CNA Cyber Self-Assessment Primer: Required Minimum Practices

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

   RMP: Implement virus controls and filtering on all systems. Minimum controls include:
   a. Installing antivirus software on all systems.
   b. Implementing a process to keep antivirus programs up to date, utilizing automatic update of virus signatures if possible.
   c. Filtering e-mail attachments and downloads to reject files with the following extensions: .exe, .vbs, .bat, .pif, .scr.
   d. Disabling unneeded services and ports including: file transfer protocol (FTP) services and telnets (network protocols).
   e. Training employees not to open e-mail attachments or click on Internet links provided within messages unless the message is expected and/or from a known and authenticated source.
   f. Executing antivirus scans on all e-mail attachments, files and downloads before the file is opened.
   g. Running a commercially available product specifically designed to function as antispyware software. At a minimum, run a monthly full scan of all devices attached to your network.
   h. Disabling any non-essential network file sharing capabilities. If file sharing is necessary, create a dedicated directory for file sharing, password protect these shared files, and restrict use to "read only" if possible.

2. **Does your firm implement security software updates in a timely manner?**

   RMP: Subscribe to vendor patch notification services for all software and systems 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 all other patches within 30 days.

3. **Does your firm replace all factory default settings to ensure your information security systems are configured securely?**

   RMP: Implement policies regarding the configuration of all network security devices and systems.
   a. Avoid default configurations, and implement specific procedures for the management of strong administrative passwords or passphrases for these devices and systems.
   b. Update policies as new vulnerabilities arise or network configurations change.
   c. The default policy for a firewall handling inbound traffic should be to block all packets and connections unless the traffic type and connections are specifically permitted.

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

   RMP: Regarding confidential or sensitive information accessible within your company:
   a. Define access controls based on "need to know" or "least privilege", which refers to granting only the access required by users to perform their duties.
   b. Centrally administer access to limit access to confidential or sensitive information.
   c. Establish separation of duties to prevent individuals from subverting access controls.
   d. Implement written procedures to change user access privileges immediately upon changes in a user's position or authority.
   e. Implement written procedures to terminate user access privileges when employment is terminated. If employment is being terminated for cause, revoke privileges concurrently with notifying the employee of termination.

5. **Does your firm have a password usage policy?**

   RMP: Maintain an easily understandable written policy on creating and using passwords or passphrases. Update the policy annually to reflect current best practice, such as those published by the National Institute of Standards and Technology.

6. **Does your firm ensure that sufficient safeguards are in place for the transmission and storage of data?**

   RMP: Authenticate and encrypt all remote access to your network, requiring user identification and strong passwords or passphrases. A Virtual Private Network (VPN) is the most common method to provide this protection. As part of your security policy, require all remote connections to occur via VPN and require two-factor authentication to confirm a user's identity.

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

   RMP: Maintain a written policy on required timeframes to eliminate inactive user accounts, and utilize software that automatically identifies and disables such accounts in accordance with the policy.

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

   RMP: Maintain a written policy regarding storage of company data on portable devices, and utilize technical methods to prevent data leakage such as disabling or monitoring usage of USB ports, content filtering, and use of network monitoring software. All downloadable data should be encrypted.

Additional practices for CPA NetProtect PRIME customers:

1. **Does your company have a documented information technology business continuity and disaster recovery program for your business? If yes, is it tested periodically?**

   RMP: Incorporate into your current business continuity plan actions to take and regularly test them (such as annually). Consider your company's unique needs; take inventory of your operational needs for one week, and then one month. Include day-to-day operations, human resources, operating manuals, supporting software and hardware, plus backup facilities in this process.

Over, please.

2. Do you perform regular backups of data, applications and system configurations?

RMP: Maintain at least two backups both physically and logically separated from the original. Keep one of the backups offline and in a separate physical location. This protocol helps to prevent against the same loss that caused the loss of the original, helps ensure that the backup is not corrupted or encrypted by malware, and helps restore data timely. Test backups on a regular (at least annual) basis to ensure restorability.

Glossary

Access Control – The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.

Antispyware Software – A program that specializes in detecting both malware and non-malware forms of spyware.

Antivirus Software – A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Backup – A copy of files and programs made to facilitate recovery, if necessary.

Business Continuity Plan – The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business functions will be sustained during and after a significant disruption.

Ciphertext – Data in its encrypted form.

Configuration – The makeup of a system. To "configure software" means selecting programmable options that make the program function to the user's desire. To "configure hardware" means assembling desired components for a custom system as well as selecting options in the user-programmable parts of the system.

Content Filtering – The process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users.

Data Leakage – The unauthorized transfer of classified information from a computer or datacenter to the outside world. Data leakage can be accomplished by simply mentally remembering what was seen, by physical removal of tapes, disks and reports or by subtle means such as data hiding.

Disaster Recovery Plan – A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

Encryption – The process of changing plaintext into ciphertext for the purpose of security or privacy; conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

Firewall – A gateway that limits access between networks in accordance with local security policy.

Malware – A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim; a virus, Trojan horse, or other code-based malicious entity that successfully infects a host.

Packet – A block of data transmitted over a packet-switched network, which is the common architecture of all local area networks (LANs) and most wide area networks (WANs) such as the Internet.

Patch – An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Plaintext – Unencrypted information.

Spyware – Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Two-factor Authentication – The use of two independent mechanisms to verify the identity of a user, such as a password and smart card or a password and fingerprint scan.

Virtual Private Network (VPN) – A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks.

Virus – A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk.

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Glossary Sources:

- Glossary of Key Information Security Terms, published by the National Institute of Standards and Technology, March 2013 available at http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
- PC Magazine encyclopedia available at http://www.pcmag.com/encyclopedia

Additional Resources:

- Small Business Information Security: The Fundamentals, published by the National Institute of Standards and Technology (NIST), November 2016 available at http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
- AICPA Cyber Security Resource Center