Security Squad

Keeping your Equipment and Information Safe

Supplemental Planning Workbook

Security Squad Video Series

University of Nebraska Lincoln EXTENSION

SRDC

Acknowledgements

The Security Squad video series was produced to help the small business owner using technology in their business operations and online connectivity for customer relations and sales. The video series and planning tool will help you address areas that affect the security of your business and customer information.

Authors

Marilyn Schlake, Associate Director, NebraskaEDGE, Department of Agricultural Economics, UNL

Connie Hancock, Extension Educator, Extension Service, UNL

Diane Becker, Owner, BKRDesign.com

Mark Hendricks, Multimedia Information Specialist, Department of Communications and Information Technology, UNL

Video Production

Mike Kamm, Production Specialist, Department of Communication and Information Technology, UNL

These materials were developed by the University of Nebraska-Lincoln as part of the Southern Rural Development Center's National e-Commerce Extension Initiative. They are based upon work supported by the **Cooperative State Research, Education, and Extension Service, U.S. Department of Agriculture**, under Award No. 2005-45064-03212

Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the view of the U.S. Department of Agriculture or the Southern Rural Development Center.

Table of Contents

Plan Overview

Welcome to the Security Squad's Video Series on how to keep your equipment and information safe. As a business owner, there are numerous actions that will help you minimize or eliminate equipment, data and identify theft that threatens you and your customers. The Security Squad's Video Series will provide you with general equipment and data safety information. The Security Squad Supplemental Planning Workbook provides the action tools to help you develop and implement a security plan for your own business.

Why Develop a Security Plan?

For a small business, a breach in data security can result in serious financial consequences. In the Ponemon Institute's Fourth Annual Cost of Data Breach, February, 2009 researchers found the average cost of a data breach was $202 per customer record in 2008. Survey results also showed that 88% of the businesses reported losses due to insider negligence and 36% reported losses due to a lost laptop, PDA or mobile phone. Although only 12% of data breach incidents were from malicious attacks, these costs were greater, averaging $225 per customer record. Besides the costs associate with handling customer data, your company could also incur greater losses if it is proven your business was negligent in protecting the customer data.

The 2009 NCSA/ Symantec Small Business Study conducted by National Cyber Security Alliance, Symantec™, and Zogby International showed how the lack of good business security practices open the door to potential security breaches:

- 66% of employees had mobile computers or PDAs that were taken off business premises with sensitive information.
- 70% of the companies did not have a formal Internet security policy.
- 28% of the companies did not regularly check their computers for anti-virus, anti-spyware, firewalls and operating system updates.
- 59% of the firms did not provide Internet safety training for their employees.
- 35% of the companies did not have any policies in place to protect customer, business or personal data.

According to the National Cyber Security Alliance, protecting your business starts with three critical tasks, steps that will be addressed in the Security Squad Series.

- Assess Risks
- Monitor Threats to Business
- Draft Cyber Plan

How to Use the Security Squad Videos and Worksheets

The following topics are covered in different Security Squad videos. Each video and its corresponding workbook section will highlight topic points and provide steps to help you implement the key action steps.

1. Security Plan Components
2. Equipment and Software Inventory – Tallying What You Have
3. Passwords – Creating Strong Passwords
4. Backups – Making Secured Copies

5. Viruses – Protecting Your Office from Malware
6. Wireless -- Limiting Your Exposure
7. Firewalls – Stopping Hackers at the Door
8. E-commerce – Buying and Selling Safely Online
9. Employee Policies – Protecting the Company and Your Employees

Once you have completed all nine videos and workbook sections, you will have a security plan document that can be shared with employees for buy-in and implementation.

Developing the Security Team

Whether you are a one person business or have multiple employees, deciding who should be involved in the development of your security plan can determine how successfully the plan will be implemented and maintained. The goal of the security plan is not to completely eliminate all risks at whatever cost, but to develop a system that helps to minimize the risks and potential losses to the company and its employees. Following are some basic guidelines for developing a successful security team.

Project Leader or Company Owner Responsibilities:

- Organize a team, include employees and/or consultants who have the skills and interest to help with the project.
- Clearly define roles and responsibilities of team members.
- Create a project time line and budget for project completion.
- Communicate recommendations, train staff and monitor implementation.
- Allocate monies to support security team recommendations.

Team Responsibilities:

- Bring knowledge and skills to the team to help accomplish tasks.
- Evaluate current security status of company data and equipment.
- Develop new security requirements and implement security protocols.
- Develop protocols for maintaining new levels of security.
- Develop procedures for reporting and responding to security incidents.
- Help implement and monitor recommended policies.
- Seek additional training as needed.
- Maintain team commitment to security, modify plan as needed.

The information provided in the Security Squad Video Series and Supplemental Workbook is a general guide to help you improve your data and equipment security protocols. At the end of the workbook is a list of additional resources that will assist you in developing and customizing your security plan to best meet your company's needs.

This is your Security Squad saying –
"Don't gamble with your business. Keep your office data safe and secure!"

Equipment & Software Inventory

Tallying What You Have

What's the Security Risk?

The phone rings at 2:00 a.m. and it's the police calling to let you know that someone has broken into your office and they want you to identify missing items. You also know the insurance company will want a list of everything that is missing. Where do you begin? Do you have a record of all the electronic devices in your office? Do you have a list of the software that you own? Do you realize how many items carry confidential information about your business? Not knowing can put your business at risk.

Keeping track of all data storage equipment is a good idea for any business, this is especially important for companies with employees who use small mobile devices and have online access. Equipment can become lost, stolen or damaged, computers can be hacked and employees can steal. If the equipment is compromised, so is the data that goes with it. The consequences can be minimal to catastrophic for the business. As the owner, you can expect hours or weeks of re-constructing work, customer order delays, lost customer contact information, lost or compromised financial information, or worse compromised customer information that results in lost customers and their trust in your business.

Keeping track of your equipment and software is a good way to prepare for the unexpected. The inventory list can be extensive if the business has multiple data storage items such as computers, portable devices, point-of-sale machines, network equipment, and cell phones. It's very important to have this information recorded and stored someplace off-site and secured. The equipment and software inventory lists are helpful for submitting insurance claims and determining replacement costs of equipment and software.

Key Points to Consider

- Each device has an identification serial number used for service contracts and manufacturer registrations. Locate and record the number on the equipment inventory list.
- Software can be expensive to replace, find the serial number or key code to verify your original purchase of the product. Record the number on the software inventory list.
- Store an electronic and printed copy of the updated inventory lists away from the office, i.e., at home, bank deposit box and any other trusted and secured location.
- Label equipment with something permanent such as an etching tool.
- Have a plan to regularly update the equipment and software inventory lists and assign a person responsible for maintaining the lists.
- Use an inventory management software, the Security Squad inventory lists or another type of listing method that works for you.

Current Situation

Review your current inventory methods. Do your current methods answer the questions, what do we have, when was it purchased, who uses the software and equipment, who is responsible for cataloging the equipment, and where are the inventory lists securely stored? Complete the Situational Analysis to better understand your current situation and identify where improvements can be made to secure your equipment, software and data.

SITUATIONAL ANALYSIS – EQUIPMENT AND SOFTWARE INVENTORY CHART

Briefly describe your company's current inventory tracking system:		
Problems/shortfalls of the current inventory system or areas that need improvement:		
Current person responsible for maintaining inventory lists:	How often inventory lists are updated:	□ Monthly □ Quarterly □ Semi-annually □ Annually □ Occasionally □ Never
Current time committed to list maintenance: ________ hours	Budget allocated to list maintenance:	$__________
Resources dedicated to inventory maintenance: □ Inventory maintenance software □ Etching tool/equipment identification method □ Safety deposit box or other method for securing inventory lists □ Dedicated staff for developing and maintaining inventory lists		

Inventory Plan of Action

With your Security Team work through the brief Inventory Plan of Action on page 7 to develop the guidelines for getting your equipment and software inventory completed. The chart will help you identify staff responsible and resources allotted to complete your inventory lists.

