1. Do you implement virus controls and filtering on all systems?

Background:

Anti-Virus — anti-virus software packages look for patterns in files or memory that indicate the possible presence of a known virus. Anti-virus packages know what to look for through the use of virus profiles or "signatures" provided by the vendor. Since new viruses are discovered every day it is important to have the latest virus profiles installed. Without this protection, viruses are free to infect your systems. Viruses may cause a variety of problems such as loss or damage to information residing on your network, network interruption and inability of customers to access your system. Liability may be incurred if weaknesses of your security measures allow the systems of third parties to be infected. It has also become commonplace that viruses carry a spyware payload. See further description below.

Spyware — refers to a category of software that, when installed on a computer, collects personal information about a user without their informed consent. Spyware may be unknowingly downloaded by users when packaged in a Trojan Horse or systems may be infected by viruses that include a spyware payload. There are significant privacy liability implications due to the information that is being harvested and sent to a third party without the user's consent.

Controls on shared drives and folders — a network share is a location on a network allowing multiple users on that network to have a centralized space on which to store files. Unprotected Windows networking shares can be exploited by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Unprotected shares can allow Distributed Denial of Service attacks to occur and are also leveraged to propagate viruses and worms both internally to a network and to other networks. There is great potential for the emergence of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

How to implement appropriate controls:

Anti-virus

- Install anti-virus software on all systems.
- Implement a process to keep anti-virus programs up to date, utilizing automatic update of virus signatures if possible.
- Filter e-mail attachments and downloads to reject files with the following extensions: .exe, .vbs, .bat, .pif, .scr.
- Disable unneeded services and ports including: FTP service, telnet.
- Train employees not to open e-mail attachments unless they are expected and from a known and trusted source.
- Execute anti-virus scans on all e-mail attachments, files and downloads before the file is opened.

The links below provide additional anti-virus resources:

- **US CERT Computer Virus Resource,** http://www.us-cert.gov/reading_room/virus.html
- **ISCA Lab,** http://www.icsalabs.com/icsa/product.php?tid=dfgdf$gdhkkjk-kkkk

Controls on shared drives & folders — if sharing of directories and files over your network is not essential, file sharing should be disabled. An alternative would be to create a dedicated directory for file sharing, and move or copy files to that directory for sharing. All network shares should be password protected and restricted to read-only access when possible.

Removal of spyware

- At minimum, run a monthly full scan with anti-virus software on all computers on your network. Anti-virus software may find and remove spyware during a scan that it does not detect during real time monitoring.
- Run a legitimate product specifically designed to remove spyware.

A list of popular products can be found at the following link:

- **ICSA Labs,** http://www.icsalabs.com/icsa/topic.php?tid=962c$b7edc94e-dd775595$1d7a-48391663

CNA

Vendor Neutral Threat Notification — It is important to utilize a vendor neutral source of vulnerability and threat information in addition to other information that may be received. This assures that timely, non-biased threat notification is available for the coordination of appropriate defenses.

Use one of the links below to subscribe to a source of vendor neutral threat information:

- **CERT National Cyber Alert System**, http://www.us-cert.gov/cas/signup.html
- **SANS Institute @RISK: The Consensus Security Alert**, http://www.sans.org/newsletters/risk/?portal=6ea651380cdb76a250c69e382baf5c61

References:

http://www.us-cert.gov/cas/tips/ST04-016.html
http://www.us-cert.gov/reading_room/home-network-security/#III-B-5
http://www.us-cert.gov/reading_room/virus.html

2. Do you check for security patches to your systems at least weekly and implement them within 30 days?

Background:

Security patch management — updates or patches are regularly provided by software vendors to fix problems within their products. Many of these patches fix vulnerabilities, which could be exploited by attackers.

How to implement appropriate controls:

Subscribe to patch notification services from vendors for software utilized, review and evaluate at least weekly, preferably daily. Where possible, enable automatic update capabilities. Test and install critical security patches and upgrades within 24 hours of availability and no later than 30 days for all patches.

Formal patch management procedures should include the following:

- An inventory of IT resources, hardware equipment, operating systems, and software applications used within your organization.
- Monitoring of security sources for vulnerability announcements, patch and non-patch remediations, and emerging threats that correspond to the software within your system inventory.
- Priority system for the order in which your organization addresses remediating vulnerabilities.
- Testing of patches and non-patch remediations on IT devices that use standardized configurations. Make sure the remediation will not disrupt operations or degrade security elsewhere on your network before implementing in your production environment.
- Automated deployment of patches to IT devices using enterprise patch management tools.
- Automatic update of applications whenever possible and appropriate.
- Verification of vulnerability remediation through network and host vulnerability scanning.

