NISTIR 7621
Revision 1

Small Business Information Security:
The Fundamentals

Celia Paulsen
Patricia Toth

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.7621r1

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

NISTIR 7621
Revision 1

Small Business Information Security:
The Fundamentals

Celia Paulsen
Patricia Toth
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.7621r1

November 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

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

National Institute of Standards and Technology Interagency Report 7621 Revision 1
54 pages (November 2016)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.7621r1

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: smallbizsecurity@nist.gov

3 Safeguarding Your Information

This publication uses the *Framework for Improving Critical Infrastructure Cybersecurity* (the "Cybersecurity Framework") to organize the processes and tools that you should consider to protect your information [CSF14]. Appendix C contains more information about the Cybersecurity Framework. This is not a one-time process, but a continual, on-going set of activities. Although the Cybersecurity Framework was originally developed specifically for critical infrastructure organizations, it has proven useful to a variety of audiences as it provides a simple, common language for helping organizations to identify, assess, and manage cybersecurity risks.

This section provides activities you can implement in your business. In addition, Section 4 of this publication lists some common practices you and your employees can implement to help keep your business safe. The specific mitigation activities in this section are grouped into the five broad categories of the Cybersecurity Framework, as pictured in Figure 3. Some of the activities in this publication are suggestions for consideration. This means that those activities are recommended when a higher level of assurance (confidentiality, integrity, or availability) is needed to protect the information and meet business needs than is provided by the more basic practices.

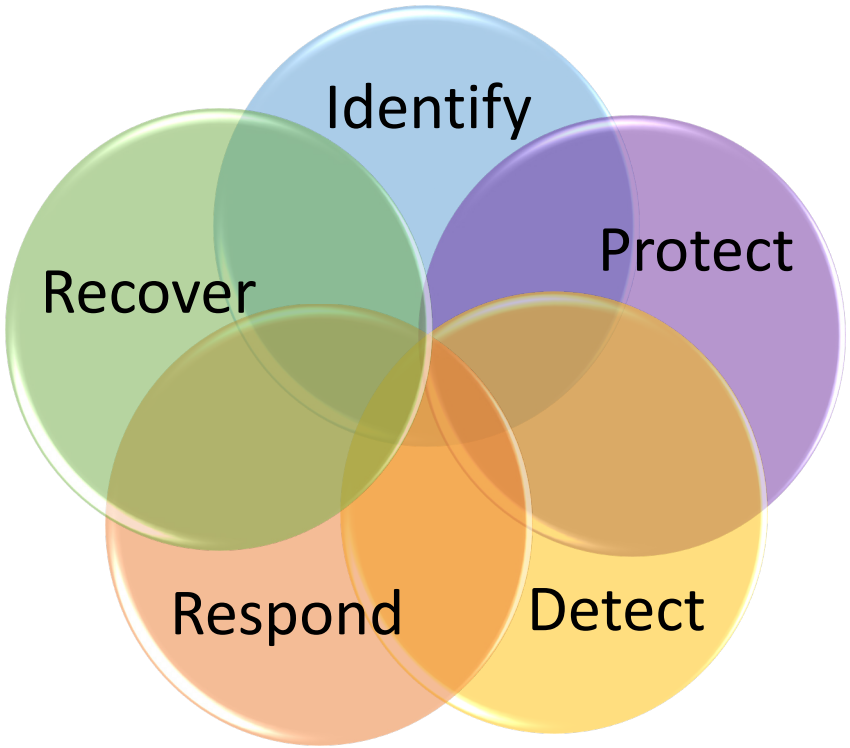

Figure 3: *The Cybersecurity Framework Categories*

3.1 Identify

As described in the Cybersecurity Framework, the activities in the Identify Function help increase an organization's understanding of their resources and risks.[5]

- *Identify and control who has access to your business information*

  Determine who has or should have access to your business's information and technology. Include whether or not a key, administrative privilege, or password is required. To help collect this information, review your list of accounts and what privileges those accounts have.