PLAN OF ACTION: INVENTORY

Inventory activities to be completed:	□ Equipment Inventory List □ Software Inventory List
Person responsible for completing lists:	Date inventory lists are to be completed:
Est. time to develop inventory lists:	____________ hours
Person responsible for maintaining inventory lists:	Update inventory lists every: □ Month □ Quarterly □ Semi-annually □ Annually
Est. time to maintain inventory lists:	____________ hrs.
Resources –Software/equipment needed for project completion. (Check only if budget allows purchase and scale of project justifies investment.) □ Inventory maintenance software □ Etching tool/equipment identification method □ Safety deposit box or other method for securing inventory list □ Other ______________________________	
Budgeted Resources: □ Staff time □ Equipment □ Outside Technician	Initial work $____________ Maintenance $____________ $____________ $____________ **Total** **$____________**

Action Worksheets

The Security Squad Equipment Inventory List on page 8 and Software Inventory List on Page 9 are examples that can be used to list your equipment and software. Blank fill-in inventory lists are available on pages 35 & 36. You can also make additional copies of the list as needed, duplicate the forms on your own computer or purchase an inventory maintenance software for cataloging your equipment. The objective is to use a method that gets the list completed and safely secured.

Note: You may choose to assign numbers to easily identify similar pieces of equipment or if your inventory is large and dispersed. Be sure to include all your equipment that holds data.

Equipment Inventory List
(Company)
Updated: __/__/20__

Description	Model	Date Purchased	Purchase Price	Serial Number	MAC Address	IP Address – Static or Registered	Location	Primary User/s	Warranty Date
Ex – Computer #5	Gateway 5300	June 2009	$1200	44235639485	00-00-5A-99-62-50	131.255.82.77	Room C	Nancy Anybody	June 12, 2012
Ex – Monitor #3	Dell 15”	Oct 2007	$325	13102D1039			Room D	Charlie Anybody	Oct 31, 2009
Ex - Printer #67	Hewlett Packard C6300	Jan 2008	$900	JD0X31099		131.255.82.78	Main Office	Prints from computers #5,#2 and #4	Jan 24, 2010
Ex - PrintServer#2	Linksys Wireless-G	Oct 2004		64524569584			Room B	All wireless capable computers have access	
Ex - Credit Card Reader #1	VeriFone Vx510	Dec 2008		10190810qp1			Front Counter	Cashier, Jane Summers	
Copy Machine									
Mobile Phone									
PDA									
External Hard Drive									
DVD									
Flash Drive - X									
Router									
Switch									
Camera - X									
Digital Camera									
VCR									
TV									

Software Inventory List
(Company)
Updated: __/__/20__

Description	Version	Date Purchased	Purchase Price	Operating Software & license, serial number or keycode	Download or CD's	Primary User/s	Location
Ex – Microsoft Office 2007	2007	June 2009	$250	Lkj-lda-09s-f922-fHka-923	CD's	Nancy Anybody	Room C
Ex – Open Office	3.01	May 2008			Openoffice.org	Charlie Anybody	Room D
Symantec Norton Anti-virus	4.0	June 2010	$80	Ake-d9s-geFs-J1014-keu	www.symantec.com	All computers	

Creating Strong Passwords

What's the Security Risk?

Anymore, we need a lot of passwords. We need to enter a password before we can use our online banking, access email, get onto Facebook™, buy plane tickets online and pay your bills. It's tempting to use the same password over and over, and that's what most of us do. It seems to work fine, except for when a hacker discovers that password and is able to access all of our personal and financial information.

For a business, identification and authentication procedures are your first line of defense, which includes setting up passwords for each and every person who logs onto the computer or network. The stronger the passwords, the less chance a hacker who is using a password-cracking software can break your passwords and access the system. Password-cracking software uses either intelligent guessing, dictionary words, or a system that tries every possible combination of characters. With enough time, an automated password cracker will succeed every time.

Once a hacker does gain access through a password, it is very difficult to prevent damage or further penetration of the system. They can access any file within the computer or system, change data, capture other passwords and erase files, sometimes without you even knowing this is happening. The loss to your company can be significant!

Besides the hackers gaining access to passwords through the computers, they also attempt to capture information through trickery in telephone conversations, emails, and social network dialog. Create strong employees policies that state no passwords or business information is to be provided, unless approved by the owner. Caution must be practiced at all times. If it looks suspicious, it probably is.

Key Points to Consider

- Always use strong passwords that have a combination of random letters, numbers and symbols and are at least 8 characters long. Do not use complete words found in the dictionary, names, teams, abbreviations, movie stars, TV shows, or hobbies. *Junebug24* is not a strong password; but *J*9!b$G!* would certainly be more difficult to crack.
- Strong passwords can be difficult to remember. If you must write down your passwords, store the paper in a secure place and destroy it when it is no longer needed. Consider purchasing commercial or shareware password lock software that encrypts and securely stores all your passwords. You need to remember only one very strong password to access the others.
- Password generators can assist in developing very strong passwords. Password lock software includes this option, or check out these websites:
    - PC Tools™ Password Generator: http://www.pctools.com/guides/password/
    - Online Password Generator: http://www.onlinepasswordgenerator.net/index.php
- Be careful about where passwords are saved on computers. Do not use the "Remember Password" feature of applications.

- Passwords should be treated as confidential information. Never share passwords with anyone.
- Use different passwords for all user accounts. Do not use the default password that comes with an application, change the password the first time you are asked to use it.
- Install password-activated screen savers that lock employee computers when not in use and lock out users after numerous failed attempts to enter a correct password.
- Change passwords immediately if you think they have been compromised.

Current Situation

Review your current password security levels. Given the key points above, does your company have strong passwords, employee policies preventing shared passwords, and protocols that help prevent password theft? Complete the below Situational Analysis to better understand your current situation and identify where improvements can be made to secure your equipment, software and data.

SITUATIONAL ANALYSIS – PASSWORD PROTECTION

Briefly describe your company's current password protection levels and employee policies:

Problems/shortfalls of the current password protection levels or areas that need improvement:

Current person responsible for implementing/maintaining password security:

How often reviewed
□ Monthly
□ Quarterly
□ Semi-annually
□ Annually
□ Occasionally
□ Never

Resources dedicated to password protections:
□ Password generation software/website use
□ Password activation screensavers
□ Other ______________________________

Current time committed to installing added password protection: _______ hours

Budget allocated to activity: $________

Password Plan of Action

With your Security Team discuss your password protocols. Complete the Plan of Action chart on page 12 to develop the guidelines for setting up added password protections. The chart will help you identify staff responsible and resources allotted to create strong business passwords.

PLAN OF ACTION - PASSWORDS

Password activities to be completed:	□ Update or set new protocols for computers/PDAs/mobile phones □ Update employee policies
Person responsible for completing activities:	Date password security is to be completed:
Est. time to complete activities:	____________ hours
Person responsible for reviewing and updating activities:	Review protocols: □ Monthly □ Quarterly □ Semi-annually □ Annually
Resources –Software/equipment needed for project completion. (Check only if budget allows purchase and scale of project justifies investment.) □ Password software, purchased or shareware □ Password screen-savers □ Other ______________________________	
Budgeted Resources: □ Staff time □ Equipment □ Outside Technician	Initial work $____________ Maintenance $____________ $____________ $____________ **Total** **$____________**

Additional Resources

"Password Management Best Practices." University of Nebraska. http://cit.information.unl.edu/tips/passwordmanagement.htm.

"System Administrator Security Best Practices." SANS Institute, InfoSec Reading Room. http://www.sans.org/reading_room/whitepapers/bestprac/system_administrator_security_best_practices_657?show=657.php&cat=bestprac.

