- Drivers license numbers.
- Employee schedules and vacation times.
- Medical and health data.
- Copyrights, patents, research data and publications.
- Confidential legal or financial data.
- Vendor and subcontractor agreements and schedules.

Facility and Physical Security

- Computer monitors that access sensitive information should not face any public spaces. A computer used to check in customers should have the monitor facing away from windows and waiting rooms.
- Teach your employees not to leave laptops, cellphones, or any device having sensitive data, unattended or unsecured. Lock the screen and require a password to get back in when an employee leaves the area. Consider cable locks for laptops, to prevent theft.
- If a laptop has sensitive data consider using LoJack or Lookout, Windows Bitlocker or FileVault 2 for Mac OS X, can also be used to prevent thieves from reading the contents of the laptop.
- Your employees are your best defense.
- Minimize printed sensitive information and shred any paper documents containing sensitive information when no longer needed.
- Develop and enforce a "Clean Desk Policy" that teaches employees about leaving sensitive information lying on a desk or out in the open.
- Keep sensitive paper files locked in a cabinet. Consider locking sensitive account information in a safe.
- Computer equipment should be destroyed properly. A hard drive no longer in use should be taken apart to break the disk inside. Drilling holes throughout the drive will also break the disk inside.

Data Breach Incident Response According to Verizon's 2014 Breach Report: *"Privilege Abuse" accounts for 88% of all "Insider Misuse."*

Data breaches can take many forms including:

- Lost, stolen, or temporarily misplaced equipment (e.g., laptops, mobile phones, portable thumb drives, etc.).
- Employee negligence (e.g., leaving a password list in a publicly accessible location, espionage, or technical staff misconfiguration, etc.).
- Policy and/or system failure (e.g., a policy that doesn't require multiple overlapping security measures. If backup security measures are absent, failure of a single protective system can leave data vulnerable).

Once you have discovered or suspect there was a breach, do the following steps:

1. Leave the infected machine running, but disconnect from networks.
2. Call your security consultant and/or law enforcement.
3. Consult your attorney.
4. Consult with law enforcement prior to complying with state laws above, to inform affected parties.
5. Once law enforcement completes their investigation, identify and document the cause, and implement your recovery procedures.
6. Revisit and revise incident response and security policies as needed. For more info download the full guide at http://mcsc.usm.maine.edu/sbcsguide.pdf

---

ALERTS FOR 2014:

- **Microsoft Support Lifecycles:**
  Expiration of support for Windows XP is not the only application effected. All Microsoft applications now have new Lifecycle Support dates for 2014, 2015, etc.

- **December 31, 2014–New PCI DSS 3.0 requirements take effect**
  Because of these new standards, EMV smartcards are being implemented by all credit card issuers and by all businesses who collect, store and processes credit card payments and non-EMV consumers and merchants will be facing new policies with penalties beginning in 2015.

- **October 1, 2015–AMEX, VISA and Mastercard NEW Counterfeit Liability Shift Policies:**
  Businesses and consumers not using the new EMV smartcards or terminals, will be held responsible in cases of breach and exposure of sensitive information.

**Some information here and in the guide was obtained from the nsa.gov website.
See the full SBCG guide for a link to MS Lifecycle Database to see when your software support expires and details on new PCI DSS 3.0 Requirements with effective dates.

Updated: August 2014

Small Business
Cyber Security Guide

This pamphlet summarizes the main contents from the full guide to get you started for explanations, other topics, and links to more resources, download the full guide at http://mcsc.usm.maine.edu/sbcsguide.pdf

Secure Your Small Business Quick Start

- Check NCSL Security Breach Notification Laws for your state.
- Devise, test and revise an Incident Response Plan for each vulnerability.
- Machines that transport sensitive information, like payroll, point of sale (POS) and public wifi, must each be isolated on their own networks, and separate from machines used for daily use.
- SSID broadcasting should be turned off where wireless routers connect to POS, payroll and business systems.
- Change your Domain Name Service (DNS) of your networked devices card(s) and your business router to avoid DNS attacks (See guide for more directions) spoof or fake sites.
- Change any default username and passwords for routers (wired or wireless), computers, printers, smartphones, and any other devices.
- Utilize strong passwords.
- Utilize antivirus software like Avast in combination with anti-malware software like Malwarebytes.
- If using Windows, check Microsoft's software support expiration dates on MS Lifecycle Support Database. See guide for details.
- If using Linux, Mac OSX or mobile devices: check Lifecycle Support dates and policies from the vendor sites.
- Don't install any software you did not go looking for.
- Remove or uninstall software you are no longer using.