Further information on patch and vulnerability management procedures can be found in:
The National Institute of Standards and Technology's Creating a Patch and Vulnerability Management Program,
http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

3. Do you replace factory default settings to ensure your information security systems are securely configured?

Background:

Firewalls, routers, VPN appliances, wireless access points and other network hardware have pre-defined "factory default" configurations. Similarly, security related software has default settings which are predetermined by the vendor. There are often inherent vulnerabilities in these default configurations if not adjusted to an operation's specific security requirements. A common problem is that administrative passwords for these devices are not changed from the default. Administrative passwords allow device configuration changes that could be used to disable security. Factory default passwords are easy for attackers to guess and, in most cases, are readily obtainable from published lists for specific manufacturers and models.

How to implement appropriate controls:

Formal policies should be implemented regarding the configuration of all network security devices and systems.

- Default configurations should be avoided and specific procedures should be put in place for the management of strong administrative passwords for these devices and systems.
- The policies should be updated as new vulnerabilities arise or network configurations change.
- Default policy for firewall handling inbound traffic should be to block all packets and connections unless the traffic type and connections have been specifically permitted.

Further information on firewall configuration and policy can be found in:
The National Institute of Standards and Technology's Guidelines on Firewalls and Firewall Policy,
http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

4. Do you have a way to detect access or attempts to access sensitive information?

Background:

Logging, monitoring and auditing — are used to track system activity both by system and application processes and by user activity on those systems and applications. These controls are designed to prevent the loss of confidentiality, integrity, or availability of information, including data and software, wherever stored within the organization's information systems. Processes such as these, provide the individual accountability, event reconstruction capability and means of intrusion detection which are needed to protect Non-Public Personal Information from unauthorized access. Likewise the "chain of custody" documentation of access to information is necessary to provide accountability for information stored on all types of media.

How to implement appropriate controls:

In regards to Non-public Personal Information entrusted to your organization, implement processes and tools which track and record the identity of those who access or have custody of this information; and record the time at which the access or custody takes place. These procedures should include:

- Logging all attempted access to sensitive data.
- Logging successful authentication to applications or databases housing sensitive data, along with as much detail of subsequent activity as possible (files accessed, deleting records or fields, printing reports, etc.).
- Maintaining these logs in a tamper evident file and limiting access to these files for separation of duties.
- Reviewing logs daily for suspicious activity.

Resources:

An Introduction to Computer Security: The NIST Handbook Chapters 14 and 18, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Common Sense Guide to Prevention and Detection of Insider Threats, United States Computer Emergency Readiness Team, http://www.us-cert.gov/reading_room/

NPE PRIMER 090808

5. Do you know what sensitive or private information is in your custody along with whose info it is, where it is, and how to contact individuals if their information is breached?

Background:

All types of sensitive or private information entrusted to your organization warrant protection according to its level of sensitivity. Of particular concern is personally identifying information such as Social Security numbers, credit card and other financial information. To be able to minimize the risk associated with handling such data, it is important to clearly understand how sensitive information flows through your organization.

How to implement appropriate controls:

- Inventory information that you have by type and location – database servers, workstations, web servers, etc. The following questions are useful in tracking the information flow:
  - Who sends sensitive information to the organization? Customers? Other businesses? Credit card companies? Banks?
  - How is information received by your organization? Through your Web site? By email? Transmitted through point of sale devices?
- Develop a plan for how to respond to privacy breaches which includes how to contact individuals whose information has been breached.

Resources:

Protecting Personal Information: A Guide for Business, Federal Trade Commission, http://www.ftc.gov/infosecurity/

Information Compromise and the Risk of Identity Theft: Guidance for Your Business, Federal Trade Commission, http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm

6. Do you authenticate and encrypt all remote access to your network and require such access to be from systems at least as secure as your own?

Background:

Authentication — identification and authentication are fundamental to network access control. Identification is the means by which a user provides a claimed identity to the system. Authentication is the means of establishing the validity of this claim. Typically this information takes the form of user ID and password.

Encryption — encryption is the conversion of data into a form, which cannot be easily understood by unauthorized individuals. To provide secure transmission of data over a public network Internet encryption is necessary to assure the data is not understandable except by the authorized recipient.

