Information Security Checklist

Due Diligence

CPA firms are responsible for due diligence when selecting and monitoring third parties and their information security services. This includes outsourcing to all third parties, such as tax return processors and cloud computing services. Agreements with third-party service providers should contain language indicating that:

- the third-party provider will treat any client data it receives as confidential and will not make any unauthorized disclosures or use of the information; and
- the provider will be financially responsible for any unauthorized disclosures or use that it commits.

Assessing and Evaluating Risks

- **Security/risk audits**; identifying and prioritizing security risks due to theft, loss, unauthorized access, viruses, or improper disposal.

- **To contract with outside vendors or not?** Generally, the larger the firm, the larger the network, and the more points of entry for hackers (and more information that is valuable to hackers). Upper-level security requires a staff of specialists and sometimes an independent third party. For instance, Service Level Agreements (SLAs) for functions such as firewall effectiveness or IT uptime provide a form of insurance, although performance, service and loss prevention are more important than reimbursements.

  Examples of mitigating resource tools (not an endorsement):
  - Audit My PC (auditmypc.com)
  - Microsoft Security Assessment Tool (MSAT) for security breaches caused by the Internet
  - Microsoft Baseline Security Analyzer (MBSA) for workstations
  - Center for Internet Security (cisecurity.org) has online benchmarks and scoring tools for assessing security. (See "Technology Resources" at the end of this checklist.)

Implementing Security Measures

- **Provide physical security** as with any other asset, including building security and access codes, visual awareness, locking up servers in a separate room, and locking laptops to a desk or equivalent item.
  - Establish written policies governing the custody and care of portable laptop and other computers.
  - Ensure that all personnel are aware of the policies.

- **Strictly define user permissions and restrictions** so that users don't have any more rights or access to a program or system than they need, also known as the "least privilege" concept. Don't allow users to install or uninstall software. Excessive user rights and unauthorized devices can allow malware to do extra harm and lead to large losses of data.

- **Apply security updates —** Apply all software security updates to your computer. Once a software vulnerability is identified, most software companies issue software updates. For example, enabling Microsoft Windows Update will ensure that your operating system and Office software are secure from most common threats. Most software companies employ automatic updates, but if the software you are using

does not have an automatic updates feature, you should develop a business practice to check for latest updates.

- **Use antivirus software —** Antivirus software is a must. There are countless ways a computer can get a virus, and the range of harm can vary from slowing down the computer to stealing data from it. Antivirus companies constantly update virus definitions to defend computers against new threats, and for the most part these software updates are seamless to the user. Most antivirus software includes spyware, adware and e-mail attachment protection. If not, they should be deployed along with antivirus software.

- **Ensure that your computers and networks, especially wireless networks, are protected by a firewall**. Secure your network and your computer so they are not visible to everyone on the Internet. Firewalls block outside access to the computer and are available in both hardware and software forms. Many standard and wireless routers come with a built-in firewall. They should be configured to block all non-Internet and e-mail traffic in and out of your network. Some software may require special configuration.

  Firewall software should also be regularly updated. If that task is too daunting, you can simply buy a new router, which in some cases may be cheaper than hiring someone to update the software. If you are using a wireless router, disable SSID (Service Set Identifier) broadcasting and use strong passwords to secure access. For best protection, you should limit devices that can access your wireless network, using MAC (Media Access Control) addresses of the devices. There is also software for intrusion detection and prevention but the cost and complexity can be prohibitive for small businesses.

- **Use strong passwords.** It is convenient not to have to enter a username and password every time you start using the computer; however, not entering them makes it equally convenient to steal data off your computer without your knowledge. Usernames and passwords are the basic building blocks of security. Use a complex (or strong) password that cannot be guessed within the account lockout attempts. Passwords should be changed frequently. In addition, always use a password-protected screen-saver to prevent unauthorized access in your absence.

  - Don’t use passwords based on personal information that can be easily accessed or guessed; make them counter-intuitive.
  - Don’t use a complete password that can be found in any dictionary of any language.
  - Use both lowercase and capital letters.
  - Make passwords at least six characters long; use both lowercase and capital letters and a combination of letters, numbers and special characters such as <, } and ~.
  - Misspell or “salt” words with special characters (e.g., “D@Wg&PoN1$#0”).
  - Use different passwords on different systems.
  - Use automated systems that change passwords at least every 90 days.
  - Don’t leave a password someplace for people to find, such as in your desk.
  - Use screensaver passwords that lock out the screen after 15 to 30 minutes.

- **Create backup copies of all important data and information on a regular basis.** The frequency of backup depends on: how often your data changes; and the impact on your business if you lose the data between the last backup and the time of loss. Store and secure backup copies away from your office location and use encryption to protect any sensitive information about your firm and clients. Regular backups better ensure that critical data is not lost in the event of a cyber-attack or physical incident such as a fire or flood.