Making Secured Copies

What's the Security Risk?

Unfortunately, accidents do happen! Consider the personal and financial loses you could incur should any of these scenarios happen to you. Backup CDs are left on a heated car seat and melted and your data is unrecoverable. A natural disaster such as a tornado, lightning strike, flood or fire hits your home or business and your equipment is useless. A computer virus, low voltage, or hard drive failure causes your computer's mother board to fail so the system won't boot. Or, consider an employee stealing your equipment or a hacker breaking into your network and deleting, or worse, stealing your data.

Data loss is basically a fact of life. It will happen, unless you are prepared. By making regularly scheduled backups of your data and storing it securely, you can save thousands of dollars and countless hours needed to recreate your financial accounts, customer lists, on-going projects, and other vital business information you need to operate your business. Don't become a business statistic.

> "50% of small businesses that experience a major data loss go out of business within a year."
> - Gartner Group

Key Points of Consider

- Methods for computer backup.
  - **How often.** First determine the critical loss point or just how long the business can go without computer use. This will help you decide how often to backup your system. For example, if the business has a few invoices once a week and the computer is not used for daily records, then the system may need to be backed up once a week or maybe once a month. However, if sales, inventory levels, customer orders, and critical projects are processed daily, then the system will need to be backed up daily. Waiting a week to backup heavy data use can be a critical mistake.
  - **Pre-installed option.** The latest Windows and Mac operating systems have pre-installed programs that automate the backup and restore processes for you. You do have to set it up. If you have an older computer system, you can purchase inexpensive software that performs the same functions of backing up, compressing, encrypting files and restoring files.
  - **Multi-layer backup**. A good backup plan should rely on a multi-layer system that allows for incremental backups. This adds another layer of precaution should one system fail. If you plan to backup daily, you will want to have two or three tapes, disks, flash drives, or an external drive that is rotated between backups.
    - For example, you could use a disk labeled "daily backup" to run at the end of each day, rotating between two disks. At the end of the week, you then backup the entire week's work on another system labeled "weekly backup", again rotating or creating new dated backup files each time. These incremental backups will only copy what information was added or changed during the designated time frame.

  - **Only backup changed files**. To save space, only backup data that is frequently changed such as address books, word processing documents, bookkeeping files, spreadsheet files, database info and picture files. Program software does not need to be copied.
  - **Entire system backup.** An entire backup should be completed periodically, quarterly, semi-annually or annually, depending on your volume and use. Backing up program software is optional.
- Backup storage options.
  - **USB, DVD or Flash drives**. There are several options to consider for backing up your files. The method you select will depend on the volume of data to be stored, the user convenience and cost. For all backup storage devices, plan to store them in a safe place such as a fireproof safe or off site in a safety deposit box or safe in your residence. Remember, your data is valuable!
    - USB flash drives are available in various sizes, from 1 gigabyte to as large 32 gigabytes. Of course, the price also increases with the increased amount of available storage. Flash drives are very convenient to use. However, they are small and can easily 'walk away', or get lost.
    - DVDs are more reliable to use than flash drives. Standard storage capacity is 4.7GBs or 8.5GBs. Large volume storage will require multiple DVDs that are properly stored and labeled. DVDs are an inexpensive storage option.
    - External hard drives are very popular for holding large volumes of data. For less than $150, you can purchase an external hard drive that holds 1 terabyte of data – more than enough space for most small business needs. Heat is a problem for external drives. Use the drive in a well-ventilated area and make sure the exhaust vents are unobstructed
  - **Online backup services.** Storing your data off-site is a convenient option. Services such as Mozy™, Carbonite™, or Quicken™ offer customer data storage for a fee.
    - Security during data transmission and storage are two key factors you must consider when selecting your online service. Look for a service that has end-to-end encryption - data is encrypted when transmitted from your computer to their server and is encrypted while stored on their server.
    - Online service performs like an external backup system. You can restore a file, the entire directory or the whole contents of your computer according to what you need.
    - The disadvantages of an online system are that it does take larger bandwidth to upload and download the files and the computer must be connected to the Internet during the pre-scheduled back up times.
    - Some online backup services only allow a limited number of restored files, at their base price. Watch for added fees.
    - Cloud computing, the newest backup and data storage option, may be an option for on-the-go staff. Cloud computing allows users to access their information from any Internet ready device, anywhere, anytime.

- Periodically, test your backups by restoring them onto a test location. This will alert you to any potential problems with your backup system and the restoration process.

Current Situation

Review your current backup methods. Are files backed up often enough-daily, weekly, or monthly? Are they backed up by different methods so that if one failed, the files are available on another storage device? Where are current backups stored? Who has been in charge of backing up files?

SITUATIONAL ANALYSIS – BACKUPS

Briefly describe your company's current backup practices and policies:		
Problems/shortfalls of the current backup system or areas that need improvement:		
Current person/s responsible for implementing/maintaining computer backups:	How often backups are performed and checked	□ Daily □ Weekly □ Monthly □ Annually □ Occasionally □ Never
Current resources dedicated to backup protection: □ Number of external drives _________ DVDs, _________ Flash drives, ______ External hard drives □ Online backup services □ Other _____________________________________		
Current time committed to securing backups: _________ hours	Budget allocated to activity: $____________	

Backup Plan of Action

With your Security Team decide what files need to be backed up and how often. Consider your storage needs and costs to be dedicated to securing your backups. Complete the Plan of Action chart below to develop the guidelines for developing your backup system. Make a schedule for when files will be backed up and who will be responsible for the process. Set up automatic backups when possible. The chart will help you identify staff responsible for the project and resources allotted for the activity.

Plan of Action - Backups

Backup activities to be completed:	□ For each computer, determine what files need to be backed up. □ Determine storage needs □ Develop backup protocols for each computer □ Implement plan	
Person responsible for completing activities:	Date backup plan to be completed:	
Est. time to complete activities:	____________ hours	
Person responsible for reviewing and updating activities:	Review backup protocols:	□ Monthly □ Quarterly □ Semi-annually □ Annually
Resources –Software/equipment needed for project completion. (Check only if budget allows purchase and scale of project justifies investment.) □ Purchase backup storage: DVDs, Flash drives, External drive □ Purchase online backup services □ Purchase backup software to help schedule backups □ Other ____		
Budgeted Resources: □ Staff time □ Equipment □ Outside Technician	Initial work $____________ Maintenance $____________ $____________ $____________ **Total $____________**	

Additional Resources

Kissel, Joe. "Creating a Backup Policy: Design and document an effective backup system for your business. MacTech." The Journal of Apple Technology. http://www.mactech.com/articles/mactech/Vol.24/24.08/CreatingaBackupPolicy/index.html.

What's the Security Risk?

There are over one million malicious codes ready to attack your computer system every day. Malware can gain access to your computer through websites, downloads, and email. They can spread through shared drives and explode over office networks. They cause computers to become slow and unresponsive; they redirect your programs to undesirable websites; and worse, they render computers useless. Some malware will also take over your computer, access your email addresses and send out spam under your name to unsuspecting customers and vendors – an embarrassing and costly problem.

According to the 2008 Symantec™ Internet Security Threat Report, the United States was the top ranking country of attack in 2008, accounting for 25% of all worldwide attack activity. Most of the data breaches led to identity theft or identity exposure. The cost of data loss to companies has been staggering. Computer Economics, Inc. reported that in 2006, the worldwide economic lost due to malware was $13.3 billion. In the United States, the average 2007 loss was $350,424 per company, as determined by the Computer Security Institute. Even though your company may not be a large corporation, your data is just as vital to you and your customers.

Key Points to Consider

Malware, short for malicious software, is designed to infiltrate a computer without the owner's consent. In general terms it is defined as annoying software or program code and includes viruses, spyware, adware, and hacker tools. Definitions of the different types of malware are provided in the **Definitions** section, pages 18 & 19.

