February 06, 2015

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Library
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Dear Computer Security Division:

The American Institute of Certified Public Accountants (AICPA) is pleased to comment on the National Institutes of Standards and Technology's (NIST's) *Small Business Information Security: The Fundamentals* (**NISTIR 7621 Rev.1)**, a reference guideline developed by the NIST in partnership with the Small Business Administration (SBA) and the Federal Bureau of Investigation (FBI) as information security awareness outreach to the small business community. With a 128 year heritage of serving the public interest, the AICPA is the world's largest association representing the accounting profession, with more than 400,000 members in 128 countries. AICPA members represent many areas of practice, including business and industry, public practice, government, education, and consulting. The AICPA sets ethical standards for the profession and U.S. auditing standards for audits of private companies, nonprofit organizations, and federal, state, and local governments. The AICPA also develops and grades the Uniform CPA Examination.

Since the introduction and integration of computers into the business environment, the AICPA has provided technology-related risk management thought leadership guidance to businesses of all sizes. As trusted advisors to businesses ranging from Fortune 10 corporations to Main Street businesses, our members are well-versed on the unique business viability and security challenges faced by small businesses. Our members have assessed and designed controls to help business cost-effectively mitigate the business and societal impacts of these threats, both from a financial and technical perspective.

Through its development and promulgation of accounting guidance, the AICPA has developed various frameworks and standards that small business' stakeholders rely on in performing various governance activities that help ensure the confidentiality, processing integrity and availability of critical business data. For example, practitioners use the AICPA's Trust Services Principles and Criteria (TSP&C) when providing attestation or consulting services to evaluate controls relevant to the security, availability, and processing integrity of a system, and the confidentiality and privacy of the information processed by the system. The AICPA also provides information security related guidance that facilitates public company compliance with various laws and regulations such as The Sarbanes-Oxley Act of 2002 (SOX), as well as required disclosures related to Security and Exchange Commission (SEC) filings.

Finally, a significant contribution to the success of small business is through our active involvement with owners, bankers and other stakeholders supporting small business. The CPA, as the small business premier trusted business advisor, provides insight and support into how shareholder concerns related to information security are addressed through various corporate governance initiatives.

We recognize and appreciate the considerable work that the NIST, SBA, and the FBI have undertaken in establishing this reference guideline for small businesses, and strongly commend such efforts to promote information security awareness within the small business community.

Our comments follow

- Generally, this is an excellent document to facilitate small business control over security. In many businesses, the effectiveness of the tactical strategies implemented as identified in the exposure document are directly related to the tone at the top (e.g., owner and/or executive management). The guide should enhance the recommendations relating to the overall governance of technology within small businesses. This should include:
    - Maintaining and encouraging an appropriate control environment that includes owners and managers who provide appropriate budgetary support, lead by example and encourage safe computing practices.
    - The performance of periodic risk assessments that facilitate in business terms, owner and manager decision-making on prioritizing risks, their remediation and concluding whether to accept, retain or transfer risk mitigation.
    - Designing controls that enforce owner and management implementation expectations of the recommendations in the exposure draft. Such expectations should take into consideration insider threats, and the segregation of responsibilities surrounding the custodianship, authorization, and recordkeeping of technology-related assets. Ensuring that owners and managers receive appropriate and accurate information that allows them to discharge their management and oversight responsibilities in a timely fashion.
    - Periodically monitoring the control environment to ensure that all related business and control objectives are achieved.

- Lines 148 – 149: Consider mentioning that regardless of their size, "small" businesses doing business internationally may be barred from doing business in the EU, India or other parts of Asia for failing to safeguard data belonging to citizens of any country with restrictive privacy laws.

- Lines 162 – 163: Consider adding “in a cost-effective manner” since many small businesses are afraid of the cost.

- Lines 180 – 182: In addition to focusing on customer and supplier interest, mention should also be made of the need of the small business to take advantage of the opportunities provided by technology.

- Lines 194 – 196: The text should also mention loss of consumer confidence, loss of business, and opportunity cost for lost time and cost of remediation.

- Line 195: Consider providing a more specific definition of “significant". What dollar value constitutes “significant”?

- Line 202 – 204: Consider mentioning who the notification laws require the small businesses to notify when there is a breach of data.

- Lines 211 – 212: Consider mentioning that the ability to accept electronic payments may be suspended due to poor security practices.

- Lines 211 – 212: Consider mentioning that the ability to accept electronic payments may be suspended due to poor security practices.

- Lines 218 – 221: Consider listing “cost–effective” information security programs in this final paragraph.

- Lines 220 – 221: It would also be beneficial to mention the importance of user security training and awareness.

- Lines 236 – 238: Consider including an additional sentence mentioning the importance of risk assessment to balance the cost of protection against the benefits of these threats.

- Lines 239 – 241: Rather than focusing solely on Cybersecurity firms, the consideration should also be reviewed by qualified professionals. For example, CPA firms and IT consultancies may have such expertise especially in the SMB market. It is important that such assessment firms remain independent of management and have no vested interest in selling other technology services.

