AICPA Private Companies Practice Section

CPA cybersecurity checklist

Roman H. Kepczyk, CPA.CITP, CGMA

The seemingly daily occurrence of major cybersecurity breaches has made many accountants somewhat numb to the security threat posed by hacker criminals. Many people assume it is a "big corporation" problem, but the reality today is that businesses of every size are more vulnerable than ever. Recent headlines show that CPA firms are of interest because of the treasure trove of client financial data housed within firm networks. It is imperative that firm owners realize they have a fiduciary responsibility to protect this data which clients entrust to them and that this information is being directly targeted by hackers.

While there is no way to be 100% protected from cybersecurity threats, there are several steps firms can take to significantly minimize the risk of becoming a statistic. Below are 22 cybersecurity best practices CPAs should consider protecting their firms and client data. Firm owners should meet with their IT personnel (internal/external) and discuss each point to understand the firm's status and to determine which steps should be prioritized for remediation of the cybersecurity risk.

☐ Workstations should limit unauthorized access

- Screens should automatically lock after 5-20 minutes of non-use.
  - This will minimize unauthorized access if the user walks away from their computer.
- Turn off computers when not in use

☐ Enforce password policies

- At a minimum, firms should mandate the following hardened password rules:
  - Requiring users to change their passwords four times per year
  - Encouraging complex passwords or pass phrases (NoHackersOnMyWatch!)
  - Using password rules with a combination of numbers, letters, and special characters unique to each application and not numerically derivative of a previous password (AiCPA!01, AiCPA!02, AiCPA!03, etc.)
- IT should be involved when any employee leaves the firm to ensure the employee's network access and passwords are terminated.

☐ Use enhanced password controls

- Implement multi-factor authentication tools such as a physical security fob, biometric scan, or a two-factor authentication application (sends a passcode to a mobile device to be entered to validate the person signing in).
- Use password managers to generate a unique, complex password for each application.

☐ Keep on-premise data secure

- On-premise file servers should be in an unmarked, locked room to avoid physical theft.
- Workstations should have encrypted storage disks or run everything on the secured server or cloud so no local data can be stolen.
- Have an updated alarm system with a unique code for each employee that is disabled when an employee no longer works at the firm.
- Shred and dispose of all physical documents once transitioned to digital files.

☐ Document all firm-owned equipment

- Utilize inventory tags to track firm-owned equipment
    - Document acquisitions, assignments, and dispositions including procedures to erase, reformat or destroy any devices that might contain data.

☐ Confirm the location of all client data is known and secured

- Know where all client data resides and secure it.
- A data map should include what is stored on internal servers, workstations and mobile devices, backup systems, USB/storage drives, and cloud applications.
    - Access to these systems should be limited to users that absolutely need it.

☐ Ensure only trusted, validated users and equipment can connect to IT resources

- Only allow trusted, validated users and equipment to connect to the firm's IT resources.
    - Mobile Device Management applications require each workstation, tablet and smartphone to be individually registered to connect to the firm's network to minimize the risk of unauthorized equipment connecting.
    - Personnel should also be reminded of the importance of keeping their mobile device's operating system and security applications updated.

☐ Set workstations to automatically update the operating system and key applications

- One of the most successful ways hackers compromise network systems is through known vulnerabilities to operating systems that the firm has not yet loaded system updates to block.
    - Setting workstations to automatically update the operating system and key workstation applications may minimize this avenue of attack.
    - Requiring employees to turn off computers at night and reboot circulates these updates and clears out system clutter making the workstation more efficient.

☐ Minimize access to necessary levels

- Hackers that obtain administrative access privileges to networks and workstations have significantly more power to take control of network resources.
- Minimize users with administrator privileges and set access levels to the minimum level required by each user to complete their work.

☐ Ensure operating systems for all equipment are current

- Operating systems for all equipment comprising the network (file servers, firewalls, routers, Internet of Things [IoT] peripherals) should be reviewed regularly to make sure they are running the most current system updates.
    - It is critically important to change default passwords on all devices connected to the firm/home network including wireless printers, security cameras, connected home appliances, and voice activated devices.

☐ Confirm each fileserver, workstation, and mobile device have antivirus/security software installed

- Installed software should be automatically updated and actively scanning for malware on a pre-set schedule.
- Utilize the expanded capabilities of these applications to include intrusion detection and prevention in addition to Spam Management that will blacklist known threats and allow the firm to whitelist valid sites.
- Workstations should be set to automatically scan external media, such as a flash drive provided by a client, before loading files.
    - Better yet - don't allow the use of any flash drives and educate clients on the use of digital portals and secure email.