- Anti-Virus software musts
  - It is absolutely necessary to install anti-virus software on **each** desktop and laptop computer within the company. Purchase "business packs" for volume pricing.
  - Schedule the anti-virus software to receive and install updates as they come available.
  - Do not install two anti-virus software packages to "double" your protection. Select one highly recommended software and use it.
  - Set the anti-virus software to scan incoming files such as those downloaded from the Internet, incoming from an email, or on a removable drive. Depending on your software you will want to periodically conduct a full scan or "sweep" of your computer.
  - If your anti-virus software was not correctly updating to include the latest virus protections, you should conduct a full scan of your computer and correct the software problem.

- Computer updates musts
    - Hackers look for vulnerabilities in operating systems. To make sure **<u>each</u>** computer has the latest vulnerability "fix or patch," configure the computer to automatically download and install updates.
        - In Windows, go to the Control Panel and open the Security Center. You will select "automatic updates and installation" option. This will tell your computer to seek out any updates as they come available.
- Good anti-virus prevention practices
    - Never open an attachment on an email that you did not expect to receive or it is sent by an unknown source. If you don't know what the file is attached to the email, do not open.
    - Block file types that are known as virus carriers: .exe, .com, .pif, .scr, .vbs, .chm, .bat. If you are uncertain about the file, research the file extension on your Anti-virus software website.
    - Block any files with more than one file type extension such a HappyDays.jpg.vbs
    - Download files from only reputable and well known websites.
    - Delete chain emails and junk email. These are considered spam and clog up inboxes and networks. Consider installing a spam filtering software to catch spam before it hits the inbox.
    - Check for the availability of anti-virus software for Smart Phones. If available, install the software.
    - Conduct employee training on email/Internet virus protection protocols. Add protocols/policies to your employee handbook and Acceptable Use Policy. See **Employee Policies**, page 32.

Current Situation

Review your current anti-virus protections. Given the key points above, does your company have enough protections in place to secure **ALL** your computers and data? Complete the below Situational Analysis to better understand your current situation and identify where improvements can be made with your anti-virus protection.

SITUATIONAL ANALYSIS – ANTI-VIRUS PROTECTIONS

Briefly describe your company's current anti-virus protection levels and employee practices:	
Problems/shortfalls of the current anti-virus software and areas that need improvement:	
Current person responsible for implementing/maintaining anti-virus software:	How often antivirus protections are checked. □ Monthly □ Quarterly □ Semi-annually □ Annually □ Occasionally □ Never
Resources dedicated to anti-virus protections: □ Anti-virus software □ Spam filtering software □ Other ________________________________	
Current time committed to installing anti-virus protection: ________ hours	Budget allocated to activity: $__________

Anti-virus Plan of Action

With your Security Squad team discuss your anti-virus coverage and protocols. Complete the Plan of Action chart below to develop the guidelines for setting up virus protections on **ALL** your computers. The chart will help you identify staff responsible and resources allotted protecting your computers and data with anti-virus software.

PLAN OF ACTION – ANTI-VIRUS

Anti-virus activities to be completed:	□ Install/update anti-virus software on computers/Smart phones □ Configure anti-virus software to receive automatic updates □ Configure computer to receive automatic updates □ Add spam filters to email software □ Review/revise employee policies to help eliminate virus risks
Person responsible for completing activities:	Date password security is to be completed:
Est. time to complete activities:	____________ hours.
Person responsible for reviewing and updating activities:	Review protocols: □ Month □ Quarterly □ Semi-annually □ Annually
Resources –Software/equipment needed for project completion. (Check only if budget allows purchase and scale of project justifies investment.) □ Purchase/Shareware anti-virus software □ Purchase/Shareware spam filtering software □ Other ______________________________	
Budgeted Resources: □ Staff time □ Equipment □ Outside Technician	 Initial work $____________ Maintenance $____________ $____________ $____________ **Total $____________**

Definitions

Below are types of malware, often generically referred to as "viruses".

- Virus – A malicious code that copies itself and infects your computer to corrupt or destroy data. A virus can spread from one computer to another through networks or shared devises.
- Trojan – A non-self replicating malware that appears to perform a usable function but instead creates unauthorized access to your computer system. Once the file is opened, the Trojan copies itself to your hard drive and allows hackers a remote access to your computer system.
- Worm – A computer malware that is self-replicating. It uses a computer network to send copies of itself to other computers on the network, usually without the user intervention. A worm does not need to attach itself to an existing program to do damage.
- Adware – Advertising software that can be added to other application software installed by the user. After installation, it automatically plays, displays, or downloads advertisements to a computer. It can also track Internet sites visited by the user.

- Spyware – Software that secretly monitors user's behavior. It can collect personal information and surfing habits and sends that information to an Internet marketing company without the user's approval or knowledge. Spyware can slow connection speeds, change home page or cause loss of Internet access or functionality.
- Crimeware – Malware specifically designed to identity theft and cyber crime. Crimeware captures a user's confidential information with the purpose of taking funds from financial accounts or completing unauthorized transactions.
- Keystroke logging or keylogging – Malware that targets the computer's operating system to allow the tracking of keys struck on a keyboard. Information is then relayed back to the computer hacker for accessing sensitive information and secured websites.

Additional Resources

"Minimizing the Effects of Malware on Your Computer." Federal Trade Commission. http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec16.shtm.

"Simple Steps to Defend Against Viruses, Spyware and Adware." Sophos. http://www.sophos.com/security/best-practice/viruses.html.

"Securing Your Data Against Today's Threats, and Tomorrow's Unknown Breakthrough." EMBARQ (prepared by Guideline, Inc.). http://docs.google.com/viewer?a=v&q=cache:hVbZmUz4T4gJ:embarq.centurylink.com/embarq/refDocs/user_guides/whitepapers/business/EMBARQ_DataSecurity_WhitePaper.pdf+computer+economic+13.3+billion+malware&hl=en&gl=us&pid=bl&srcid=ADGEESgH9vD2JL8rqsTDLRK9SetB36sJ1eJGgv8W11MQpmk8RCP3MtLiQf0zaHFblzw-vYZZnsVcmYRkNw3hpvBV5GKr775_rMt0UJU4PYYp14q8CJ-tAg2bLyOZpYiS5LNLxc428k40&sig=AHIEtbShvDYNC4NGdkpgD_YuRgll75LuPg. May, 2008.

Wireless

Limiting Your Exposure

What's the Security Risk?

Today we all expect to have Internet connectivity - whether it's while you wait at the doctor's office, or sitting at the coffee shop or local restaurant. It seems like a great customer service to provide wireless connections, but actually, without safeguards, it can pose problems for the business owner and the person who is using the wireless service.

With an unsecured connection, anyone can come within range of your wireless signal and go online. If you provide an unsecured or open wireless Internet connection, you don’t have control over what people are doing using your connection. Illegal activity can be traced back to your network, or someone may break into your system and gain access to confidential data.

On the flipside, logging onto an open wireless connection when you are away from the office exposes your business to data loss. An open connection could potentially link your laptop, PDA, mobile phone to others who are using the same connection and interested in accessing your confidential information. An open wireless connection also exposes data that is sent by email or over the Internet to be intercepted by another computer, unless steps are taken to encrypt the data. Computers, PDAs or mobile phones with Bluetooth® connections are also susceptible to outside connections from anyone else who has Bluetooth® capabilities.