  Be aware of anyone who has access to your business. Do not allow unknown or unauthorized persons to have physical access to any of your business computers. This includes cleaning crews and maintenance personnel. Do not allow computer or network repair personnel to work on systems or devices unsupervised. No unrecognized person should be able to enter your office space without being questioned by an employee. If a criminal gains physical access to an unlocked machine, they can relatively easily steal any private or sensitive information on that machine.

  Physically lock up your laptops and other mobile devices when they are not in use. You should also utilize the session lock feature included with many operating systems, which locks the screen if the computer is not used for a specified period of time (e.g. 2 minutes). Use a privacy screen or position each computer's display so that people walking by cannot see the information on the screen.

- *Conduct Background Checks*

  Do a full, nationwide, criminal background check, sexual offender check, and if possible a credit check on all prospective employees (especially if they will be handing your business funds). You can request one directly from the FBI or an FBI-approved Channeler [FBI].

  In addition, consider doing a background check on yourself. Many people become aware that they are victims of identity theft only after they do a background check on themselves and find reported arrest records and unusual previous addresses where they never lived. This can be an indication that your identity has been stolen.

  If prospective employees are applying for a job with educational requirements, call the schools they attended and verify their actual degree(s), date(s) of graduation, and GPA(s). If they provided references, call those references to verify the dates they worked for a company and other specifics to ensure the employee is being honest.

[5] The Cybersecurity Framework includes those processes found in section 2 of this publication in the "Identify" function of the Framework [CSF14].

- *Require individual user accounts for each employee.*

  Set up a separate account for each user (including any contractors needing access) and require that strong, unique passwords be used for each account. Without individual accounts for each user, you may find it difficult to investigate data loss or unauthorized data manipulation. Ensure that all employees use computer accounts without administrative privileges to perform typical work functions. This will hinder any attempt—intentional or not—to install unauthorized software. Consider using a guest account with minimal privileges (e.g. internet access only) if needed for your business.

- *Create policies and procedures for information security*

  Policies and procedures are used to identify acceptable practices and expectations for business operations, can be used to train new employees on your information security expectations, and can aid an investigation in case of an incident. These policies and procedures should be readily accessible to employees – such as in an employee handbook or manual.

  The scope and breadth of policies is largely determined by the type of business and the degree of control and accountability desired by management. Have a legal professional familiar with cyber law review the policies to ensure they are compliant with local laws and regulations.

  Policies and procedures for information security and cybersecurity should clearly describe your expectations for protecting your information and systems. These policies should identify the information and other resources that are important and should clearly describe how management expects those resources to be used and protected by all employees. See Appendix E for sample policy and procedure statements. Other examples are readily available online or a legal, insurance, or cybersecurity professional may have example policies.

  All employees should sign a statement agreeing that they have read the policies and relevant procedures, that they will follow the policies and procedures. If there are penalties associated with the policies and procedures, employees should be aware of them. The signed agreement should be kept in the employee's HR file.

  Policies and procedures should be reviewed and updated at least annually and as there are changes in the organization or technology. Whenever the policies are changed, employees should be made aware of the changes and sign the new policy acknowledging their understanding. This can be done in conjunction with annual training activities (see Section 3.2).

3.2 Protect

The Protect Function supports the ability to limit or contain the impact of a potential information or cybersecurity event.[6]

- *Limit employee access to data and information*

  Where possible, do not allow any employee to have access to all of the business's information or systems (financial, personnel, inventory, manufacturing, etc)[7]. Allow employees to access only those systems and only the specific information that they need to do their jobs. Likewise, do not allow a single individual to both initiate and approve a transaction (financial or otherwise). This includes executives and senior managers.

  Insiders – employees or others who work for a business – are a main source of security incidents. Because they are already known, trusted, and have been given access to important business information and systems, they can easily harm the business (deliberately or unintentionally). Unfortunately, these types of events can be difficult to detect, so protecting against them is very important.