Remote users systems often present the weakest link in otherwise secure networks. Not only is data vulnerable during transport over public networks through eavesdropping by unauthorized individuals, but the systems of others such as vendors or contractors, and employee home computers may be less secure than the organization, which they are accessing.

How to implement appropriate controls:

- All remote access should require user identification and authentication utilizing strong passwords.
- Encryption should be used to provide secure communication between the remote users and your networks. A Virtual Private Network (VPN) is the most common method to provide this protection. When properly implemented, e-mail and other traffic will be encrypted, minimizing the risk to privacy.
- As part of your security policy, allow access only from other networks that meet your organization's security requirements. Use of a VPN does not eliminate the need for normal precautions for offsite computers or networks.

Resources:

Security for Telecommuting and Broadband Communications, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf

An Introduction to Computer Security: The NIST Handbook, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

NPE PRIMER 090808

7. Do you have a company policy governing security and acceptable use of company property?

Background:

An information security policy is a written statement designed to protect an organization's information assets against accidental or malicious disclosure, modification, or destruction. Information security management enables information to be shared while ensuring protection of that information.

How to implement appropriate controls:

Implement and enforce an information security policy with objectives of preserving the confidentiality, integrity and availability of the organization's information assets. The policy should address network access by employees, contractors or any other person with access to the company's network. Key elements of such policy include:

- Acceptable Use Policy for Users
  - Intended and/or appropriate use
  - Password management
  - Guidelines for accessing unprotected programs or files
  - Disciplinary actions for unauthorized and/or unacceptable behaviors, such as:
    - Breaking into accounts
    - Cracking passwords
    - Disrupting service
    - electing weak passwords
- Policy statement for Privileged (Administrative) Users – Guidelines should be more robust for these users, covering additional areas, such as:
  - Authority and conditions for monitoring user activity (e.g., e-mail, network traffic, other actions)
  - Causing service disruptions
  - Using vulnerability testing tools
  - Accessing protected programs or files
  - Disciplinary actions for unauthorized and/or unacceptable behaviors, such as:
- Sharing/creating accounts
- Cracking passwords

Further information on creating an information security policy:
SANS Security Policy Project - sample policy templates,
http://www.sans.org/resources/policies/?portal=873ffb7dab1ed3ddc1c46037229e061e
http://www.sans.org/reading_room/
http://www.isalliance.org/

8. Do you re-assess security threats and upgrade your risk controls in response at least yearly?

Background:

A periodic comprehensive assessment of the management, operational and technical security controls in an information system is necessary to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of the assessment are used to reassess the risks and update the system security strategy and policies.

How to implement appropriate controls:

Test information security procedures and technical controls annually at a minimum. Utilize a reputable outside vendor or adequately trained staff member.

- Assess the vulnerability of your networks to commonly known or reasonably foreseeable attacks.
- Scan computers on your network to identify and profile the operating system and open network services.
- Utilize resources such as US-CERT, the SANS Institute, and the Federal Trade Commission, to monitor the constantly evolving threat environment and to stay abreast of emerging privacy issues.
- Update your security plan according to the results of testing, changes in operations or other circumstances that might impact information security.

Resources:

Protecting Personal Information: A Guide for Business, Federal Trade Commission, http://www.ftc.gov/infosecurity/

Security Check: Reducing Risks to your Computer Systems, Federal Trade Commission, http://www.ftc.gov/bcp/conline/pubs/buspubs/security.shtm

SANS Top-20 2007 Security Risks (Annual Update), SANS Institute, http://www.sans.org/top20/#prevent

US-CERT – United States Computer Security Readiness Team, http://www.us-cert.gov/

Information Security Handbook: A Guide for Managers, National Institute for Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

9. Do you limit access to data on a need-to-know basis?

Background:

Managing system user access privileges or Access Control is the means of controlling what information users can utilize, the programs they can run and the modifications they can make. Access Control may be built into the operating system, incorporated into applications, or may be implemented through add-on security packages. Access controls help protect:

- Operating systems and other system software from unauthorized modification or manipulation.
- The integrity and availability of information by restricting the number of users and processes with access.
- Confidential information from being disclosed to unauthorized individuals.

How to implement appropriate controls:

- Define access controls based on "need-to-know" or "least privilege", which refers to the granting users only the access required to perform their duties.
- Access Controls should be centrally administered, so that one office or individual is responsible for configuring access controls. Restricting the ability to make changes to very few individuals allows for strict control over information.
- Formal procedures should be put in place to revoke user access privileges as soon as possible after a change in these privileges, such as the when an individual leaves the organization. In the case of an "unfriendly" termination initiated by the organization, consideration should be given to revoking privileges at the same time as or even before the employee is notified of the dismissal.

