NISTIR 7621

Small Business Information Security: The Fundamentals

Richard Kissel

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

NISTIR 7621

Small Business Information Security: The Fundamentals

Richard Kissel
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

October 2009

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director

Acknowledgements

The author, Richard Kissel, wishes to thank his colleagues and reviewers who contributed greatly to the document's development. Special thanks goes to Mark Wilson, Shirley Radack, and Carolyn Schmidt for their insightful comments and suggestions. Kudos to Kevin Stine for his awesome Word editing skills.

Table of Contents

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 95% of all businesses. The small business community produces around 50% of our nation's Gross National Product (GNP) and creates around 50% of all new jobs in our country. 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 much 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 small businesses.

Therefore, it is important that each small business appropriately secure their information, systems, and networks.

This Interagency Report (IR) will assist small business management to understand how to provide basic security for their information, systems, and networks.

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 this small business. They expect an appropriate level of security in this 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 requires special protection for confidentiality (to ensure that only those who need access to that information to do their jobs actually have access to it). Some of the information used in your business needs protection for integrity (to ensure that the information has not been tampered with or deleted by those who should not have had access to it). Some of the

1 US Small Business Administration, Table of Small Business Size Standards, http://www.sba.gov/idc/groups/public/documents/sba_homepage/serv_sstd_tablepdf.pdf

information used in your business needs protection for availability (to ensure that the information is available when it is needed by those who conduct the organization's business). And, of course, some information used in your business needs protection for more than one of these categories of information security.

Such information might be sensitive employee or customer information, confidential business research or plans, financial information, or information falling under special information categories such as privacy information, health information, or certain types of financial information. Some of these information categories have special, much more restrictive regulatory requirements for specific types of information security protections. 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 $130.00 per person. If you have 1000 customers whose data ***might have been*** compromised in an incident, then your minimum cost would be $130,000, per incident. Prevention of identity theft is a goal of these laws/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 small 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); there were over 1.6 million new viruses and other malicious programs detected in 2008 (Symantec – Internet Security Threat Report, April 14, 2009). 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 a small 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 the NIST Computer Security web page at: http://csrc.nist.gov.

2. The "absolutely necessary" 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.

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

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

Many commercial software vendors provide adequate protection at a reasonable price and some 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 provides multiple layers of protection (in addition to anti-virus and anti-spyware protection).

You should be able to set the antivirus software to automatically check for updates at some scheduled time during the night (12 Midnight, for example) and then set it to do a scan soon afterwards (12:30am, for example). Schedule the anti-spyware software to check for updates at 2:30am and to do a full system scan at 3:00am. This assumes that you have an always-on, high-speed connection to the Internet. Regardless of the actual scheduled times for the above updates/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.

2.2 Provide security for your Internet connection.

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 hour a day/7 day 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 may be a function of a router provided by the Internet Service Provider (ISP) of the small business. There are many hardware vendors which provide firewall wireless access points/routers, firewall routers, and firewalls.

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, change the administrative password 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) to/from the Internet.

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

Install, use, and keep updated 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. You have to ensure that the firewall is operating, but it should be available.

To check the software firewall provided with Microsoft Windows XP, click on “Start” then “Settings”, then “Control Panel”, then “Windows Firewall”. Select the “General” tab on the top of the popup window. You can see if the firewall is on or off. If it is off, select “On-Recommended” in the hollow circle next to the green check-mark icon.

To check the software firewall provided with Microsoft Windows Vista, click on “Start” then “Control Panel” then “Windows Firewall.” If your firewall is working, you should see a message that “Windows Firewall is helping to protect your computer.” If not, click on ‘Turn Windows Firewall on or off” (in the upper left corner of the window) and select “Turn on firewall.”

When using other commercial operating systems, ensure that you fully review operations manuals to discover if your system has a firewall included and how it is enabled.

There are commercial software firewalls that you can purchase at a reasonable price or free that you can use with your Windows systems or with other operating systems. Again, internet searches and using online/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.

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.

2.4 Patch your operating systems and applications.

All operating system vendors provide patches and updates to their 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. Ensure that you know how to update and patch any operating system you select. Operating system vendors include: Microsoft (various versions of Windows), Apple (Mac OSX, Snow Leopard), Sun (SunOS, Solaris), and sources of other versions of Unix and Linux. Note: when you purchase new computers, update them immediately. Same for new software installation.

For Microsoft Windows XP, select “Start”, then “Control Panel”, then “System”, then “Automatic Updates”. After that, set the day and time to download and install updates. Select “Apply” and click “OK”.

