Lawyers Data Breach and Network Security Endorsement Primer

We can show you more.®

PROFESSIONAL SERVICES

1. Does your firm have a virus protection program and firewall in place?

Background:

Anti-Virus – Antivirus software packages look for patterns in files or memory that indicate the possible presence of a known virus. Antivirus 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 most recent virus profiles installed. Without this protection, viruses may result in infections to your systems. They may cause a variety of problems on computer systems 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 in your security measures allow the systems of third parties to become infected. It has also become commonplace that viruses carry a spyware payload, as noted in greater detail below.

Spyware – Spyware refers to a category of software that, when installed on a computer, collects personal information about a user without the user's informed consent. Spyware may be unknowingly downloaded by users when packaged in a Trojan Horse. Systems also may be infected by viruses that include a spyware payload. Significant privacy liability implications arise 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. However, unprotected Windows networking shares can be exploited by intruders in an automated manner in order to place tools on large numbers of Windows-based computers attached to the Internet. Unprotected shares also can allow Distributed Denial of Service attacks to occur and are leveraged to propagate viruses and worms both internally to a network and to other networks. A significant potential exists for the emergence of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

How to implement appropriate controls:

Antivirus strategies to consider in formulating a proactive program include the following

- Install antivirus software on all systems.
- Implement a process to keep antivirus 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, and .scr.
- Disable unneeded services and ports including FTP service and telnet.
- Train employees not to open e-mail attachments unless they are expected and from a known and trusted source.
- Execute antivirus scans on all e-mail attachments, files and downloads before the file is opened.

The links below provide additional antivirus resources:

US CERT Computer Virus Resources, http://www.us-cert.gov/reading_room/virus.html

ISCA Labs, http://www.icsalabs.com/icsa/product.php?tid=dfgdf$gdhkkjk-kkkk

Controls on shared drives and folders – If sharing of directories and files over your network is not essential, file sharing should be disabled. An alternative to this approach would include creation of a dedicated directory for file sharing, with files moved or copied 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 a minimum, run a monthly full scan with anti-virus software on all computers on your network. Antivirus software may find and remove spyware during a scan which it does not detect during real time monitoring.
- Run an industry-recognized product specifically designed to remove spyware.

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

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

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 protocol helps to assures that timely, nonbiased 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:

https://www.us-cert.gov/ncas/tips/ST15-003

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. Does your firm implement security software updates within 30 days of release?

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:
In order to ensure that proper controls are implemented, the following measures are noted:

- Subscribe to patch notification services from vendors for software utilized. Such notification should be reviewed and evaluated 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 activities:

- Create an inventory of IT resources – hardware equipment, operating systems, and software applications used within your organization.
- Monitor security sources for vulnerability announcements, including remediation of patch and non-patch functionalities, as well as emerging threats that correspond to the software within your system inventory.
- Establish a priority system for the order in which your organization addresses remediation of vulnerabilities.
- Test patches and non-patch remediations on IT devices that use standardized configurations. Ensure the remediation will not disrupt operations or degrade security elsewhere on your network before implementing in your production environment.
- Install an automated deployment of patches to IT devices using enterprise patch management tools.
- **Activate an automatic update of applications, whenever possible and appropriate.**
- Verify 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,
Guide to Enterprise Patch Management Technologies
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

3. Does your firm replace factory default settings to ensure that your information security systems are configured in a secure manner?

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. For example, inherent vulnerabilities exist in these default configurations if not adjusted to the specific security requirements of your operation. A common problem involves administrative passwords for these devices that are not changed from the default. As a result, 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 of specific manufacturers and models.

How to implement appropriate controls:

Formal policies should be implemented regarding the configuration of all network security devices and systems, which should address the following concerns:

- Default configurations should be avoided and specific procedures should be implemented 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.
- A default policy for firewall handling of inbound traffic should include blocking of all packets and connections unless the traffic type and connections have been expressly authorized.

Further information on firewall configuration and policy can be found in:

Guidelines on Firewalls and Firewall Policy- Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

4. Does your firm control access to information that resides on data storage devices such as servers, desktops, PCs, laptops and smartphones?

Background:

Access Control – Access controls are used to track system activity both by system and application processes and by user activity. These controls are designed to prevent the loss of confidentiality, integrity, or availability of information, including data and software, wherever stored within an organization's information systems. Access control processes are intended to provide individual accountability, event reconstruction capability and means of intrusion detection which are needed to protect non-public personal information from unauthorized access. Similarly, 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:

Regarding 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, including 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, and
- 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

Insider Threat Research, United States Computer Emergency Readiness Team http://www.cert.org/insider_threat/

5. Does your firm enforce a password management policy?

Background:
Passwords are the primary method of authentication utilized by most organizations. Having a password policy and ensuring organizational compliance with the policy represent two important steps in protecting sensitive information.

How to implement appropriate controls:

- Ensure that your password policy permits a simple mechanism for compliance, while maximizing security by adopting the following measures:
  - o The minimum length of a password should be 8 characters, with no maximum if possible.
  - o Applications must allow all printable American Standard Code for Information Interchange (ASCII) characters, including spaces.
  - o Check new passwords against a dictionary of poor or known compromised passwords.
  - o Do not enforce composition rules (no requirement lower/upper/special character).
  - o Do not expire passwords without a reason. (i.e. no expiration after 60 days).
- In addition to account lockout, all passwords must be protected by a strong hashing algorithm.

Resources:
DRAFT NIST Special Publication 800-63B Digital Authentication Guideline – Authentication and Lifecycle Management, National Institute of Standards and Technology, https://pages.nist.gov/800-63-3/sp800-63b.html

6. Does your firm ensure that sufficient safeguards are established and implemented for the transmission and storage of data?

