Cyber Security for Businesses

Computer crimes involve the illegal use of or the unauthorized entry into a computer system to tamper, interfere, damage, or manipulate the system or information stored in it. Computers can be the subject of the crime, the tool of the crime, or the target of the crime.

As the subject of a crime, a criminal would use your computer or another computer to willfully alter the information stored in your computer, add fraudulent or inaccurate information, delete information, etc. Motives for this include revenge, protest, competitive advantage, and ransom.

As the tool of a crime, a criminal would use a computer to gain access to or alter information stored on another computer. In one common mode of attack a hacker would send a "spear phishing" e-mail to employees who have access to the business bank account. The e-mail would contain an infected file or a link to a malicious website. If an employee opens the attachment or goes to the website, malware that gives the hacker access bank account log-ins and passwords would be installed on the computer. The hacker would then have electronic payments made to accounts from which the money would be withdrawn. Criminals also use computers to commit various frauds and steal identities and other information.

As the target of a crime, computers and information stored in them can be stolen, sabotaged, or destroyed. Sabotage includes viruses, malware, and denial-of-service attacks. Trade secrets and sensitive business information stored in computers can be lost in these kinds of attacks.

Your computers and the information in them should be protected as any valuable business asset. The following tips deal with physical and operational protective measures, Wi-Fi hacking and hotspot dangers, personnel policies and employee training, anti-virus and spyware protection, protecting your bank accounts, use of social media, preventing and dealing with data breaches, and safer use of the Internet. For more details see National Institute of Standards and Technology (NIST) Interagency Report NISTIR 7621 entitled *Small Business Information Security: The Fundamentals*, dated October 2009. It's available online under NIST IR Publications on http://csrc.nist.gov.

Also, consider joining the FBI's InfraGard, a partnership with the private sector with the goal of promoting an ongoing dialogue and timely communications between its members and the FBI. Its members gain access to information that enables them to protect their assets from cyber crimes and other threats by sharing information and intelligence. Go to www.infragard.net to apply for membership.

Physical Protective Measures

- Do not allow unauthorized persons to have access to any of your computers. This includes cleaning crews and computer repair persons.
- Install surface locks, cable locking devices, and fiber-optic loops prevent equipment theft.
- Install computers on shelves that can be rolled into lockable furniture when employees leave their work areas.
- Locate the computer room and data storage library away from outside windows and walls to prevent damage from external events.
- Install strong doors and locks to the computer room to prevent equipment theft and tampering.
- Reinforce interior walls to prevent break-ins. Extend interior walls to the true ceiling.
- Restrict access to computer facilities to authorized personnel. Require personnel to wear distinct, color-coded security badges in the computer center. Allow access through a single entrance. Other doors should be alarmed and used only as emergency exits.

Personnel Policies and Employee Training

Employees can do a great deal of damage to a business by ignorance of security policies, negligence in protecting business secrets, deliberate acts of sabotage, and the public release of sensitive information. The following measures will help prevent this.

- Conduct a comprehensive background check on prospective employees. Check references, credit reports, criminal records, and schools attended.
- Interview prospective employees. Seek to hire individual who are team-oriented, can respond well to criticism, and can deal well with conflicts, i.e., ones unlikely to become insider threats.
- Require vendors, suppliers, and other contractors to use similar standards in hiring their employees. Include language in all contracts that makes contractors liable for actions of their employees.
- Treat all employees fairly and make sure none are teased by their peers or supervisors because of their ethnicity, speech, financial situation, social skills, or other traits.
- Monitor activities of employees who handle sensitive or confidential data. Watch for employees who work abnormally long hours, weekends, or holidays, or who refuse to take time off. Many computer crime schemes require regular, periodic manipulation to avoid detection. Also watch for employees who collect material not necessary to their jobs, such as data printouts, software manuals, etc.
- Train your employees in your basic computer usage and security policies. Also cover penalties for not following your policies, and have employees sign a statement that they understand and will follow your policies.

- Train your employees about security concerns and procedures for handling e-mails, clicking on links to websites, responding to popup windows, and installing infected USB drives. For example, they should not: open e-mail from an unknown sender, open unexpected e-mail attachments, click on any links in e-mail messages even if they look real, respond to popup windows, bring back and install "found" USB drives, etc.
- Train your employees to be aware of what others are doing and to report any suspicious behavior that threatens your security.
- Conduct periodic re-training because people forget things. Use pamphlets, posters, newsletters, videos, etc.

Preventing and Dealing with Data Breaches

The five key principles defined by the Federal Trade Commission in its video entitled *Protecting Personal Information: A Guide for Business* at http://business.ftc.gov/privacy-and-security/data-security will help you protect personal information in your business and prevent data breaches. They are: (1) Take stock, (2) Scale down, (3) Lock it, (4) Pitch it, and (5) Plan ahead. You should do the following for each.