- **Encrypt your client data** to protect it from hackers and thieves. The following are three basic areas to be considered:

- **Hard-Drive Encryption —** Secures data in case you lose a computer or someone steals it. Hard-drive encryption locks down the computer after several unsuccessful login attempts. The most common technique for stealing data is to plug the hard drive into another computer (i.e., drive swapping), and almost all hard-drive encryption software prevents this kind of theft. Another reason to encrypt your hard drive is to prevent thieves from stealing your business data with hard-drive recovery software, which can happen when you recycle your computer.

- **Data Encryption —** If you use software that stores data in a detached database or other structured data formats, consider encrypting sensitive data like Social Security numbers, tax ID numbers, driver's license numbers, etc., on individual data element level. Most software programs are designed to be portable and scalable, but the downside of portability is that someone can walk away with the database or the backup of the database and read all of the sensitive information. When purchasing or designing software, ask vendors if the sensitive data can be encrypted in the individual data element level.

- **File Encryption —** E-mail has become the number one collaboration tool used to exchange files with sensitive data in them. Plain text e-mail and attachments can be read by people sniffing e-mail on the Internet cloud or by someone who can reach your computer. The common practice of leaving your computer unlocked and using the "remember my password" check-box means anyone who can get to your computer can read all of your e-mail, some of which may contain sensitive data about your business or clients. A good example of a low-cost and robust solution to that problem is Adobe PDF, which encrypts files with a password or phrase. In the standard version of Adobe Acrobat, you can lock your document with a password, and Adobe will use that password or phrase to encrypt the document. For added security, the password should be communicated over the phone.

- **Remote Mobile Device Security** enables a user to prevent access to protected files in the event a computer has been lost or stolen. Protected files are encrypted, and the application periodically authenticates the identity of the user. Some programs will track laptops when they are connected to the Internet.

  Safeguards that protect without user involvement appear to be most effective in reducing vulnerabilities. Encryption policies and other protective actions can be managed by the firm or by a third-party MSP (managed service provider). Both approaches should protect the organization independently of the end-user, and should work whether the computer is online or offline. Some services are available by online subscription, without the need to purchase or support hardware or software infrastructure. For example, Beachhead Solutions (www.beachheadsolutions.com) offers multiple options online. CAMICO offers its policyholders a 10 percent discount on services from Beachhead Solutions.

- **E-mail Digital Certificates —** File encryption protects attachments, but it does not help if you are exchanging sensitive data in the e-mail message body. One solution is to sign your e-mail with a digital certificate that encrypts the entire e-mail message so that only the intended recipient can read it. It also ensures the e-mail message has not been altered or manipulated. An e-mail digital certificate requires some preparation to set-up, and you have to maintain the subscription of your certificate. Digital certificates can be purchased from security identity management companies like Verisign, Thawte and GoDaddy, on annual, three- or five-year renewal terms.

- **E-mail Spam Filter** — E-mail scams not only hamper office productivity but are also a big security threat. Often the scam appears to be from someone you know or some legitimate organization, but it has a virus or spyware attached to it, or it directs you to a website that can infect your computer. Hackers are constantly developing new techniques to fool end-users and spam filters, so be sure to use e-mail spam filtering services from a reputable company that is constantly investing in improving their spam filter engines.

- **Internet Usage** — There are some simple best practices when using the Internet on your work computer. Never download free movies, music and software unless the vendor and product are reputable (e.g., Adobe Acrobat). Most of these sites are not well maintained and are a breeding ground for computer viruses and spyware. Limit your Internet usage to legitimate websites only. Many illegitimate websites, foreign and domestic, exploit software weaknesses to install spyware on your computer. Don't let anyone play online games on your work computer, as many viruses are downloaded unknowingly that way.

- **Erase or destroy all data on hard drives when recycling them.** The Environmental Protection Agency has been known to fine enterprises $200,000 for not having documented proper computer disposal. An audit trail of serial-numbered inventory of equipment, and certification that personal data has been destroyed, will go a long way toward helping the firm meet the burden of proof in the event of investigation or litigation. This function can be outsourced to an external service provider. More information can be found on major vendor sites such as dell.com, hp.com, or ibm.com.

- **Be prepared for emergencies.** Create a contingency plan for continuing business operations (at an alternate location if necessary) and for recovering from an emergency. Test or review the plan annually. For more information on how to prepare for an emergency, go to www.ready.gov or www.us-cert.gov or www.cert.org

Personnel

- **Conduct regular computer security awareness training** for all computer users, including executives, IT staff and others with privileged access. Training sessions should enhance awareness of all risks, including social engineering and web application attacks. Tools alone cannot fully protect a firm from all computer and data security threats. Users need to also educate themselves on best practices. Many training organizations offer training classes, and there are many resources on the Internet to help educate users security-related topics.