  When an employee leaves the business, ensure they no longer have access to the business's information or systems. This may involve collecting their business ID, deleting their username and account from all systems, changing any group passwords or combination locks they may have known, and collecting any keys they were given.

- *Install Surge Protectors and Uninterruptible Power Supplies (UPS)*

  Surge protectors prevent spikes and dips in power from damaging your electronic systems. Uninterruptible Power Supplies (UPS) provide a limited amount of battery power to allow you to work through short power outages and provide enough time to save your data when the electricity goes off. UPS's often provide surge protection as well. The size and type of UPS should be sufficient to meet the needs of your particular business.

  Ensure each of your computers and critical network devices are plugged into a UPS. Plug less sensitive electronics into surge protectors. Test and replace UPSs and surge protectors as recommended by the manufacturer.

[6] The Cybersecurity Framework specifies cybersecurity events only, but can be applied to information security events [CSF14].

[7] The "process of granting access to information system resources only to authorized users, programs, processes, or other systems" is called "access control" [SP800-32].

- *Patch your operating systems and applications*

  Any software application including operating systems, firmware, or plugin installed on a system could provide the means for an attack. Only install those applications that you need to run your business and patch/update them regularly. Many software vendors provide patches and updates to their supported products in order to correct security concerns and to improve functionality. Ensure that you know how to update and patch all software on each device you own or use.

  When you purchase new computers, check for updates immediately. Do the same when installing new software. You should only install a current and vendor-supported version of software you choose to use. Vendors are not required to provide security updates for unsupported products. For example, Microsoft ended support for Windows XP on April 8, 2014 and no new patches will be provided for that operating system, even though it has known vulnerabilities [Msoft WLFS].

  It may be useful to assign a day each month to check for patches. There are products which can scan your system and notify you when there is an update for an application you have installed. If you use one of these products, make sure it checks for updates for every application you use. You can check for updates directly with the original manufacturers of the applications you have installed.

- *Install and activate software and hardware firewalls on all your business networks*

  Firewalls can be used to block unwanted traffic such as known malicious communications or browsing to inappropriate websites, depending on the settings. Install and operate 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. Ensure there is antivirus software installed on the firewall.

  For these devices, change the administrative password upon installation and regularly thereafter. Consider changing the administrator's log-in as well. The default values are typically known or 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.

  In addition, install, use, and regularly update a software firewall on each computer system used in your small business (including smart phones and other networked devices if possible). If given the option, ensure logging is enabled which will aid in the investigation of an event by providing evidence. Many operating systems include a firewall, but you should ensure that the firewall is operating and logging activity [8].

[8] See Microsoft's *Safety & Security Center* [Msoft SSC] and Apple's OSX support page [Apple16].

You should only use a current (updated), authentic, and vendor-supported version of the hardware and software firewall.

It is necessary to have firewalls on each of your computers and networks even if you use a cloud service provider or a virtual private network (VPN). If employees are allowed to do any kind of work at home, ensure that their home network and systems have hardware and software firewalls installed and operational, and that they are regularly updated.

In addition to a basic hardware firewall, you may want to consider installing an Intrusion Detection / Prevention System (IDPS). These devices analyze network traffic at a more detailed level and can provide a greater level of protection.

- *Secure your wireless access point and networks*

  If you use wireless networking, set up your router as follows (view the owner's manual for directions on how to make these changes):

  - Change the administrative password that was on the device when you received it.
  - Set the wireless access point so that it does not broadcast its Service Set Identifier (SSID).
  - Set your router to use WiFi Protected Access 2 (WPA-2), with the Advanced Encryption Standard (AES) for encryption. **Do not use WEP (Wired-Equivalent Privacy)** as it is not considered secure.

  If your business provides wireless internet access to customers, ensure that it is separated from your business network.

  Avoid connecting to unknown or unsecured / guest wireless access points, even for performing non-business activities. Access only those wireless access points that you own or trust (i.e. are assured of their security).