For Microsoft Windows Vista, select “Start”, then “Control Panel”, then “Security”, then “Turn Automatic Updating on or off”. If the circle is marked which says “Install updates automatically (recommended)”, check to see that the day/time tabs are set to “every day” and “11:00pm” or some other convenient time. If the circle is not marked which says “Install updates automatically (recommended)”, then check the circle to activate automatic updates and select “every day” on the left tab, then select an appropriate time (11:00pm is fine) for the right tab. Then, towards the bottom of the window, check

"Recommended Updates" and for "Update Service" check "Use Microsoft Update". Then click on "OK" at the bottom of the window and you are all set for automatic updates for your Windows Vista system.

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

2.5 Make backup copies of important business data/information.

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 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 (for which you should have distribution CDs from your vendor). This automatic backup should be done at least once a week, and stored on a separate hard disk on your computer if not off line using some form of removable media or online storage. The hard disk should have enough capacity to hold data for 52 weekly backups. The size of the storage device 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 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 1000 Gigabytes capacity). On the hard drive, create a separate folder for each of your computers, and create 2 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 this monthly backup for each computer used in your business.

2.6 Control physical access to your computers and network components.

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.

2.7 Secure your wireless access point and networks.

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 it for encrypting your wireless traffic.

2.8 Train your employees in basic security principles.

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.

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

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

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, numbers, and special characters – and are at least 8 characters long.

To better protect systems and information, ensure that all employees use computer accounts which do not have administrative privileges. This will stop 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 which 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.

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

Use good business practices to protect your information. Do not provide access to all data to any employee. Do not provide access to all systems (financial, personnel, inventory, manufacturing, etc) to any 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 already are inside, they are already trusted, and they have already been given access to important business information and systems. So, when they perform harmful actions (deliberately or otherwise), business information, systems, and networks suffer harm. (and, the business itself suffers harm).

3. Highly Recommended Practices

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

3.1 Security concerns about email attachments and emails requesting sensitive information.

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 most 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 in an email.

3.2 Security concerns about web links in email, instant messages, social media, or other means.

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 (for example, 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 Security concerns about popup windows and other hacker tricks.

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 antivirus or antispyware 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.

Most 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.

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 installs 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 on your business computers to help prevent such malicious programs from installing on your systems.

3.4 Doing online business or banking 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 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.

If you use Microsoft Internet Explorer as your web browser, erase the web browser cache, temporary internet files, cookies, and browsing history by selecting "Tools," then "Options," then under the General tab, click on "Delete" (under Browsing History). This will erase your temporary files, history, cookies, saved passwords, and web form information. (These instructions are for Internet Explorer version 7.0 – instructions for other versions of Internet Explorer may be slightly different)

If you use Mozilla Firefox as your web browser, erase the erase the web browser cache, temporary internet files, cookies, and browsing history by selecting "Tools," then clicking on "Clear Private Data" towards the bottom of the popup window. To continue clearing information, click on "Tools", then "Options," then under the Privacy tab, select Show Cookies, then select "Remove All Cookies." This will erase your session information. (These instructions are for Firefox version 3.0 – instructions for other versions of Firefox may be slightly different)

3.5 Recommended personnel practices in hiring employees.

When hiring new employees, 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. You can't afford to hire someone who has a history of past criminal behavior. In some areas, the local police department provides a computer on which to request 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 Security considerations for web surfing.

No one should surf the web using a user account which has 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 has. It is best to set up a special account with "guest" (limited) privileges to avoid this vulnerability.

3.7 Issues in downloading software from the Internet.

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 How to get help with information security when you need it.

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 Service Corps of Retired Executives (SCORE – usually co-located with your local SBDC office) Office for advice and recommendations. You might 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, go to: http://www.ftc.gov/bcp/edu/microsites/idtheft/ - this is the Federal Trade Commission's web page.

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 firms' 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 (Because you probably don't want a firm which set up shop last week).

3.9 How to dispose of old computers and media.

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 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 & media and recycle everything else.

3.10 How to protect against Social Engineering.

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 publically 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.

4. Other planning considerations for information, computer, and network security.

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

4.1 Contingency and Disaster Recover planning considerations

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 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 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 scarce 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.

4.2 Cost-Avoidance considerations in information security.

In Section 1 (Introduction), 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 (perhaps employee health information, employee personally identifiable information, or customer financial information). 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 which is a template to generate financial exposure amounts for different scenarios of data/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 to 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.

4.3 Business policies related to information security and other topics.

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 those information and other resources which 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 violation of the businesses 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 that violates the policies of the business.

To sum it all up: Implementing the best practices described in this publication will help your business cost-avoidance efforts and will be useful as a tool to market your business as one in which the safety and security of your customer's information is of highest importance.

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. **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?
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.

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	**$**	**$**	**$**