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 a 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 such as the internet encryption is necessary to ensure that 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 that of the organization which they are accessing.

How to implement appropriate controls:
Appropriate controls may be implemented by taking the following steps

- All remote access should require user identification and authentication utilizing strong passwords and 2 factor authentications.
- **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 used 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 fulfill your organization's security requirements. Use of a VPN does not eliminate the need for customary precautions for offsite computers or networks.
- All mobile devices (phones, laptops, flash and external hard drives) should utilize full disk encryption.

Resources:
Guide to Enterprise Telework and Remote Access Security – Recommendations of the National Institute of Standards and Technology (NIST), U.S. Chamber of Commerce http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf

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

7. Does your firm monitor user accounts to identify and eliminate inactive users?

Background:
While many organizations focus on provisioning access annually, equally important is de-provisioning that access once it is no longer needed. This issue can arise when an employee leaves the organization, but also may occur as employees change roles within the organization.

How to implement appropriate controls:
Organizations should have a process in place (automated is preferable) to quickly and completely remove access, when necessary, by considering incorporation of the following protocols:

- **Document which systems control access to sensitive data.**
- **Ensure the procedures are in place to allow access changes to be made quickly.**
- Conduct a quarterly access review with all employees to verify that their level of authorization matches their job function.

Further information on creating an Access Control policy: NISTIR 7874, Guidelines for Access Control System Evaluation Metrics
http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7874.pdf

8. Does your firm control access to information that can be displayed, printed and/or downloaded to external storage devices?

Background:
Understanding points of access and leakage for sensitive information within your environment is of the upmost importance. Such understanding requires a review of the entire lifecycle of information as it is received, processed, stored, printed, sent to third parties, and destroyed.

How to implement appropriate controls:
Perform a data life cycle analysis for all sensitive information in the company's care/custody/control. This analysis should include ingress/egress points, and an inventory of where it is stored through the following mechanisms:

- Ensure that data is encrypted at both rest and in transit.
- Implement controls on workstations (especially those in publicly accessible areas) to enable screen lockout after a period of inactivity. Also disable USB ports when not needed for business purposes.
- Consider enabling secure print, where shared printers are used. This protocol requires the print requestor to be physically present before the documents will print.
- Ensure that employees read and understand policies governing the control of data, so that they are aware of their responsibilities (for example to encrypt sensitive email attachments).
- Ensure that data is destroyed/removed from all devices before they are decommissioned, including nonstandard computing platforms such as network printers and mobile devices.

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://business.ftc.gov/documents/bus58-security-check-reducing-risks-your-computer-systems

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

Cyber Security Framework, National Institute for Standards and Technology, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.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 effect. 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, and
- confidential information from being disclosed to unauthorized individuals

How to implement appropriate controls:
Access to data on a need-to-know basis may be implemented, as follows:

- *Define access controls based on "need to know" or "least privilege"*, which refers to 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 established to revoke user access privileges as soon as possible after a change in these privileges, such as 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

Insider Threat Research, United States Computer Emergency Readiness Team http://www.cert.org/insider_threat/

10. Do you outsource your information security to a firm specializing in information security or have staff responsible for implementation 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 re-assessed frequently to identify when changes within the organization and new threats require an adjustment to managerial, operational or technical controls. Your firm must designate an individual or individuals with the necessary security training and experience to tie all of the various 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/ch-directory/default.aspx
Information Systems Audit and Control Association http://www.isaca.org/

11. On your wireless networks, do you use security at least as strong as Wi-Fi Protected Access (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 intercepted in a covert manner. Eavesdropping on, or manipulation of these communications by an attacker, is a much simpler task. To bring these networks to levels of security analogous to 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 (medium assess control) address filtering. When the broadcast feature is enabled, the WLAN's SSID is visible in plaintext 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:
Guide to Securing Legacy IEEE 802.11 Wireless Networks – Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

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

Background:
Configuration Management (CM) addresses the 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 being scanned continuously 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://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.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 upon 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
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) – addresses the privacy of personal health care information
- Children's Online Privacy Protection Rule (COPPA) – applies to the online collection of information from persons under 13 years of age

In general, a privacy policy delineates what information you compile from the persons or entities with whom you do business, 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 compile or use personal information, you must alert customers to the change in policy.
- Create a culture of compliance. Train all employees on the organizations privacy policy and how to protect sensitive data.

Resources:

Privacy Policies: Say What You Mean and Mean What You Say, Federal Trade Commission – BCP Business Center, http://www.amerinde.com/docs/20_Privacy%20Policies_%20Say%20What%20You%20Mean%20and%20Mean%20What%20You%20Say%20_%20BCP%20Business%20Center.pdf

Getting Noticed: Writing Effective Financial Privacy Notices, Federal Trade Commission, http://business.ftc.gov/documents/bus55-getting-noticed-writing-effective-financial-privacy-notices

In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, http://business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act

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 misled, as a major vulnerability. As technical network security controls have intensified, 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 acknowledging 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 know vulnerabilities.

Resources:

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

User training materials:

CNA Risk Control, Privacy and Network Security Resources, www.cna.com/riskcontrol

To learn more about CNA's Lawyer's Data Breach and Network Security Endorsement, contact (fill in state administrator contact information).

CNA

One or more of the CNA companies provide the products and/or services described. The information is intended to present a general overview for illustrative purposes only. It is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. "CNA" is a service mark registered by CNA Financial Corporation with the United States Patent and Trademark Office. Certain CNA Financial Corporation subsidiaries use the "CNA" service mark in connection with insurance underwriting and claims activities. PS3190C