- Lines 241 – 244: Consider simplifying the definition of a penetration test. It should state that a simulated attack on the business's computers occurs for the purpose of learning where an actual attack might focus.

- Lines 241 – 244: Given the limited budgets that many small businesses have to contract with outside experts, guidance should be provided as to when to do a penetration test vs. when to do a security audit vs. when to do a risk assessment. For many small businesses, using outside expertise for risk assessment assistance makes good business sense. In addition, it’s also important to help small businesses differentiate between penetration testing and vulnerability testing and understanding which is right for their unique situation.

- Lines 242 – 244: Consider providing examples of vulnerabilities in the security systems.

- Lines 264 – 267: As lines 239 through 244 appear to be implying that they have adequate funds to afford a penetration test, you may want to consider not promoting the free service or explain the advantages.

- Lines 268 – 273: Consider also mentioning the importance associated with keeping browsers and software up to date. Small businesses may not be aware that their software has fallen out of support and cannot be protected with new patches and updated malware.

- Lines 274 – 275: Consider explicitly saying buy vs. implying copying.

- Lines 274 – 276: Consider mentioning that doing business at home often exposes small business employees to greater risks.

- Lines 290 – 291: Small businesses should be asked to prohibit their employees from using their home networks and computers to process sensitive data.

- Lines 298 – 299: Consider including a recommendation that an Intrusion Protection System (IDS) or Intrusion Prevention System (IPS) and perimeter Anti-Virus be installed on the firewall. Activity on network devices should be logged and reviewed on a regular basis.

- Lines 306 – 307: As lines 239 through 244 appear to be implying that they have adequate funds to afford a penetration test, you may want to consider not promoting the free service or explain the advantages.

- Lines 307 – 309: This is an example of balancing risk assessment expenses vs. penetration testing expenses for outsider contracted services.

- Lines 312 – 315: Consider including information on outsourcing. Since firewalls can be complex and difficult to maintain, small business should consider outsourcing as many applications to a third party or cloud provider who is qualified to configure a firewall.

- Lines 360 – 362: Consider mentioning that if business needs dictate, it may be necessary for automatic data backups to run more frequently than once a week.

- Lines 360 – 362: Consider including a recommendation that backup data to removable or off-site storage be encrypted.

- Lines 415 – 423: Small businesses should also be aware of the wireless networks that attach to their devices. Consider adding guidance on how to view and disable unknown networks.

- Lines 450 – 451: This section should also caution small business owners to look for default accounts. Guidance should prompt small business owners to ask their value added resellers who install their systems to remove or disable default accounts.

- Lines 464 – 465: Consider mentioning that a system should mandate a password change every 3 months, and that employees should refrain from providing passwords over the phone.

- Lines 469 – 472: Consider adding a line to stress the importance of segregating responsibilities in a manual system between custodianship, recordkeeping and authorization.

- Lines 469 – 472: Consider including who should be responsible for each of these separate duties.

- Lines 475 – 479: Consider also making note of the fact that this often results in small businesses not enforcing preventive controls on these individuals and not adding detective controls such as monitoring.

- Line 559 – 560: Consider also mentioning the use of a Known Good Computer, which is booted from a read only CD/DVD before each use. The Lightweight Portable Security CD is available free from at http://www.spi.dod.mil/lipose.htm.

- Lines 565 – 571: Small business owners should also be prompted to consult with legal counsel, as common law cases have established that background check failures cannot be the sole cause for denial of employment.

- Lines 626 – 632: This should also make mention of printers. Depending on the model, they will need to beware of many of these same risks regarding printers.

- Lines 653 – 659: Consider also including that automated inventory detection should be done and reconciled, if possible, to the appropriate accounting records to make sure appropriate licenses are in place.

- Lines 666 – 672: There is no explicit mention in this section of the difference between the use of encrypted and un-encrypted removable devices. If a small business must use removable devices it is generally best practice to require that they be encrypted.

- Lines 666 – 672: There is no explicit mention of what a pre-boot agent is, but there is a significant difference from a risk/exposure perspective between having endpoint encryption with and without a pre-boot agent enabled.
- Lines 716 – 720: This should also make mention of record keeping, as they will want to consider the record keeping needed to effectively process insurance claims for damages.

- Lines 757 – 762: Consider re-emphasizing the importance of employee training for small businesses, by suggesting that employees sign these policy sheets upon successful completion of training at the beginning of their employment. In addition, consider mentioning that training should be an annual procedure, with policies re-taught and covered each year.

We appreciate the opportunity to comment and welcome the opportunity to serve as a resource to NIST on information security-related governance and risk management issues. If we can be of further assistance please contact Susan Pierce at (919) 402-4805 or at spierce@aicpa.org.

Sincerely,

Jeannette Koger

Jeannette Koger
American Institute of CPAs
Vice President – Member Specialization and Credentialing