as your user account. It is best to set up a special account with "guest" (limited) privileges to avoid this vulnerability.

3.7 Be concerned when downloading software from the Internet.

CF Function(s): ***Protect***

Do not download software from any unknown web page.

Only those web pages belonging to businesses with which you have a trusted business relationship should be considered reasonably safe for downloading software. Such trusted sites would include the Microsoft Update web page where you would get patches and updates for various versions of the Windows operating system and Microsoft Office or other similar software. Most other web pages should be viewed with suspicion.

Be very careful if you decide to use freeware or shareware from a source on the Web. Most of these do not come with technical support and some are deliberately crippled so that you do not have the full functionality you might be led to believe will be provided.

3.8 Get help with information security when you need it.

CF Function(s): ***Identify, Protect, Detect, Respond, Recover***

No one is an expert in every business and technical area. Therefore, when you need specialized expertise in information/computer/network security, get help. Ask your SBDC or SCORE Office–often co-located with your local Small Business Administration (SBA) office–for advice and recommendations. You might also consider your local Chamber of Commerce, Better Business Bureau, community college, and/or technical college as a source of referrals for potential providers. For information on identity theft, visit the Federal Trade Commission's (FTC) site on this topic: http://www.ftc.gov/bcp/edu/microsites/idtheft/.

When you get a list of service providers, prepare a request for quotes and send it out as a set of actions or outcomes that you want to receive. Carefully examine and review the quote from each firm responding to your request. Research each firm's past performance and check its references carefully. Request a list of past customers and contact each one to see if the customer was satisfied with the firm's performance and would hire the firm again for future work. Find out who (on the firm's professional staff) will be doing your work. Ask for their professional qualifications for doing your work. Find out how long the firm has been in business.

3.9 Dispose those old computers and media safely.

CF Function(s): ***Identify, Protect***

When disposing of old business computers, remove the hard disks and destroy them. The destruction can be done by taking apart the disk and beating the hard disk platters with a hammer. You could also use a drill with a long drill bit and drill several holes through the hard disk and through the recording platters. Remember to destroy the hard drive electronics and connectors as part of this project. You can also take your hard disks to companies who specialize in destroying storage devices such as hard disks.

When disposing of old media (CDs, floppy disks, USB drives, etc), destroy any containing sensitive business or personal data. Media also includes paper. When disposing of paper

containing sensitive information, destroy it by using a crosscut shredder. Incinerate paper containing very sensitive information.

It is very common for small businesses to discard old computers and media without destroying the computers' hard disks or the media. Sensitive business and personal information is regularly found on computers purchased on eBay, thrift shops, Goodwill, etc, much to the embarrassment of the small businesses involved (and much to the annoyance of customers or employees whose sensitive data is compromised). This is a practice which can result in identity theft for the individuals whose information is retrieved from those systems. Destroy hard disks and media and recycle everything else.

3.10 Protect against Social Engineering.

CF Function(s): ***Protect, Detect***

Social engineering is a personal or electronic attempt to obtain unauthorized information or access to systems/facilities or sensitive areas by manipulating people.

The social engineer researches the organization to learn names, titles, responsibilities, and publicly available personal identification information. Then the social engineer usually calls the organization's receptionist or help desk with a believable, but made-up story designed to convince the person that the social engineer is someone in, or associated with, the organization and needs information or system access which the organization's employee can provide and will feel obligated to provide.

To protect against social engineering techniques, employees must be taught to be helpful, but vigilant when someone calls in for help and asks for information or special system access. The employee must first authenticate the caller by asking for identification information that only the person who is in or associated with the organization would know. If the individual is not able to provide such information, then the employee should politely, but firmly refuse to provide what has been requested by the social engineer.

The employee should then notify management of the attempt to obtain information or system access.

3.11 Perform An Asset Inventory (and identify sensitive business information).

CF Function(s): ***Identify***

Do an inventory of all of your hardware and software assets. This should include identifying all of your important business data that you use to run your business/organization. See Appendix A— for details about inventorying your business information. When you are done, you will have a list of hardware assets (e.g., computers, mobile devices, wireless routers, etc.), software assets (programs for word processing, accounting, etc), and information assets (e.g.,proprietary information, employee information, customer information, etc). The inventory should be kept updated by repeating it at least annually. See Section 4.1 for additional information.