> “An unsecured wireless network is an open invitation to hackers to walk right into your computer and steal your personal information, upload malware onto your computer, and otherwise terrorize you.”
>
> - Daily Wireless.com

Key Points to Consider

- Wireless Network security protocols
  - **Separate Public/Private networks.** If you are providing free wireless connections for your customers, you should consider a public network for your customers and a private network for your business. Work with your IT provider to either split your current network into two separate public and private segments or set up two wireless routers - one which is secure for your business and the other which is open for customers.
  - **Wireless settings.** When setting up your wireless connection, the best practice is to set the encryption at the highest or most secure level. Most routers have a WPA-2 (Wi-Fi protected access), which is the most current encryption available for wireless networks. This is your first layer of protection. To add more security you should implement another protocol where the router recognizes the MAC (media access control) address of any device attempting to connect. If the router doesn't recognize the MAC address, they cannot access the wireless connection. To discover how to find your MAC address, see **Additional Resources**, page 22.
  - **Wireless use agreements**. To help eliminate undesirable activity on your open wireless, consider setting up a web page where a person who uses the connection agrees not to do any

illegal activity including downloading pirated software, threatening a government official, etc. This helps protect you as the provider of the wireless connection. After agreeing to comply with your rules the user could receive a temporary password, which you would change periodically.

    - **Broadcasting wireless access.** Another option to consider when providing wireless is to decide if you want to broadcast the router name or not. If you really want to be secure, do not publicly broadcast the name of your router. However, this does make it less convenient for customers who want to log on.

- Other wireless devices
    - **Bluetooth® Settings.** Check your Bluetooth® settings on your computer, PDAs and mobile phones. Change it to alert you when a Bluetooth® device wants to connect. You then have the choice of connecting to the requesting device, or not.
    - **Encryption software.** Not all devices can encrypt files. If you carry sensitive files with you on your PDAs or mobile phones, you should consider encryption software for your device.
    - **Wireless printers.** Take extra caution in printing sensitive documents as wireless printers store information. You will want to make sure you turn the wireless printer off at the end of the day to delete stored information.

Current Situation

Review your current wireless security levels. Given the information above, does your network provide you with adequate protection? Complete the below Situational Analysis to better understand your current situation and identify where improvements can be made to secure your equipment, software and data.

SITUATIONAL ANALYSIS – WIRELESS NETWORK & WIRELESS EQUIPMENT SECURITY

Briefly describe your company's current wireless system, and/or equipment that uses wireless networks.	
Problems/shortfalls of the current wireless system/wireless equipments or areas that need improvement:	
Current person responsible for maintaining wireless security:	How often wireless protections are checked. □ Monthly □ Quarterly □ Semi-annually □ Annually □ Occasionally □ Never
Resources dedicated to wireless networks/wireless equipment: □ Wireless router/s □ Encryption software □ Other ____________________________________	
Current time committed to wireless maintenance: _________ hours	Budget allocated to wireless maintenance: $__________

Wireless Plan of Action

With your Security Squad team discuss your wireless security plan. Complete the Plan of Action chart below to develop the guidelines for setting up your wireless network. The chart will help you identify staff responsible resources allotted for better securing your wireless network and other wireless/Bluetooth® devices.

PLAN OF ACTION - WIRELESS

Wireless activities to be completed:	□ Updates/secure router/s □ Implement MAC address security □ Implement usage policy for guests □ Develop employee wireless policy □ Set Bluetooth® protocols
Person responsible for completing activities:	Date wireless security is to be completed:
Est. time to complete activities:	____________ hours
Person responsible for reviewing and updating activities:	Review protocols: □ Monthly □ Quarterly □ Semi-annually □ Annually
Resources –Software/equipment needed for project completion. (Check only if budget allows purchase and scale of project justifies investment.) □ Updated WPA2 routers □ Encryption software □ Website revised to include online usage agreement □ Other ______________________________	
Budgeted Resources: □ Staff time □ Equipment □ Outside Technician	Initial work $____________ Maintenance $____________ $____________ $____________ **Total $____________**

Additional Resources

"How Do I Find My Pocket PC's MAC Address?" Pocket PC Central. http://www.pocketpccentral.net/help/ppc_mac_address.html.

"How to Find your MAC Address." Suite101.com. http://computernetworking.suite101.com/article.cfm/how_to_find_your_mac_address.

"How to Secure a Wireless Internet Connection." E-How. http://www.ehow.com/how_2009138_secure-wireless-internet.html.

"Take your Wireless Back: How to Secure Your WLAN." Softpedia. http://news.softpedia.com/news/Take-Your-Wireless-Connection-Back-How-to-Secure-Your-WLAN-79671.shtml.

Firewalls

Stopping Hackers at the Door

What's the Security Risk?

Throughout the Security Squad series we look at different types of protection for your computer system. Your computers, especially if connected to the Internet, are subject to all sorts of security threats. With the right knowledge, hackers could connect to your computer and have complete access to all your files. They could log your keystrokes, gain backdoor access to your networks, and spy on your email. They can also infiltrate your system and install a virus or make your computer a "Zombie" that performs malicious tasks under remote direction.

Having anti-virus tools, strong passwords, and using good computer practices may not be enough to stop a hacker from accessing your company computers. Hackers have devised programs to randomly attack Internet Ports (IP addresses) to see if they can get into a computer. Once they've hacked your computer, they have a continued access until you physically break the phone line or Internet connection. Any of your computers that are continually on the Internet are especially susceptible to these outside attacks.
To help prevent hackers from accessing your system, install your next line of defense -- your firewall.

Compare your firewall to the defensive line of a football team. The guards on the front line need to hold their ground and not let the offensive line gain yardage. In the same way, you need a strong defense against those who are trying to score with your privacy information. A firewall is a program or hardware device that guards what's coming through the Internet into your computer. It checks for suspicious activity and blocks it out. For example, let's say a hacker was using software that continually asked your computer for its IP address. The firewall would block this activity and go on the offensive to stop any other unauthorized requests until you give it permission. That would be a quarterback sack.

Key Points to Consider

- Hardware/Software firewalls
  - A hardware firewall is a separate piece of network equipment and is installed between the Internet source and your computer or network. Most hardware firewalls use a web-based interface to configure its access rules.
  - A small business hardware firewall normally costs under $100 and may be combined with your cable or DSL router.
  - Software firewalls are programs installed on each computer that also control access.
  - Use both hardware and software firewalls to give your computers double protection.
- Installing firewalls
  - Newer Windows operating systems have firewalls pre-installed and are enabled by default. However, double check to make sure they are turned on.

    - Newer Apple® computers also have a pre-installed firewall called Leopard. The firewall can be accessed through the System Preferences menu. Again, make sure the default is turned on.
    - Commercial firewall software can also be purchased and installed. The complexity of the firewall will depend in the security needs of your business and data. Discuss your firewall needs with your technician.
    - Only use one firewall software at a time to avoid programming conflicts.
    - Make sure your firewall is enabled on every computer in your office. One computer left open can make your whole office susceptible.
    - If your service provider says they have a firewall on their system that will work for you, you should still set up a firewall on your own computers or network for added security.
    - Make sure your network is behind the firewall and is configured to allow file sharing between your office computers. Work with your technician to properly install a network firewall.

- Security levels
    - Firewalls control the access in and out of a company's network or computers. Firewalls can be set to deny specific IP addresses.
    - By default most computers are set to be at the "Allow all incoming connections" mode. Changing the default to "Set access for specific services and applications" mode allows you to manage the flow of information. Firewalls can recognize and deny specific domain names, or specific protocols such as Web servers or FTP servers. If you allow employees to access the Internet, the Firewall will open port 80. If you want to block FTP servers, then port 21 will be denied access.
    - Many Internet software such as RealPlayer® or iTunes® require changes in firewall permission settings. At installation, the software will often automatically change permissions. You have the choice to allow or deny these changes.
    - Home and small business operations will usually need only an application gateway firewall, or proxy firewall. Corporate networks will usually include "packet filters", "circuit-level firewalls" and "stateful inspection firewalls." They do require major upkeep. If you think you need a more sophisticated firewall, discuss it with your technician.