  If you or your employees must connect to unknown networks or conduct work from home, you may want to consider implementing an encrypted virtual private network (VPN) capability, which will allow for a more secure connection.

- *Set up web and email filters*

  Email filters can help remove emails known to have malware attached and prevent your inbox from being cluttered by unsolicited and undesired (i.e. "spam") email. Email providers may offer this capability. If your business hosts your own email servers, use filtering if possible.

  Similarly, many web browsers allow web filtering – notifying the user if a website may contain malware and potentially preventing them from accessing that website. Enable this option if available.

You may want to consider blocking employees from going to websites that are frequently associated with cybersecurity threats. This may include sites with pornographic content or social media. This can help prevent employees from accidentally downloading malware, wasting business resources, and conducting illicit activity using business resources. Many firewalls and routers can be set up to block certain addresses (blacklist), or allow only certain addresses (whitelist). Blacklists can be downloaded online or obtained as part of a service.

- *Use encryption for sensitive business information*

  Encryption is a process of making your electronically stored information unreadable to anyone not having the correct password or key[9]. Use full-disk encryption—which encrypts all information on the storage media – on all of your computers, tablets, and smart phones. Many systems come with full-disk encryption capabilities. Not all mobile devices provide this capability.

  Do not forget your encryption password or key! If you lose or forget your key, you will lose your information. Save a copy of your encryption password or key in a secure location separate from where your backups are stored.

  If, in your business, you send sensitive documents or emails, you may want to consider encrypting those documents and/or emails. Many document, and email applications provide for this capability. Typically, the receiver will need to have the same application to de-crypt the message or document as you used to encrypt it. If you need to send them a password or key, give it to them via phone or other method. Never send it in the same email as the encrypted document.

- *Dispose of old computers and media safely*

  Small businesses may sell, throw away, or donate old computers and media. When disposing of old business computers, first electronically wipe the hard drive(s). Many operating systems provide this capability and there are several downloadable applications that can also do this. If you can't wipe the hard drive for any reason, consider degaussing the hard drive.

  After wiping the hard drive(s), remove them and have them physically destroyed. You can sell, donate, or recycle the machine after the hard drive has been removed. Many companies will crush or shred them for you. Consider choosing companies that will allow you to watch the process.

[9] NIST SP 800-101 Rev. 1, *Guidelines on Mobile Device Forensics*, defines encryption as "Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data" [SP800-101].

Install a remote-wiping application on your computer, tablet, cell phone, and other mobile device. If the device is lost or stolen, you can use these applications wipe all information from the device.

When disposing of old media (CDs, floppy disks, USB drives, etc), first delete any sensitive business or personal data. Then destroy the media either by shredding it or taking it to a company that will shred it for you. When disposing of paper containing sensitive information, destroy it by using a crosscut shredder.

You may want to consider incinerating paper and other media that contains very sensitive information.

- *Train your employees*

  Train employees immediately when hired and at least annually thereafter about your information security policies and what they will be expected to do to protect your business's information and technology. Ensure they sign a paper stating that they will follow your policies, and that they understand the penalties for not following your policies.

  Train employees on the following:

  - What they are allowed to use business computers and mobile devices for, such as if they are allowed to use them to check their personal email.
  - How they are expected to treat customer or business information, for example whether or not they can take that information home with them.
  - What to do in case of an emergency or security incident (see Section 3.4).
  - Basic practices as contained in Section 4 of this document.

  You may be able to obtain training from various organizations, such as your local Small Business Development Center (SBDC), SCORE Chapter, community college, technical college, or commercial training vendors. In addition, the Small Business Administration (SBA) and Federal Trade Commission (FTC) produce videos and topic-specific tips and information which can be used for training [SBA LC] [FTC].

  Continually reinforce the training in everyday conversations or meetings. Monthly or quarterly training, meetings, or newsletters on a specific subject can help reinforce the importance of security and develop a culture of security in your employees and in your business.

3.3 Detect

The activities under the Detect Function enable timely discovery of information security or cybersecurity events.