3.12 Implement Encryption To Protect Your Business Information.

CF Function(s): ***Protect***

Encryption is a process of protecting your sensitive business information by using an encryption program to make the information unreadable to anyone not having the encryption key. In several editions of Microsoft Windows 7 and Windows 8, the encryption function is called BitLocker. It is good practice to use full-disk encryption—which encrypts all information on the storage media—with BitLocker or another full-disk encryption product. Some other encryption programs for the Windows operating system include: Symantec Drive Encryption (Symantec Corporation); CheckPoint Full Disk Encryption and McAfee Endpoint Encryption (SafeBoot). For computers using the Apple OS X operating system (versions 10.3 and later), FileVault disk encryption is provided with the operating system. CheckPoint Full Disk Encryption and McAfee Endpoint Encryption also work with Apple OS X and Linux operating systems. For other operating systems, see the manufacturer's manual for information on full-disk encryption capabilities.

When implementing any full-disk encryption function, **do not forget your encryption key**—write it down and lock up the information in a safe place.

It is important to consider all computing and communications devices when considering encryption. For example, most businesses are using smartphones to help run the business. When smartphones have business information on them, it is important to encrypt those devices to help protect that business information from being stolen, modified or deleted. Most smartphone manufacturers are now providing encryption capabilities with their smartphones. This also applies to tablet devices used in the business.

4 More Advanced Cybersecurity Practices.

In addition to the operational guidelines provided above, there are other considerations that a small business needs to understand and address.

4.1 Plan for Contingency and Disaster Recovery.

CF Function(s): ***Identify, Protect, Detect, Respond, Recover***

What happens if there is a disaster (flood, fire, tornado, etc.) or a contingency (power outage, sewer backup, accidental sprinkler activation, etc.)? Do you have a plan for restoring business operations during or after a disaster or a contingency? Since we all experience power outages or brownouts from time to time, do you have Uninterruptible Power Supplies (UPS) on each of your computers and critical network components? They allow you to work through short power outages and provide enough time to save your data when the electricity goes off.

Have you done an inventory of all information used in running your business? Do you know where each type of information is located (on which computer or server)? Have you prioritized your business information so that you know which type of information is most critical to the operation of your business–and, therefore, which type of information must be restored first in order to run your most critical operations? If you have never (or not recently) done a full inventory of your important business information, now is the time. For a very small business, this shouldn't take longer than a few hours. For a larger small business, this might take from a day to a week or so (see Appendix A— for a worksheet template for such an inventory).

After you complete this inventory, ensure that the information is prioritized relative to its importance for the *entire* business, not necessarily for a single part of the business. When you have your prioritized information inventory (on an electronic spreadsheet), add three columns to address the kind of protection that each type of information needs. Some information will need protection for confidentiality, some for integrity, and some for availability. Some might need all three types of protection (see Appendix B— for a worksheet template for this information).

This list will be very handy when you start to decide how to implement security for your important information and where to spend your limited resources to protect your important information. No one has enough resources to protect every type of information in the best possible way, so you start with the highest priority information, protecting each successive priority level until you run out of resources. Using this method, you will get the most "bang for your buck" for protecting your important information.

In the event of a security incident which results in "lost" data because of malicious code, hackers, or employee misconduct, establish procedures to report incidents to employees and/or customers. Most states have notification laws requiring specific notifications to affected customers.

Insurance companies are offering various cybersecurity policies to cover all or part of the cost of a cybersecurity incident. Ask your business insurance agent for information on how this might work for your business–including coverage, cost, and exclusions. As part of the application

process for such insurance, you will be required to implement a basic-level cybersecurity program for your business.

4.2 Identify Cost-Avoidance considerations in information security.

*CF Function(s): **Protect***

In Section 1 we discussed cost avoidance factors. It is important to have an idea of how much loss exposure that your business has if something bad happens to your information.

Something "bad" might involve a loss of confidentiality. Perhaps a virus or other malicious program compromises one of your computers and steals a copy of your business' sensitive information (e.g., employee health information, employee personally identifiable information, customer financial information, etc.). Such a loss could easily result in identity theft for employees or customers. It's not unusual for business owners or managers to be unaware of the financial risk to the business in such situations.