- Outside access permissions
    - If you have employees who need to access the system remotely, you will want to install software, such as a Virtual Private Network (VPN) software to allow users to tunnel through the firewall using permissions and passwords.
    - Remote access does slightly open your network to hackers. Check your software documentation to set your remote access permissions to the highest level.

Current Situation

Review your current firewall protections. Does your company have both hardware and software protections? Are your permissions set to the highest level? Complete the below Situational Analysis to better understand your current situation and identify where improvements can be made with your firewall protection.

SITUATIONAL ANALYSIS – FIREWALL PROTECTIONS

Briefly describe company's current firewall protection levels:		
Problems/shortfalls of the current wireless system/wireless equipments or areas that need improvement:		
Current person responsible for implementing/maintaining firewalls:	How often firewall protections are checked.	□ Monthly □ Quarterly □ Semi-annually □ Annually □ Occasionally □ Never
Resources dedicated to firewall protections: □ Hardware firewall □ Software firewall □ Remote accessing software □ Other ______________________________		
Current time committed to firewall maintenance: _________ hours	Budget allocated to activity:	$_________

Firewall Plan of Action

With your Security Team discuss your need for firewall protection? Are the default firewalls enough or do you need to purchase a more complex firewall software? Do you have hardware firewalls for your network or individual computers? Complete the Plan of Action chart below to develop the guidelines for setting up firewall protections on your computers. The chart will help you identify staff responsible for the project and resources allotted for the project.

Plan of Action - Firewalls

Firewall activities to be completed:	□ Activate/Install firewall software on computers □ Install hardware firewalls □ Configure firewall software for increased security □ Install remote accessing software
Person responsible for completing activities:	Date firewall protections are to be completed:
Est. time to complete activities:	___________ hours
Person responsible for reviewing and updating activities:	Review protocols: □ Monthly □ Quarterly □ Semi-annually □ Annually
Resources –Software/equipment needed for project completion. (Check only if budget allows purchase and scale of project justifies investment.) □ Purchase firewall hardware □ Purchase firewall software □ Purchase remote accessing software	
Budgeted Resources: □ Staff time □ Equipment □ Outside Technician	 Initial work $___________ Maintenance $___________ $___________ $___________ **Total $___________**

Additional Resources

"Cyber Security Tip ST04-004." United States Computer Emergency Readiness Team. http://www.us-cert.gov/cas/tips/ST04-004.html.

Horowitz, Michael. "Tech 101: Understanding Firewalls." Wi-Fi Planet. http://www.wi-fiplanet.com/columns/article.phpr/3832801.

Kumar, Arun. "Understanding Firewalls, Part 1 – What is a Firewall?
http://www.brighthub.com/computing/smb-security/articles/62022.aspx.

Kumar, Arun. "Understanding Firewalls, Part 2 – Am I Protected?
http://www.brighthub.com/computing/smb-security/articles/62023.aspx.

Kumar Arun. "Understanding Firewalls, Part 3 – Limitations of Firewalls.
http://www.brighthub.com/computing/smb-security/articles/62024.aspx.

Buying and Selling Safely Online

What's the Security Risk?

Thinking about buying your next product online? You're not alone. Forrester Research Inc. predicts online retail sales to rise from $155 billion in 2009 to $249 billion in 2014 --- a 10% company annual growth rate that is creating opportunities for large and small businesses alike.

Unfortunately, as web retail increases, so does the number of unscrupulous venders. How do you know when you are doing business with a trustworthy vendor? When you search a website, do you wonder about the integrity of the online store? Is it safe to give them your credit card information? On the flip side, are you confident that visitors who are viewing your website know it to be a trusted location? How confident are you that your online customers' information is securely transmitted?

Trust is a major determinant for online sales. If you trust a retailer you are more likely to purchase from that retailer time and time again. Same logic applies to your online business. If your customer does not have trust in your online website, you are losing sales. Fortunately, there are some simple safety protocols that will help you establish your customers' trust. It is then up to you to maintain that trust through good customer service and product delivery.

Key Points of Consider

Whether you are buying or selling online, there are key protocols and symbols to look for and follow.

Data Security Transmission

- All companies that collect and transmit customer data should secure their transmissions through a Secure Socket Layer (SSL) protocol. The SSL uses an encryption protocol that secures the data as it is transmitted between the web server and the browser. Every major browser has SSL support already included for the computer side.
- On the server side, your web server administrator needs to purchase and install a SSL certificate. If you use a commercial web host, they will probably have an SSL certificate as part of their web hosting services. You connect to the secure portion of the server when you want SSL enabled.
- A secured page is identified a couple of ways:
  - Locked padlock will appear in the browser status, **or**
  - Green safety bar will appear in the browser address bar, **and**
  - URL address will begin with https:// instead of the usual http://

- Website Authenticity
  - Secured websites that have been authenticated by a third party will display an icon from a digital authority such as VeriSign®, Thawte® or GeoTrust®. This ensures the website visitor that the web server they are accessing is correctly associated with the company.

    - To obtain an authenticity certificate, a company submits a request to a digital authority. The certificate authority works with the webhost to verify the security protocols and verifies the company and domain name. Once approved, the company can legally use the authority icon and public certificate on their website.
    - Costs to obtain a digital certificate range from hundreds to thousands of dollars. Add this cost to your online business plan or consider purchasing e-commerce services from an already authenticated service such as Paypal™.
- E-commerce should have's
    - Company telephone numbers and address should be easily found on the website for customer contact should there be problems after the sale.
    - A privacy policy should be included on the website that states how the company will and will not use customer information. Customers need to be assured their information will not be distributed without their consent.
- Credit Card Use
    - The Fair and Accurate Consumer Transaction Act of 2003 basically requires all businesses, regardless of size and industry, to properly protect and dispose of the personal information they collect about their customers and employees.
        - Companies must have an internal policy regarding proper record keeping and disposal, including employee training and specific data destruction carried out and documented at regular intervals.
        - Do not send email or written confirmation to your customer that includes their full credit card number or other private user information.
        - Limit employee exposure to credit card information.
        - Discuss compliance measures with your bank, credit card merchant account and Internet service provider.
- Cookie Use
    - Cookies are bits of data put onto a computer by an online store to track customer's purchases and user information. Cookies are used to "Mine" demographics, shopping behaviors, and browser habits. They are also the coding that fills in forms and helps personalize the website.
        - Advantage, cookies save time as they remember information and automatically plug the information into the purchasing forms.
        - Disadvantage, cookies also auto-fill sensitive information like credit card numbers, addresses, etc. If a computer is stolen or the password is obtained, the thief can potentially purchase something in your name.
    - As a user, you have the choice to automatically delete cookies and re-enter information every time, or keep the cookies active.
        - To delete cookies in Explorer, go to **Tools** and scroll down and click to open **Internet Options**. Click the **General tab**, and then, under **Browsing history**, click **Delete**. Select the **Cookies** check box, click **Delete**, and then click **OK**.

        - To delete cookies in Firefox, go to **Tools** and click **Options**. Select the **Privacy** panel. Set Firefox will to: **Use custom setting for history**. Additional options will appear in the box. **Deselect** box for **Accept cookies** from sites. This will stop future cookies from being saved. Next go back to **Tools**, select **Clear Recent History**. On the Time range to clear, select **Everything** and click on the **Clear Now** button.
    - If you plan to retain cookies, do not have your browser store your passwords for you. It is an added convenience but it also makes it easier for someone else to access.

Current Situation

Review your current online security protocols. Do you have online sales? Is there a secured transaction process installed on your web server or through your e-commerce provider? Do your customers know that your website is a trusted location? Complete the below Situational Analysis to better understand your current online protocols and identify where improvements can be made.