1. **Take Stock.** Know what personal information you have in your files and in your computers.
    - Inventory all file-storage and electronic equipment. Know where your business stores sensitive data.
    - Talk to your employees and outside service providers to determine who sends you personal information and how it is sent.
    - Consider all the personal information you collect from customers, and how you collect it.
    - Review where you keep the information you collect, and who has access to it.
2. **Scale Down.** Keep only what you need for your business.
    - Use Social Security Numbers (SSNs) only for required and lawful purposes. Don't use them for employee or customer identification.
    - Keep customer credit or debit card information only if you have a business need for it. Don't keep any information you don't need.
    - Change the default settings on your software that reads customer's credit or debit cards.
    - Review the credit application forms and fill-in-the-blank web screens you use to collect data from potential customers, and eliminate requests for any you don't need.
    - Use no more that the last five digits of credit or debit card numbers on electronically printed receipts that you give to your customers. And don't use the card's expiration date.
    - Develop a policy for retaining written records that is consistent with your business needs and the law.
3. **Lock It.** Protect the information that you keep and transmit.

- Keep documents and other materials containing personal information in locked rooms or file cabinets.
- Remind employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Create a security policy for your employees when using laptops in and out of your office. (See prior section on Special Measures for Laptops.)
- Control access to your building.
- Encrypt sensitive information you send over public networks or use a secure file transfer service. Don't send personal information by e-mail.
- Run up-to-date anti-virus and anti-spyware programs on all your computers. Use a firewall to protect your computers and network. (See prior section on Anti-virus and Spyware Protection.)
- Require employees to use strong passwords.
- Set access controls so employees only have access to information they need for their jobs. (See prior section on Procedural and Operational Protective Measures.)

4. **Pitch It.** Properly dispose of what you no longer need.
    - Create and implement secure information disposal practices for employees in your office and for those who travel or work at home.
    - Train your staff to separate sensitive and other paper records. Dispose of the former by shredding, burning, or pulverizing them. Use cross-cut shredders. The latter can be put in the trash.
    - Make shredders available throughout your office, especially next to the copiers.
    - Remove and destroy the hard disk of any computer or copier headed for the junkyard. Or wipe them securely.
    - Remove and securely wipe hard drives of rented copiers before returning them. Or clear the memory and change the pass codes.
    - Destroy CDs, floppies, USB drives, and other data storage devices, or securely wipe them before disposal.
5. **Plan Ahead.** Create a plan for dealing with security breaches.

    In addition to having plans to protect personal information and prevent breaches, businesses should have response plan to deal with possible breaches. Wisconsin requires businesses to notify persons whose personal information has been compromised in a security breach and the specific information involved. The notice requirement is triggered if the breach involves a person's name in combination with any of the following: Social Security Number; driver's license; financial account, credit card, or debit card number along with any PIN or other access code required to access the account; medical information; or health insurance information. The letter of notice should also recommend measures to take to deal with the breach.

- Organize a response team and designate a team leader to manage the activities.
- Draft contingency plans for dealing with various kinds of breaches, including hacking, lost laptop, etc.
- Investigate breaches immediately.
- Disconnect a compromised computer from the Internet.
- Create a list of who to notify inside and outside of your business in the event of a breach. The latter include the appropriate law enforcement agencies, the persons whose information has been compromised, and the media.
- Draft notification letters and other written communications.
- Consider what outside assistance is needed, e.g., in forensics, media relations, etc.

Procedural and Operational Protective Measures

- Classify information into categories based on importance and confidentiality. Use labels such as "Confidential" and "Sensitive." Identify software, programs, and data files that need special access controls. Employee access should be limited to what he or she needs to do their jobs. No employee should have unlimited access.
- Install software-access control mechanisms. Require a unique, verifiable form of identification, such as a user code, or secret password for each user. Install special access controls, such as a call back procedure, if you allow access through a dial telephone line connection.
- Have your Information Technology (IT) manager change administrative password on a regular basis. A number of free tools are available for this if manual modification is not practical. This password should also be changed during non-business hours.
- Require that passwords consist of a random sequence of at least eight letters, numbers, and special characters. Passwords should be changed at least every three months and not be shared.
- Employee user accounts should not have administrative privileges. This will prevent the installation of any unauthorized software or malicious code that an employee might activate.
- Change security passwords to block access by employees who change jobs, leave, or are fired. The latter become a high risk to your business for revenge or theft.
- Encrypt confidential data stored in computers or transmitted over communication networks. Use National Institute of Standards and Technology (NIST) data encryption standards.
- Design audit trails into your computer applications. Log all access to computer resources with unique user identification. Separate the duties of