Appendix C— contains a worksheet template to generate financial exposure amounts for different scenarios of data and information incidents. This worksheet should be filled out for each data type used in your business, from the highest priority to the lowest priority.

It is important to understand that there is a real cost associated with not providing adequate protection of sensitive business information and that this cost is usually invisible until something bad happens. Then it becomes all too real (and all too expensive) and visible to current and potential customers.

4.3 Create Business policies related to information security.

*CF Function(s): **Identify, Protect, Detect, Respond, Recover***

Every business needs written policies to identify acceptable practices and expectations for business operations.

Some policies will be related to human resources, others will relate to expected employee practices for using business resources, such as telephones, computers, printers, fax machines, and Internet access. This is not an exhaustive list and the range of potential policies is largely determined by the type of business and the degree of control and accountability desired by management. Legal and regulatory requirements may also require certain policies to be put in place and enforced.

Policies for information, computer, network, and Internet security, should communicate clearly to employees the expectations that the business management has for appropriate use. These policies should identify the information and other resources that are important to management and should clearly describe how management expects those resources to be used and protected by all employees.

For example, for sensitive employee information a typical policy statement might say, "All employee personnel data shall be protected from viewing or changing by unauthorized persons."

This policy statement identifies a particular type of information and then describes the protection expected to be provided for that information.

Policies should be communicated clearly to each employee, and all employees should sign a statement agreeing that they have read the policies, that they will follow the policies, and that they understand the possible penalties for violating those policies. This will help management to hold employees accountable for violations of the business' policies. As noted, there should be penalties for disregarding business policies. And, those penalties should be enforced fairly and consistently for everyone in the business who violates the policies of the business.

Appendix A—Identifying and prioritizing your organization's information types

1. **Think about the information used in/by your organization. Make a list of all the information types used in your organization. (define "information type" in any useful way that makes sense to your business)**

2. **Then list and prioritize the 5 most important types of information used in your organization. Enter them into the table below.**

3. **Identify the system on which each information type is located.**

4. **Identify who has access to each information type.**

5. **Finally, create a complete table for all your business information types – in priority order.**

Table 1: The 5 Highest Priority Information Types In My Organization

Priority	Type of Information	Stored On Which System?	Who has access to this information?
1			
2			
3			
4			
5			

Use this area as your "scratch pad"
(Once you finish this exercise, fill out a full table for all your important business information)

Appendix B—Identifying the protection needed by your organization's priority information types

1. **Think about the information used in/by your organization.**

2. **Enter the 5 highest priority information types in your organization into the table below.**

3. **Enter the protection required for each information type in the columns to the right. (C – Confidentiality; I – Integrity; A - Availability) <"Y"-needed; "N"-not needed>**

4. **Finally, finish a complete table for all your business information types.**

(Note: this would usually be done by adding three columns to Table 1)

Table 2: The Protection Needed by the 5 Highest Priority Information Types in My Organization

Priority	Type of Information	C	I	A
1				
2				
3				
4				
5				

Appendix C—Estimated costs from bad things happening to your important business information

1. **Think about the information used in/by your organization.**

2. **Enter into the table below your highest priority information type.**

3. **Enter *estimated* costs for each of the categories on the left. If it isn't applicable, please enter NA. Total the costs in each column in the bottom cell.**

4. **After doing the above three steps, finish a complete table for all your information types.**

(Note: this would usually be done by adding three columns to Table 1)

Table 3: The Highest Priority Information Type in My Organization and an estimated cost associated with specified bad things happening to it.

	<data type name> Issue: Data Released	<data type name> Issue: Data Modified	<data type name> Issue: Data Missing
Cost of Revelation			
Cost to Verify Information			
Cost of Lost Availability			
Cost of Lost Work			
Legal Costs			
Loss of Confidence Costs			
Cost to Repair Problem			
Fines & Penalties			
Other costs—Notification, etc.			
Total Cost Exposure for this data type & issue			

Appendix D—NIST Framework for Improving Critical Infrastructure Cybersecurity

The *Framework for Improving Critical Infrastructure Cybersecurity* includes the five Framework Core Functions defined below. These Functions are not intended to form a serial path, or lead to a static desired end state. Rather, the Functions can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

  The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

  The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

  The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

  The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

  The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

For additional information, see NIST's Cybersecurity Framework homepage: http://www.nist.gov/cyberframework/index.cfm.