SITUATIONAL ANALYSIS – E-COMMERCE

<table>
<tr><td colspan="4">Briefly describe your company's current e-commerce practices and policies:</td></tr>
<tr><td colspan="4">Problems/shortfalls of the current wireless system/wireless equipments or areas that need improvement:</td></tr>
<tr><td colspan="2">Current person/s responsible for implementing/maintaining e-commerce website:</td><td>How often e-commerce protocols are . reviewed</td><td>□ Monthly
□ Quarterly
□ Semi-annually
□ Annually
□ Occasionally
□ Never</td></tr>
<tr><td colspan="4">Current resources dedicated to e-commerce protection:
□ Secured Socket Layer Protection
□ Authenticated Certificate
□ Secured merchant/e-commerce transaction service
□ Other ______________________________</td></tr>
<tr><td>Current time committed to securing online transactions:</td><td>__________ hours</td><td>Budget allocated to activity:</td><td>$__________</td></tr>
</table>

E-commerce Plan of Action

With your Security Team decide what e-commerce protocols best meet the safety needs of your customer. Consider purchasing e-commerce services to increase your transaction security. Complete the Plan of Action chart below to develop the guidelines for your e-commerce transactions. Make a schedule for when security is reviewed and who will be responsible for the process.

PLAN OF ACTION – E-COMMERCE

E-commerce activities to be completed:	□ Determine e-commerce security needs □ Purchase SSL/e-commerce services □ Authenticate website □ Implement plan
Person responsible for completing activities:	Date e-commerce plan to be completed:
Est. time to complete activities:	____________ hours
Person responsible for reviewing and updating activities:	Review protocols: □ Month □ Quarterly □ Semi-annually □ Annually
Resources –Software/equipment needed for project completion. (Check only if budget allows purchase and scale of project justifies investment.) □ Purchase e-commerce services □ Purchase authentication services □ Other ______________________________	
Budgeted Resources: □ Staff time □ Equipment □ Outside Technician	Initial work $____________ Maintenance $____________ $____________ $____________ **Total** **$____________**

Additional Resources

Raysman, Richard; Brown, Peter. “Data Breaches in Credit Card Transactions.” Law.com. http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202428984185.

Southern Rural Development Center (http://srdc.msstate.edu). A free bi-monthly e-commerce online newsletter.

University of Nebraska Extension (http://ebusiness.unl.edu). A 4-part curriculum on how to set-up an online storefront.

Employee Policies

Protecting the Company and Employees

What's the Security Risk?

Let's say you walk into your office and you see an employee downloading illegal copies of music onto your company computer. This is an illegal activity that could cost your company big bucks. It can also open your computer networks to multiple viruses and malware. In another instance, you discover that an employee has been copying your customer data and using the information for his own business. Or, imagine an employee simply opening an email link which activated a nasty virus. All of these employee initiated activities can cause harm to your computer data and subsequently to your company's bottom line. Other activities such as Facebook™, e-mail, online shopping, also diminish employee productivity. This too can be viewed as employee misuse of the computers, and your company time.

What can you do to protect your company and customers from illegal and damaging actions knowingly or unknowingly committed by employees? By developing an Acceptable Use Policy (AUP), you can effectively outline the acceptable use of computer equipment, software, and customer data. The policies will apply to whoever uses the company's equipment -- employees, contractors, consultants, temporaries and volunteers. Consequences for not following company policy should be clearly outlined in the AUP.

> "59%
> of ex-employees admitted to stealing confidential company information.
> - Ponemon Institute, 2008 Survey

Consider developing a confidentiality agreement as part of the employee handbook or AUP. Each employee will sign the agreement indicating they are fully aware of the need to keep all business related information, including customer data, confidential. Even small companies need a privacy policy. This helps to ensure your employees know privacy expectations, and it helps to assure customers that company information is kept confidential.

Acceptable Use Policies should complement existing company policies. Have your attorney review your Internet and email policies so they are consistent with your other employee policies and federal employee privacy laws.

Key Points to Consider

- Owner Responsibilities
  - **Business owner should have administrative rights to each computer**. Should you need to fire an employee, you can quickly gain access to their assigned computer through your administrative password and delete the employee password and their access to the computer.

    - **Evaluate what data each employee needs to perform their work.** If you have a network drive, partition the drive and assign access according to the needs of the employees. Take steps to eliminate access to sensitive information by nonessential employees.
    - **Encrypt sensitive company files.** Use the security feature built into most Windows and Mac operating systems to encrypt and password protect files. You can also purchase encrypting software to protect files.
    - **Complete the Equipment and Software Inventory Section of the Security Plan.** Detail who has access to which computers. Maintain a password list of employees with network drive access. Keep both lists in a secured location.
- Employee Computer Use
    - **Develop file portability rules.** What files are employees allowed to copy from the office computers onto portable drives to work from home? Remember, portable drives can be lost, stolen, or infected with a virus from a home computer.
    - **Develop computer use policies when working from home.** Discuss with your employees how they are to manage home security. Consider purchasing anti-virus software for employees working from home or require additional home security before employees are authorized to work from home. Have employees turn on Bluetooth® notifications to prevent unauthorized access of their laptops and Smart phones.
    - **Have employees secure their workspace while away from the desk.** Employees should log off their computers when they leave their desks for a period of time and secure sensitive data. Consider installing password secured screen savers or set computers to power down when not in use. Computers located in public visitation areas may also need a privacy screen filter.
    - **Implement an employee training on proper computer use and company data security.**
- Email/Internet Use
    - **Determine rules for employee email privacy.** Some companies monitor employee email. Although there is uncertainty in email privacy law, judicial interpretations state that employees need to be informed of the company policies in written form. According to Duke Law and Technology Review technology policy statements should include:
        - Declaration that the employer's e-mail system is the employer's property and should be used for the purpose of furthering employer business.
        - If personal e-mails are permitted, a definition of limitations of personal use of the system must be stated. Include a sentence that the "employee has no expectation to privacy regarding any e-mails sent, received, or stored at the workplace."
        - Rules that govern the use of the e-mail system.
        - Affirmation of the employer's ability and right to monitor, intercept, record and review all communications sent by employees over the company's e-mail system.
        - Employer's business reasons behind the monitoring and the circumstances under which such monitoring will take place.

    - **Determine how much Internet use is acceptable during business hours.** Policy statements may include:
        - The use of the Internet is a privilege and should only be used to assist them in their job performance.
        - All employees are to use the Internet for professional, lawful and ethical use.
        - Abuse of Internet use can result in dismissal or civil and/or criminal liability.
        - Activities not allowed by the company may include downloading large or illegal files, playing games, personal shopping, sending mass emails, accessing streaming audio/video files, stock trading, engaging in chat groups or otherwise unnecessary use of network bandwidth.
    - **Determine e-mail and Internet use violations.** It should be made clear that any illegal activity, hate-related or racially motivated email is not allowed. Consequences for these actions should be stipulated in your handbook. Again, contact an attorney for specific language.
- Handling Sensitive Data
    - **Develop procedures on how to handle sensitive documents**. Remind your employees not to leave sensitive documents or portable storage devices on their desks. Have a secured location where sensitive data/equipment is kept overnight. Software and customer files should also be locked away when not in use. A cross-cut shredder can be used to destroy unneeded copies of sensitive documents.
    - **Procedures are needed for handling credit card information or sensitive customer data.**
        - Will employees be subject to background checks if they do handle sensitive information?
        - What is the definition of sensitive information?
        - What information is permissible to give out to requesting suppliers, customers, or prospects?
        - Advise employees not to give out any customer or other business information without contacting you or another supervisor in the office.
- Smart phone Use
    - **Be smart about Smart phone use.** Develop policies on what information can and cannot be downloaded on to the phone. Talk with employees about how to minimize security risks on Smart phones such as making the phone password protected, turning the Bluetooth® signal off when not in use and installing encryption software onto the phone.