Resources:

An Introduction to Computer Security: The NIST Handbook Chapters 10 and 17, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Common Sense Guide to Prevention and Detection of Insider Threats, United States Computer Emergency Readiness Team, http://www.us-cert.gov/reading_room/

NPE PRIMER 090808

10. Do you outsource your information security to a firm specializing in information security or have staff responsible for and training in information security?

Background:

Due to the potential severity of privacy injury, network damage and business interruption that can be caused by security breaches, information security cannot be learned by trial and error. Security is not static and must be reassessed frequently to identify when changes within the organization and new threats require an adjustment to managerial, operational or technical controls. A designated individual or individuals with security training and experience is necessary to tie all of the individual activities together into a working security protection mechanism for your organization.

How to implement appropriate controls:

Designate trained staff to coordinate the organization's information security effort or outsource to a qualified vendor. Consider individuals with information security certifications such as CISSP (Certified Information Systems Security Professional) or CISA (Certified Information System Auditor).

Resources:

**Database of information security professionals certified by (ISC)², ** https://www.isc2.org/cgi-bin/directory.cgi?displaycategory=503

Information Systems Audit and Control Association, http://www.isaca.org/

NPE PRIMER 090808

11. On your wireless networks, do you use security at least as strong as WPA authentication and encryption?

Background:

Exploitation of wireless network security weaknesses have been implicated in several high severity security breaches which have recently come to light. The primary difference between wireless networks and wired networks is also the root of the security concerns involved with use of these networks. The radio links used for network communications in a wireless network can be easily covertly intercepted. This makes eavesdropping on or manipulation of these communications by an attacker a much simpler task. To bring these networks to levels of security near that of traditional wired networks, encryption (which makes these intercepted signals unreadable to unauthorized parties) and strong authentication techniques are necessary.

Wired Equivalent Privacy or WEP was the first security specification introduced to address the inherent insecurity of Wireless Local Area Networks (WLANs). Shortly after the introduction of WEP, researchers began to publish papers indicating weaknesses in its encryption and message authentication mechanisms. Attack tools used to exploit these weaknesses are now widely available.

How to implement appropriate controls:

Develop a formal security policy regarding the use and deployment of wireless technology. This policy should address user security awareness, an approval process for adding, monitoring and configuring wireless network hardware, and procedures for registering all wireless Network Interface Cards which are used in devices connecting to the network.

Change WLAN access point Service Set Identifiers (SSIDs) and administrative passwords from factory defaults to unique values for your business. The SSID is a name assigned to a WLAN to allow wireless devices to distinguish one WLAN from another. Administrative passwords allow access point configuration changes which could be used to disable security.

Disable access point SSID broadcast features and enable MAC address filtering. When the broadcast feature is enabled the WLAN's SSID is visible in plain text to anyone with a wireless device. If this SSID has not been carefully chosen to be vague, it may provide information regarding the identity of the network which could be valuable to an attacker. MAC address filtering permits access only to wireless devices with MAC IDs specified by the network administrator.

Do not depend on WEP (Wired Equivalent Privacy) as a primary means of securing wireless networks. At minimum utilize Wi-Fi Protected Access (WPA). Stronger encryption algorithms are available through the use of WPA2 but wireless network hardware, which meets the requirements of IEEE 802.11i must be utilized. A Virtual Private Network (VPN) is also an option for securing wireless links. The VPN should be configured such that it must be used for all WLAN devices and that all wireless traffic is through a VPN device before entering the corporate network.

Resources:

Are Your Company's Wireless Networks Putting Your Sensitive Data at Risk?, CNA Insurance,
http://www.cna.com/vcm_content/CNA/internet/Static%20File%20for%20Download/Risk%20Control/Network%20Security/CNA%20-%20Wireless%20Technology.pdf

Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, National Institute of Standards and Technology,
http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

NPE PRIMER 090808

12. Do you control and track changes to your network to ensure that it remains secure?

Background:

Configuration Management — is a compilation of procedures for keeping track of changes and evaluating changes to hardware, software and network configurations to ensure that changes to the system do not unintentionally or unknowingly diminish security. Seemingly insignificant changes to information systems can have significant impact on the security of those systems. Systems are constantly being scanned and probed by potential intruders for the types of exploitable weaknesses that may be introduced by these changes. Locking down system configuration makes it much more difficult for unauthorized executable files or malicious code to be surreptitiously installed.