- Utilize Google Chrome or Chromium for a browser. If you must use Internet Explorer or Firefox, keep in mind they are major targets so keep them up to date and configured properly and be sure to check lifecycle expiration dates.
- Utilize Thunderbird, Web-based email (like gmail), or a more technical client (like BAT) for email applications.
- If you must use Outlook, check Microsoft's software support expiration dates on MS Lifecycle Support Database. See guide for more details.
- Before clicking any link, check the actual address by hovering the cursor over a link (bottom left in Chrome and Internet Explorer 10 and 11), make sure it looks legitimate.
- When accessing financial or sensitive login pages, make sure you see "https:" in the address bar at the top of the page, with a padlock in front of it. Click padlock to check if it looks legitimate.
- If you need remote access to your business network, install a Virtual Private Network (VPN), using Hamachi open source VPN on all devices to encrypt the connection.
- If you get a pop-up similar to "you are infected, click here to clean, click here to ignore," DON'T CLICK ON ANYTHING. Press and hold "ALT-F4" on the keyboard to kill the browser window (if you click on ignore it or the x your machine may get infected).

Password Security Fundamentals

- Utilize different passwords for different accounts.
- Change your passwords often.
- Say NO to letting a website or browswer "remember" your password. Consider using a password manager such as LastPass instead.
- Don't store your passwords on your computer or on paper left near computers.
- If you must write a password down, lock it away! It's valuable after all.
- Don't give out your passwords to anyone. Anyone who is authorized to be on the system would have their own login credentials.

Building a Password

- Bigger is better, at least 16 characters long when possible, otherwise use the maximum size allowed.
- Include combinations of uppercase, lowercase, numbers, and special characters. (!@#$%...).
- Avoid single words and simple phrases! Passwords containing words from the dictionary are easier to crack. If you must do so, surround the word or phrase with letters, characters, and/or numbers, or the first three letters or every other letter of the site you are logged into. A random mess makes it harder for a criminal to figure out all of your passwords.
- Don't use personal tidbits just because they are easy to remember, such as birthdays, favorite color, and pet names.

Network Security Fundamentals

- Limit Admin access to internal network.
- Implement an alternate DNS provider.
- Implement WPA2 on wireless networks.
- Implement strong passwords on all network devices.
- Turn off UPNP on all network devices.
- Separate devices with sensitive data on dedicated subnetworks by using 3 routers in a "Y configuration.

Secure Browsing Fundamentals

- Avoid Microsoft Internet Explorer.
- Google Chrome is currently the best choice.
- Login as a Limited User.
- Use NoScript or NotScripts.
- Know what link you are clicking.
- IOS Browsing, be sure you using at least iOS Safari 6.1.6 (Safari iOS 7 has a "Fraud Warning" service built into it).

Email Security Fundamentals

- Migrate to Microsft Office 2011 or later (check Microsoft's software support expiration dates on MS Lifecycle Support Database).
- Avoid sending or accepting sensitive information via email unless encryption is used.
- Be aware of hoaxes and scams, and educate employees on how to recognize phishing and spam attempts.
- Look for an email provider with strong anti-spam filtering capabilities.
- Educate employees on how to identify spam and use email spam filters.
- Set up your company's server to reject executable files and remove header response information.
- Consider viewing email in plain text.
- Avoid using automatic email replies.
- Utilize seperate emails for work and home.

Securing Windows Host OS

- Check Microsoft software lifecycles.
- Migrate to a modern OS and 64 bit hardware platform.
- Set OS updates to "Automatic."
- Limit use of the Administrator account.
- Utilize a web browser with sandbox capabilities.
- Utilize PDF Reader with sandbox capabilities.
- Implement Full Disk Encryption (FDE).
- Turn off autorun or autoplay (USB, CD, etc).
- Don't use unknown USB drives.
- Disable services and uninstall programs not used.
- Enable Data Execution Prevention (DEP) for all programs.

Securing Apple Host OS and IOS

- Maintain an up-to-date OS.
- Apple iPad note: The iPad requires a physical connection (e.g., USB) to a host running iTunes in order to receive updates. A good practice is to connect the iPad to an iTunes host at least once a month or just prior to any travel where the iPad will be used.
- Keep third party applications software up-to-date.
- Limit use of Administrator account.
- Enable Data Protection on the iPad.
- Implement FileVault2 on Mac OS Laptops.
- Install "Find iPhone" software.

Securing Linux/Unix OS/Android

- Maintain an up-to-date OS.
- Disable bluetooth and wireless when not in use.
- Only download trusted applications.
- Install security software for you system and devices.
- Utilize data and email encryption.
- Utilize remote storage solution when necessary.

Securing Mobile Devices

- Utilize Virtual Private Networks (VPN) when possible.
- Restrict use of public wifi.
- Utilize Full Disk Encryption.
- Utilize security software such as Lookout.

Securing sensitive information Understand what is sensitive information

- Social security numbers (SSNs).
- Credit card or other financial account numbers.