Current Situation

Review your employee handbook and the Acceptable Use Policies. Does it cover the issues above and address them adequately? Are there security issues specific to your company that needs a new or improved policy statement? Even if you are comfortable with your current policies, it is good to periodically review and revise as the company grows in its employee roster and structure.

Employee Policy Plan of Action

Working with the Security Team and including staff from human resources, if applicable, develop policies for employee computer and Internet use. Complete the Plan of Action chart below. Compare your policies to examples listed in the **Additional Resources** at the end of this section on page 36. Consult an employment law attorney to ensure policies and statements are compliant with federal or state regulations. Have employees sign a statement stating they understand the contents of the Acceptable Use Policies, agree to abide by the policies, and understand the consequences of not abiding by those policies. If recommended, have employees sign a confidentiality agreement.

PLAN OF ACTION – EMPLOYEE POLICIES

Policy activities to be completed:	□ Convene a team to review current policies □ Evaluate employee procedures for security breaches □ Write/revise new employee handbook and AUP □ Consult an employment law attorney □ Implement the new/revised employee policies
Person responsible for completing activities:	Date handbook & policy manual are to be completed:
Est. time to complete activities:	____________ hours
Person responsible for reviewing and updating activities:	Review protocols: □ Semi-annually □ Annually
Resources –Software/equipment needed for project completion. (Check only if budget allows purchase and scale of project justifies investment.) □ Purchase anti-virus software for employees working from home □ Purchase encryption software for computers/laptops/Smart phone □ Other ____	
Budgeted resources: □ Staff time □ Equipment □ Outside Technician □ Attorney	Initial work $____________ Maintenance $____________ $____________ $____________ $____________ **Total** **$____________**

Additional Resources

"Employee Acceptable Use Policy Internet and E-Mail." Union County Public Schools. http://techserv.ucps.k12.nc.us/Policies/AUP_employee.pdf. Format for an agreement form.

"Monitoring Employee E-mail: Efficient Workplaces vs. Employee Privacy." Duke Technology and Law Review. http://www.law.duke.edu/journals/dltr/articles/2001dltr0026.html.

Ries, David. “The Law’s on Your Side.” Biztech. 8/21/2008. http://www.biztechmagazine.com/article.asp?item_id=479

“SANS InfoSec Acceptable Use Policy”. SANS Institute. http://www.sans.org/security-resources/policies/Acceptable_Use_Policy.pdf Format is available for modification and use by organizations.

Shinder, Deb. “Creating and Enforcing Acceptable Use Policies.” TechRepublic . 4/24/2006. http://articles.techrepublic.com.com/5100-10878_11-6063307.html.

Other Maintenance and Security Practices

There are some quick computing maintenance practices that you and your staff should use to keep your systems running smoothly and longer. Physical maintenance of a computer is a good practice as most computer malfunctions are related to dirt and debris, not excluding the occasional mouse! Regularly cleaning your hard drive space can also leave less space for hackers to leave unattached coding.

These top 10 maintenance practices should be included in your employee training sessions.

Physical Maintenance

1. **Interior/Exterior Cleaning.** Physically clean the interior and exterior of computers to remove dust and debris from cooling fans, power supplies and hardware components. Use only battery operated vacuums specifically designed for safe computer use. Use only approved screen cleaners and soft cloth to clean LCD screens. More helpful suggestions for cleaning the interior/exterior of your computer, go to Computer Hope at http://www.computerhope.com/cleaning.htm.
2. **Provide good ventilation.** Never block the air vents of your computer. Check manufacturer specifications for air clearance. Generally allow a 2-inch clearance.
3. **Minimize static around computers.** When working on a computer, make sure the computer is unplugged and that you and the computer are grounded. Use caution when plugging in USB devices. If a static charge is generated, the peripherals may stop working.
4. **Avoid moving hardware while powered on.**
5. **Use power protection on each computer.** Power strips provide no protection. Surge protectors protect against voltage spikes. Uninterruptible Power Supply (UPS) protect against voltage spikes and power losses. Invest in a battery backup UPS that signals or shuts down the computer when power losses occur.

Operating System Maintenance

6. **Shut down computer properly.** A proper shutdown is when you shut down through the operating system. In Windows, go to Start, Shutdown or Turn off. If you do experience an improper shutdown, on the next boot your computer will conduct a "Check Disk" scan. Allow the computer to run through the Check Disk to make sure the hard drive is working properly.
7. **Clean up desktop of unused icons.** Having too many icons on the desktop can clutter up and slow down users. Delete unused shortcuts (the icons with the tiny arrow on the bottom right). The files to the shortcuts will remain stored in the directory. If you have files saved on the desktop, consider moving them to other directories or creating a desktop folder to group the files together.
8. **Defragment the hard drive.** As files are added and deleted, data on the hard drive becomes fragmented and slows down the processing. Periodically defragging the hard drive helps to keep the operating system running smoothly.
    a. Windows OS XP– Go to **Start**, **All Programs, Accessories, Systems Tools**, and **Disk Defragmentation**. First run a check disk to see if you do need to defrag the hard drive. If needed, start defragging. You will also want to shut off your automatic sleep mode to prevent your system from powering down during the defragging. Go to your **Control**

Panel, select **Power Options**, extend the sleep mode or tell it to never sleep. Remember to restore the power options after you have defragged your hard drive.

   b. MAC OS – If you run a MAC OS X system, it is not necessary to defrag your system, unless you have extremely large editing videos. MACs use a different system that uses read-ahead and write-behind caching that minor fragmentation has less effect on system performance.

9. **Use the Disk Cleanup Utility**. The Disk Cleanup tool can easily determine which files are no longer needed on your hard drive and will delete the identified files. Click **Start**, **Program Files**, **Accessories**, **System Tools**, **Disk Cleanup**. Files you will want to clean up are:

   a. Downloaded Program Files - These temporarily files stored in the Downloaded Program Files folder. They are not program files or zip files that you have downloaded from other locations.

   b. Temporary Internet Files – This is your Internet browser cache of Web pages that are stored on the hard drive for quicker viewing. None of your personal web settings are affected by selecting this category, nor does it delete any cookie files.

   c. Recycle Bin – This is the Recycle Bin for the selected hard drive or partition. If you have a partition drive, you will need to delete files from each partition.

10. **Scan for Disk Errors**. Scanning your computer for disk errors can solve some minor computer problems and improve the performance of your computer. Go to **Start**, **Computer**, **Properties**, **Tools**, **Error-Checking**. You will want to select **Automatically Fix File System Errors** and **Scan for and Attempt Recovery of Bad Sectors**. Run error-check.

Most of the maintenance practices are to be conducted daily or monthly. Defragging, Disk Cleanup and Error-checking should be scheduled every six months, or as needed. The frequency of cleaning the computer's interior will depend on the dust and debris around the computers work space.

Key Contacts

The following individuals are responsible for ensuring our company's technology security. Please contact them with questions, concerns and problems.

Technical Areas	Contact/s	Email/s	Telephone/s
Inventory	1. 2.	1. 2.	1. 2.
Equipment problems	1. 2.	1. 2.	1. 2.
Network problems	1. 2.	1. 2.	1. 2.
Website problems	1. 2.	1. 2.	1. 2.
E-commerce, billing/invoice	1. 2.	1. 2.	1. 2.
Credit Card Company Notifications: Experian™ EquiFax® TransUnion®	1. 2. 3.	1. 2. 3.	1. 2. 3.

Equipment Inventory List

(____)

Updated: __/__/20__

Description	Model	Date Purchased	Purchase Price	Serial Number	MAC Address	IP Address – Static or Registered	Location	Primary User/s	Warranty Date

Software Inventory List

(____)

Updated: __/__/20__

Description	Version	Date Purchased	Purchase Price	Operating Software & license, serial number or keycode	Download or CD's	Primary User/s	Location

Security Squad Video Series and Workbook