How to implement appropriate controls:

A Configuration Management process should be implemented which addresses the following key elements:

- **Configuration Management Policy and Procedures** — addresses purpose, scope, roles, responsibilities, and compliance; and formal, documented procedures to facilitate the implementation of the CM policy and associated CM controls.
- **Documentation of Baseline Configuration** — documented baseline configuration of the information system and an inventory of the system's constituent components.
- **Configuration Change Control** — documentation and control of changes to the information system. Appropriate organization officials should approve information system changes in accordance with organizational policies and procedures which should include separation of duties such that no individual can subvert this process.
- **Monitoring Configuration Changes** — security impact analyses to determine the effects of the changes.

Resources:

Information Security Handbook: A Guide for Managers, Chapter 14, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

13. Do you have a prominently disclosed privacy policy and do you honor it?

Background:

Privacy policies are needed for any organization handling Nonpublic Personal Information (NPI). Depending on your organization's operations and the type of information handled, specific regulatory guidelines may apply to the implementation and content of such a policy. Some examples include:

- The Gramm-Leach-Bliley Act (GLBA) — addresses consumer financial privacy
- Health Insurance Portability and Accountability Act (HIPAA) — addresses the privacy of personal health care information
- Children's Online Privacy Protection Act (COPPA) — applies to the on-line collection of information from persons under 13 years of age

In general, a privacy policy details what information you gather from the persons or entities that you do business with, how it is protected and the situations in which this information may be shared with a third party.

How to implement appropriate controls:

Implement, prominently disclose and honor a privacy policy following the general guidelines provided below. Note that the guidelines provided are derived from Federal Trade Commission information on compliance with GLBA. GLBA is one of the most widely applicable privacy regulations but may or may not apply to your organization's operations. Consult your attorney when drafting the specific language of your privacy policy.

- Design your policy with your customers in mind. Your privacy policy should be clear, direct and easy to understand.
- Say what you mean and mean what you say. The FTC has taken privacy actions against companies that overstated their security measures and experienced a security breach which contradicts the standard of care portrayed in the policy. Treat these statements the same as advertising claims you make.
- Call customer attention to any changes in policy. If you modify how you gather or use personal information you must call the customers attention to the change in policy.
- Create a culture of compliance. Train all employees on the organization's privacy policy and how to protect sensitive data.

Resources:

Privacy Policies: Say What You Mean and Mean What You Say, Federal Trade Commission,
http://www.ftc.gov/bcp/edu/pubs/articles/art09.shtm

GETTING NOTICED: Writing Effective Financial Privacy Notices, Federal Trade Commission,
http://www.ftc.gov/bcp/conline/pubs/buspubs/getnoticed.shtm

In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act,
http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.shtm

14. At least once a year, do you provide security awareness training for everyone who accesses your network?

Background:

Almost all major reports on the current state of the information security threat environment point to users, who are easily mislead as a leading, if not the leading, vulnerability. As technical network security controls have hardened, attackers have increased their efforts toward sophisticated and effective social engineering techniques. Increasingly well-known threats such as phishing have evolved into more complex attacks such as spear phishing and whaling. The payloads of viruses and Trojan horses which are introduced because of user interaction have also become more damaging.

How to implement appropriate controls:

Develop a security awareness training program with the following key elements:

- Train users on your organization's privacy and acceptable use policies annually. Require employees to sign an agreement that they understand and will abide by these policies.
- Provide annual security awareness training for all users. This training should provide information on how to recognize and report security threats. Periodic alerts and reminders should be provided to alert employees to new threats as they emerge and to maintain vigilance in following appropriate procedures to avoid known vulnerabilities.

Resources:

Protecting Personal Information: A Guide for Business, Federal Trade Commission, http://www.ftc.gov/infosecurity/

User training materials:

CNA Risk Control, Network Security Awareness,
http://www.cna.com/cnaeportal/eportal/site/cna/menuitem.b326c7a71ff625c3b892ba97556631a0/

Risk Control Services - Technology,
http://www.cna.com/cnaeportal/eportal/site/cna/menuitem.ae6cce2c310a4b1d4312a3a2a86631a0/?vgnextoid=5f15065fbefc9010VgnVCM1000008966130aRCRD

Federal Trade Commission, http://www.ftc.gov/bcp/conline/edcams/infosecurity/teach.html