- *Install and update anti-virus, -spyware, and other –malware programs*

  Malware (short for Malicious Software or Malicious Code) is computer code written to steal or harm[10]. It includes viruses, spyware, and ransomware. Sometimes malware only uses up computing resources (e.g. memory), but other times it can record your actions or send your personal and sensitive information to cyber criminals.

  Install, use, and regularly update anti-virus and anti-spyware software on every device used in your business (including computers, smart phones, and tablets).

  It may be useful to set the anti-virus and anti-spyware software to automatically check for updates at least daily (or in "real-time", if available), and then set it to run a complete scan soon afterwards. Many businesses run their anti-virus programs at some scheduled time each night (e.g. 12:00 midnight) and schedule a virus scan to run about half an hour later (e.g. 12:30 am); then they run their anti-spyware software (e.g. 2:30 am) and run a full system scan (e.g. 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.

  If your employees do any work from home computers or personal devices, obtain copies of your business anti-malware software for those systems or require your employees to use anti-virus and anti-spyware software.

  You may want to consider using two different anti-virus solutions from different vendors. This can improve the chances a virus will be detected. Often routers, firewalls, and Intrusion Detection / Prevention Systems will have some anti-virus capabilities, but these should not be exclusively relied upon to protect the network.

- *Maintain and monitor logs*

  Protection / detection hardware or software (e.g. firewalls, anti-virus) often has the capability of keeping a log of activity. Ensure this functionality is enabled (check the operating manual for instructions on how to do this). Logs can be used to identify suspicious activity and may be valuable in case of an investigation. Logs should be

[10] CNSSI 4009-2015 and NIST SP 800-53 Rev. 4 define Malicious Code as: "Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code." [CNSSI4009, p.79] [SP800-53, p.B-13]

backed up and saved for at least a year; some types of information may need to be stored for a minimum of six years[11].

You may want to consider having a cybersecurity professional review the logs for any unusual or unwanted trends, such as a large use of social media websites or an unusual number of viruses consistently found on a particular computer. These trends may indicate a more serious problem or signal the need for stronger protections in a particular area.

3.4 Respond

The Respond Function supports the ability to contain or reduce the impact of an event.

- *Develop a plan for disasters and information security incidents*

  Develop a plan for what immediate actions you will take in case of a fire, medical emergency, burglary, or natural disaster.

  The plan should include the following:

  - **Roles and Responsibilities**. This includes who makes the decision to initiate recovery procedures and who will be the contact with appropriate law enforcement personnel.

  - **What to do with your information and information systems in case of an incident.** This includes shutting down or locking computers, moving to a backup site, physically removing important documents, etc.

  - **Who to call in case of an incident**. This should include how and when to contact senior executives, emergency personnel, cybersecurity professionals, legal professionals, service providers, or insurance providers. Be sure to include relevant contact information in the plan.

    Many states have "notification laws," requiring you to notify customers if there is a possibility any of their information was stolen, disclosed, or otherwise lost. Make sure you know the laws for your area and include relevant information in your plans.

    Include when to notify appropriate authorities. If there is a possibility that any personal information, intellectual property, or other sensitive information was stolen, you should contact your local police department to file a report. In addition, you may want to contact your local FBI office [DoJ15].

[11] E.g., Patient health records have a retention requirement of "at least 6 years from date of last entry, and longer if required by State statute." 42 C.F.R. §491.10(c), *Patient health records.* Available at: http://www.ecfr.gov/cgi-bin/text-idx?SID=8575b14705ead743d3cbeb9b04fc6896&mc=true&node=se42.5.491_110&rgn=div8 (accessed 10/13/2016).

- **Types of activities that constitute an information security incident**. This should include activities such as your business website being down for more than a certain length of time or evidence of information being stolen.

You may want to consider developing procedures for each job role that describe exactly what the employee in that role will be expected to do if there is an incident or emergency. Appendix E discusses what a procedure document should contain.

3.5 Recover

The Recover Function helps an organization resume normal operations after an event.