☐ Review backup logs regularly, verifiy data is accessible, and make shadow copies of changed files throughout the day

- IT personnel should regularly review backup logs to verify that data backups are complete, and randomly restore files to verify the data is accessible.
  - Encrypted data backups not only protect firms from lost/corrupted data but are critical if the firm is the target of a ransomware attempt.
  - Shadow copies of all changed files should be made throughout the day, so the most recent versions can be restored.
- All backup data should be encrypted, including that which is going offsite via the Internet.

☐ Utilize encrypted email and/or portal solutions for transmitting files

- All firm personnel should be trained on utilizing encrypted email and/or portal solutions for the secure transmission of files to and from clients. Firms should invest time in teaching clients to use the firm's system to foster adoption.

☐ Train employees to verify secure connections or to utilize a VPN connection when outside the office

- All employees should be trained to verify secure connections to websites (green padlock image and https: in the web address bar) or to utilize a Virtual Private Network (VPN) connection when working outside the office and accessing the Internet and/or firm resources.
  - When working remotely, personnel should also verify the SSID/password for client-provided Wi-Fi access or utilize a secure digital cellular mobile hotspot rather than public Wi-Fi such as hotels, coffee shops or airports which can be stealthily compromised.

☐ Review IT policies annually and remind users of changes

- Technology is evolving rapidly and few firms have updated their IT/HR policies to reflect current changes including the security ramifications of BYOD (Bring Your Own Device), social media, and the remote workplace.
- Firms should review policies annually and remind users of changes along with updated Internet and computer usage policies.

☐ Provide security training as part of the firm's annual CPE curriculum

- In addition to providing an annual update on IT policies, all employees should be educated on current threats including:
  - Ransomware
  - Phishing
  - SMiShing (SMS phishing)
  - Vishing (voice mail phishing)
  - Other social engineering examples designed to make employees download malware that compromises the firm's security or inadvertently give out sensitive information.
- Employees should be reminded to be suspicious of unsolicited support calls and never provide login, password or to download a file without first confirming the identity of the caller.

☐ Promote awareness of current phishing schemes and recommended staff responses

- Employees need to be regularly reminded of current phishing schemes and to be trained on what to do if they receive a suspicious email.
  - Hovering over the sender's email address in the header or any hyperlinks allows users to verify properties and to ensure they match.
  - Employees should not click on a link or open an attachment within an email if the email is unexpected and suspicious.
  - If the user has any concerns, there should be a process to notify a member of the IT team to review the email or to contact the sender to verify intent.
- There are several services that provide ongoing phishing/security training and testing of employee's response to phishing emails which seem to peak in accounting firms around tax deadlines and holidays.

☐ Conduct background checks on anyone given access to the firm network

- A surprising percentage of breaches occur with the help of internal employees, so it is important to conduct background checks on anyone being given access to the firm network.
- IT needs to be involved to not only provide the minimum level of access to do the work, but to monitor access and terminate it when the project is completed.

☐ Develop a policy to greet office visitors

- Employees should be trained to ask unrecognized visitors in the office if they can provide assistance and escort them to the person they are meeting with.
- If there are any concerns about the validity of the visitor's response, a member of the management or administrative team should be notified immediately.

☐ Secure cybersecurity expertise

- If the firm's internal IT personnel are not able to provide an optimum level of cybersecurity expertise to protect the firm, they should consider partnering with external security-focused integrators.
    - These experts can help review the firm's network security and provide direction and implementation assistance on securing the firm including intrusion detection, prevention and ongoing system monitoring.

☐ Develop a breach response plan

- The best time to develop a cybersecurity incident response plan is before the firm finds out it has been hacked.
- IT should document the process and educate employees on what they are to do if they suspect a breach.
    - This training should include the steps IT will take to verify and mitigate the breach including identifying external resources and meeting insurance requirements.

☐ Review insurance policies

- Even the most protected firms are not immune to innovative new hacker threats, so it is important that firms also review their insurance policies to understand to what extent they are covered for lost productivity resulting from a cybersecurity breach.
- Firms should also include coverage for damages caused to any clients whose data may have been compromised and become victims of identity theft because of the breach.

While most compromised organizations envision super-sophisticated hackers using complex technical expertise to breach their system, the actual breach findings have shown that hackers most often utilize common phishing techniques, known system vulnerabilities, and social engineering approaches to get access to confidential data. In most cases, firms that address and deploy the above solutions can avoid most hackers.