systems programmers, application programmers, and computer programmers.
- Review automated audit information and control reports to determine if there have been repeated, unsuccessful attempts to log on both from within and outside your facility. Look for unauthorized changes to programs and data files periodically.
- Use monitoring or forensic tools to track the behavior of employees suspected of malicious activities.
- Monitor incoming Internet traffic for signs of security breaches.
- Make backup copies of important business information, i.e., documents, spreadsheets, databases, files, etc. from each computer used in your business. This is necessary because computers die, hard disks fail, employees make mistakes, malicious programs can destroy data, etc. Make backups automatically at least once a week if possible. Test the backups periodically to ensure that they can be read reliably. Make a full backup once a month and store it in a protected place away from your business.
- Delete all information stored in your printers, copiers, and fax machines at least once a week. Use a secure data deletion program that will electronically wipe your hard drives. Simply hitting the delete key will leave some data on the hard drive.
- Be careful in getting outside help with computer security problems. Start with a list of vendors or consultants. Then define the problem, send out a request for quotes, examine each quote, and check the provider's references and history before hiring one.
- If you become a victim of Internet fraud or receive any suspicious e-mails you should file a complaint with the Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center (NW3C), at www.ic3.gov. The IC3 website also includes tips to assist you avoiding a variety of Internet frauds.

Protecting Bank Accounts

- Set up dual controls so that each transaction requires the approval of two people.
- Establish a daily limit on how much money can be transferred out of your account.
- Require all transfers be prescheduled by phone or confirmed by a phone call or text message.
- Require that all new payees be verified.
- Check bank balances and scheduled payments at the end of every workday, rather than at the beginning, and contact the bank immediately if anything is amiss. Timely action can halt the completion of a fraudulent transaction because transfers usually aren't made until the next morning. Inquire about your bank's defenses against cyber attacks and review the

terms of your banking agreement with regard to responsibilities for fraud losses. Shop around for banks that provide better protections.
- Conduct online business only with a secure browser connection, which is usually indicated by a small lock in the lower right corner of your web browser window. Erase your browser cache, temporary Internet files, cookies, and history after all online sessions. This will prevent this information from being stolen if your system is compromised.

Special Measures for Laptops

Special security measures are needed for laptops to reduce the threat from determined thieves.

- Issue desktops instead of laptops to employees who seldom leave their offices.
- Have employees lock up their laptops when they are left unattended in their offices. Never leave laptops unguarded.
- Have employees carry their laptops in a sports bag or briefcase instead of the manufacturer's bag.
- Do not leave laptops in vehicles.
- Determine if employees need all the data on their laptops to perform their jobs. Remove any data that is not needed.
- Train employees in the need for special measures to protect laptops and their data wherever they may be used.
- Create a loss response team to monitor compliance with laptop and data security measures, investigate losses, assess data needs, and remove data no longer needed.
- Protect data with strong passwords.

Other measures should be considered to protect your business in the event a laptop is lost or stolen.

- Have employees back up their files so they can be recovered if their laptop is lost or stolen.
- Don't store passwords on laptops.
- Encrypt all sensitive information so it cannot be compromised.
- Keep a record of all laptop model and serial numbers, and makes so if one is recovered you can prove it is yours.
- Place stickers on the laptops with a phone number to call if one is lost and found by an honest person. But don't put the name of your employee or business on it. That information could be used by criminals to guess passwords or assess the sensitivity of the data stored on the laptop.
- Install hardware, software, or both to aid in recovery of the laptop. After you report the laptop lost or stolen the software enables a monitoring company to track the laptop when the thief logs onto the Internet.

Hardware systems work the same but have a Global Positioning System (GPS) device that can pinpoint its location.
- Install software that will enable you to erase sensitive information when the thief logs onto the Internet.

Use of Social Media

While the use of social media can stimulate innovation, create brand recognition, generate revenue, and improve customer satisfaction, it has inherent risks that can negatively impact business security. Thus businesses need to develop a social media strategy and a plan to address these risks. Some risk mitigation techniques for business and employee use of social media are listed below.

- Ensure that anti-virus and anti-malware controls are updated daily.
- Use content filtering to restrict or limit access to social media sites.
- Establish policies for the use of mobile devices to access social media. Install appropriate controls on mobile devices.
- Conduct awareness training to inform employees of the risks in using social media.
- Provide employees with clear guidelines regarding what information about the business can be posted.
- Scan the Internet for unauthorized or fraudulent use of the business name or brand.