- *Make full backups of important business data/information*[12]

  Conduct a full, encrypted backup of the data on each computer and mobile device used in your business at least once a month, shortly after a complete virus scan. Store these backups away from your office location in a protected place so that if something happens to your office (fire, flood, tornado, theft, etc), your data is safe. Save a copy of your encryption password or key in a secure location separate from where your backups are stored.

  Backups will let you restore your data in case a computer breaks, an employee makes a mistake, or a malicious program infects your system. Without data backups, you may have to recreate your business information manually (e.g. from paper records). Data that you should backup includes (but is not limited to) word processing documents, electronic spreadsheets, databases, financial files, human resources files, accounts receivable/payable files, system logs, and other information used in or generated by your business. Back up only your data, not the software applications themselves.

  You can easily store backups on removable media, such as an external USB hard drive, or online using a Cloud Service Provider. If you choose to store your data online, 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.[13]

  If you use a hard drive, ensure it is large enough to hold all of your monthly backups for a year. It is helpful to create a separate folder for each of your computers. When you connect the external disk to your computer to make your backups, copy your data into the appropriate designated folder.

[12] The Cybersecurity Framework defines making backups as a "Protect" activity, and restoring from a backup as a "Recover" activity. For this document, both making and restoring from the backups is listed under "Recover" for simplicity [CSF14].

[13] The Cloud Security Alliance (CSA) provides information and guidance for using the Cloud safely [CSA11].

Test your backups immediately after generating them to ensure that the backup was successful and that you can restore the data if necessary.

- *Make incremental backups of important business data/information*[14]

  Conduct an automatic incremental or differential backup of each of your business computers and mobile devices at least once a week. This type of backup only records any changes made since the last backup. In some cases, it may be prudent to conduct backups every day or every hour depending on how much information is changed or generated in that time and the potential impact of losing that information. Many security software suites offer automated backup functions that will do this on a regular schedule for you.

  These backups should be stored on:

  - removable media (e.g. external hard drive);
  - a separate server that is isolated from the network, or
  - online storage (e.g. a cloud service provider).

  In general, the storage device should have enough capacity to hold data for 52 weekly backups[15], so its size should be about 52 times the amount of data that you have. *Remember this should be done for each of your computers and mobile devices*. You may choose to store your backups in multiple locations (e.g. one in the office, one in a safety deposit box across town, and one in the cloud). This provides additional security in case one of the backups becomes destroyed.

  Periodically test your backed up data to ensure that you can read it reliably. If you don't test your backups, you will have no grounds for confidence that you can use them in the event of a disaster or security incident.

  You may want to consider encrypting your backups. Many software applications will allow you to encrypt your backups. This provides an added layer of security and is important if your backups contain any sensitive personal or business information. Make sure to keep a copy of your encryption password or key in a secure location separate from where you keep your backups.

- *Consider cyber insurance*

  Cyber insurance is similar to other types of insurance (e.g. flood, fire) that you may have for your business. Cyber insurance may help you respond to and recover from a security incident. In some cases, cyber insurance companies may also provide cybersecurity

[14] The Cybersecurity Framework defines making backups as a "Protect" activity, and restoring from a backup as a "Recover" activity. For this document, both making and restoring from the backups is listed under "Recover" for simplicity [CSF14].

[15] Various industries may have specific requirements for how long data backups should be kept, but for cybersecurity, 52 weekly backups provide ability to both recover from and track incidents that weren't noticed immediately.

expertise and help you identify where you are vulnerable, what kinds of actions you need to take to protect your systems, and help you investigate an incident and report it to appropriate authorities.

As you might with any type of insurance, perform due-diligence when considering cyber insurance. Determine your risks (see Section 2) before purchasing a policy. Research the company offering protection, the services they provide, the type of events they cover, and ensure that they have a good reputation and will be able to meet their contractual agreement.

- *Make improvements to processes / procedures / technologies*

  Regularly assess your processes, procedures, and technology solutions according to your risks (see Section 2). Make corrections and improvements as necessary.