- **Test training results.** One way to test awareness is by "inoculation," in which all users are sent phishing e-mail that is benign. Those who err are then educated or lose their user rights.

- **Who is responsible for safeguarding information** at your firm? Someone with the firm should take ownership of this responsibility.

- **Ensure that security requirements are addressed by the firm's policies and procedures.** Develop specific policies governing the custody and care of mobile devices and other computers. Ensure that all personnel are aware of the policies.

- **Institute internal controls** and background checks for key personnel.

- **Constantly monitor systems** for overall performance. Service Level Agreements (SLAs) may help in this effort.

- **What are the firm's procedures following a loss or compromise of client information?**
  - In the event of lost or compromised client information, have a person or committee in place for conducting a debriefing of all employees with knowledge of the compromised information.
  - The client may need to be notified of the time and scope of the compromise immediately following its detection, depending on the obligations imposed by the laws of the state where the company is located.

Results

- Preventing loss of business and other costs due to a data breach.
- Preserving confidentiality and integrity of information in its accuracy and completeness.
- Making information available and accessible to authorized parties.
- Creating new selling points to clients and prospective clients.

The references to vendors in this checklist are provided as examples only for reader convenience and are not endorsements of the vendors.

See the following "Technology Resources" for sources of information.

Jagdeep Randhawa, CAMICO vice president of information technology, contributed to the updating of this checklist.

Technology Resources

AICPA Information Management and Technology Assurance (IMTA) division (aicpa.org)

Resources, tools, information, including security. Certified Information Technology Professional (CITP) credential offered. Generally Accepted Privacy Principles (GAPP), FAQ on GAPP, Webtrust and Systrust engagements, SOC Reports 1, 2 and 3.

Center for Internet Security (cisecurity.org)

501c3 nonprofit, offers security benchmarks, standards and metrics; MS-ISAC, Integrated Intelligence Center

CERT® Division Coordination Center (cert.org)

Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Penn. (See U.S. Computer Emergency Readiness Team under following "Governmental Agencies".) Cybersecurity research and solutions, responses

CISOHandbook.com

Resources for Chief Information Security Officers, Chief Security Officers, security professionals, executives, managers, and practitioners who develop or manage enterprise security programs.

Global Information Assurance Certification (giac.org)

Information security certifications. Several designations offered, for example:

- GIAC Information Security Fundamentals (GISF)
- GIAC Security Essentials Certification (GSEC)
- GIAC Certified Mobile Device Security Analyst (GMOB)

ISACA (previously known as Information Systems Audit & Control Association) (isaca.org)

Information technology governance, security and audit; affiliated with the **IT Governance Institute (itgi.org)**; publishes Control Objectives for Information and Related Technology (COBIT)
Designations offered:

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in the Governance of Enterprise IT (CGEIT)
- Certified in Risk and Information Systems Control (CRISC)

Information Technology Alliance (italliance.com)

Association of professionals who work in mid-market IT solutions, best practices.

Institute of Internal Auditors (theiia.org)

Internal auditing, risk management, governance; publishes the Global Audit Information Network (GAIN) Annual Benchmarking Study (ABS).

National Cyber Security Alliance (StaySafeOnline.org)

Non-technical cybersecurity and safety resources.

SANS (SysAdmin, Audit, Network, Security) Institute (sans.org)

Information security resources, training, certification and research; publishes free resources.

Information Sharing and Analysis Centers (ISACs)

Financial Services ISAC (fsisac.com)

Several federal government agencies and the financial services sector form this center to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats.

InfraGard (infragard.net)

A partnership between the FBI and the private sector to share information and intelligence to prevent hostile acts against the U.S.

Internet Security Alliance (isalliance.org)

A multi-sector trade association and think-tank in collaboration between industry and Carnegie Mellon University. Cybersecurity standards, best practices, and technologies.

Multi-State ISAC (msisac.org)

Not-for-profit membership resource for state, local, territorial and tribal (SLTT) governments. Incident response resources, advisories and alerts.

Governmental Agencies

National Institute of Standards and Technology (nist.gov)

Includes Computer Security Resource Center, providing tools, practices, standards, guidelines, resources and publications, including Cybersecurity Framework 1.0 (Feb. 12, 2014).

U.S. Computer Emergency Readiness Team (us-cert.gov)

A part of the Department of Homeland Security's National Cybersecurity and Communications Integration Center. Coordination of cyber information sharing.

U.S. Dept. of Homeland Security/Federal Emergency Preparedness Agency (ready.gov)

Disaster preparedness and business continuation planning

U.S. Secret Service, Electronic Crimes Task Forces (secretservice.gov/ectf.shtml)

Brings together federal, state and local law enforcement, prosecutors, private industry and academia for the prevention, detection, mitigation and investigation of electronic crimes