  You may want to consider conducting training or table-top exercises which simulate or run-through a major event scenario in order to identify potential weaknesses in your processes, procedures, technology, or personnel readiness. Make corrections as needed.

4 Working Safely and Securely

Many incidents can be prevented by practicing safe and secure business habits. Unlike the previous section, which looked at programmatic steps you can take within your business, this section focuses on every-day activities you and your employees can do to help keep your business safe and secure. While criminals are becoming more sophisticated, most criminals still use well-known and easily avoidable methods. This section provides a list of recommended practices to help protect your business. Each employee should be trained to follow these basic practices.

- *Pay attention to the people you work with and around*

  Get to know them and maintain contact with your employees, including any contractors your business or building may employ (e.g. for cleaning, security, or maintenance).[16] Watch for unusual activity or warning signs such as the employee mentions financial problems, begins working strange hours, asks for a lot of overtime, or becomes unusually secretive. In most cases, this activity is benign, but occasionally it can be an indicator that the employee is or may begin stealing information or money from the business, or otherwise damaging the company.

  Watch for unusual activity near your place of business or in your industry. Similarly, know if other businesses in your area perform any activities which may pose an environmental or safety risk. An event that affects your neighbors may affect your business as well, or indicate new risks in your area, so it is important to remain aware.

- *Be careful of email attachments and web links*

  One of the more common means of distributing malware is via email attachments or links embedded in email. Usually the malware is attached to emails that pretend to be legitimate or from someone you know ("phishing" or "spear phishing" attacks). Links and attachments can be disguised to appear legitimate but in reality download malware onto your computer.

  Do not click on a link or open an attachment that you were not expecting. If it appears important, call the sender to verify they sent the email and ask them to describe what the attachment or link is.

  Before you click a link (in an email or on social media, instant messages, other webpages, or other means), hover over that link to see the actual web address it will take you to (usually shown at the bottom of the browser window). If you do not recognize or trust the address, try searching for relevant key terms in a web browser. This way you can find the

[16] Current or former employees, contractors, or other business partners who have or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems is called "insider threat" (Software Engineering Institute CERT, https://www.cert.org/insider-threat/).

article, video, or webpage without directly clicking on the suspicious link. Train employees to recognize phishing attempts and who to notify when one occurs.

- *Use separate personal and business computers, mobile devices, and accounts*

  As much as possible, have separate devices and email accounts for personal and business use. This is especially important if other people such as children use your personal devices. Do not conduct business or any sensitive activities (e.g. online business banking) on a personal computer or device and do not engage in activities such as web surfing, gaming, downloading videos, etc., on business computers or devices. Do not send sensitive business information to your personal email address.

  Personal or home computers and electronics may be less secure than business systems. Personal devices may be used for web surfing to untrustworthy sites and have untrustworthy applications installed such as games which are not required for work and which add vulnerabilities that a hacker could exploit.

  Some businesses may want to consider using a separate computer that is not connected to any network for certain business functions or for extremely sensitive information. Because most cyber attacks require network connectivity, disconnecting extremely sensitive information from the network prevents these kinds of attacks.

- *Do not connect personal or untrusted storage devices or hardware into your computer, mobile device, or network.*

  Do not share USB drives or external hard drives between personal and business computers or devices. Do not connect any unknown / untrusted hardware into your system or network and do not insert any unknown CD, DVD, or USB drive. These devices may have malware on them. Criminals are known to place USB drives in public places where their target business's employees gather, knowing that curious individuals will pick them up and plug them in. What is on them is generally malware which will spy on or take control of the computer.

  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.

- *Be careful downloading software*

  Do not download software from an unknown web page.

  Only those web pages belonging to reputable businesses with which you have a business relationship should be considered reasonably safe for downloading software.

Be very careful if you decide to download and use freeware or shareware. Most of these do not come with technical support and some do not have the full functionality you might believe will be provided.

- *Do not give out personal or business information*

  Social engineering is an attempt to obtain physical or electronic access to your business information by manipulating people. A very common type of attack involves a person, website, or email that pretends to be something it's not. A social engineer will research your business to learn names, titles, responsibilities, and any personal information they can find. Afterwards, the social engineer usually calls or sends an email with a believable, but made-up, story designed to convince the person to give them certain information.

  If you receive an unsolicited phone call asking for personal information from a company you recognize (such as from your bank or doctor's office), ask for identifying information that only a person associated with the organization would know. If this is not possible, ask the person for their name and office or division and tell them you will call them right back. Call the company using the information from their website or on your contract or bill – do not use any phone number provided by the person who called you. Then ask for the representative who called you.

  Never respond to an unsolicited phone call from a company you do not recognize that asks for sensitive personal or business information. Employees should notify their management whenever there is an attempt or request for sensitive business information.

  Never give out your username or password. No company should ask you for this information for any reason. Also beware of people asking what kind of operating system you use, what brand firewalls you have, what internet browser you use, or what applications you have installed. This is all information that can make it easier for a hacker to break in to your system.

- *Watch for harmful pop-ups*

  When connected to and using the Internet, do not respond to popup windows requesting that you click "OK" for anything. Use a popup blocker and only allow popups on websites you trust.

  If a window pops up on your screen unexpectedly, *DO NOT* close the popup window, either by clicking "okay" or by selecting the X in the upper right corner of the popup window, especially if the pop up is informing you that your system has a virus and suggesting you download a program to fix it. Do not respond to popup windows informing you that you have to download a new codec, driver, or special program for the web page you are visiting. Some of these popup windows are actually trying to trick you into clicking on "OK" which will allow it to download and install spyware or other malware 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.

If you encounter this kind of pop-up window, disconnect from the network and force the browser to close (in Windows, hit "ctrl + alt + del" and delete the browser from running tasks. In OSX, right-click the application in the bar and select "force close"). You should save any files you have open and reboot the computer, then run your anti-virus software.

- *Use strong passwords*

  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[17]. For systems or applications that have important information, use multiple forms of identification (called "multi-factor" or "dual factor" authentication). For example, when a user logs in with a password, they may be sent a text message with a code they have to enter as well. Biometrics (e.g. fingerprint scanners) and other devices may be used, but can be expensive and difficult to install or maintain.

  Many devices come with default administration passwords – these should be changed immediately when installing and regularly thereafter. Default passwords are easily found or known by hackers and can be used to access the device. The manual or those who install the system should be able to show you how to change them.

  Passwords that do not change for long periods of time allow hackers time to crack them and may be shared and become common knowledge to an individual user's coworkers. Therefore, passwords should be changed at least every 3 months[18]. Consider configuring systems and devices to require users to change their passwords every 3 months if possible.

  Passwords to devices and applications that deal with business information should not be re-used. If a hacker gains access to one account, they will have access to all others that share that password. It may be difficult to remember a number of different passwords so a password management system may be an option. However, these systems place all passwords into one place which may be lost or compromised. Carefully compare password management solutions before purchasing.

  You may want to consider using a password management application to store your passwords for you. Ensure the application encrypts all passwords stored on it. Use a strong password on the application and change the password regularly.

[17] NIST SP 800-63-2, *Electronic Authentication Guideline* discusses password entropy [SP800-63].

[18] Ibid.

- *Conduct online business more securely*

  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 or upper left of your web browser window.

  Erase your web browser cache, temporary internet files, cookies, and history regularly. Make sure to erase this data after using any public computer and after any online commerce or banking session. This prevents important information from being stolen if your system is compromised. This will also help your system run faster. Typically, this is done in the web browser's "privacy" or "security" menu. Review your web browser's help manual for guidance.

  If you do online business banking, you may want to consider having a dedicated computer which is used ONLY for online banking. Do not use it for Internet searches, personal banking, or email. Use it only for online banking for the business and disconnect it when not in use.