CPA
Practice Advisor

FIRM MANAGEMENT

Data Security: What Could Go Wrong?

At the end of the day, cyberattacks can have a detrimental impact to firms. Don't wait until it's too late to develop an effective data security plan.

Christopher Stark • Oct. 03, 2022

The reality is, when it comes to data security, zero risk does not exist. There is nothing on the market today that can 100% protect you from a cyberattack unless you completely disconnect yourself from the internet.

In 2021, IBM reported that the average size of a data breach is 25,575 records, with each record costing the company $165 on average, and the total cost to a company averaging over $4.24+ million. It is critical that CPA firms implement proactive IT strategies using a multifaceted approach to protect their data security. Before we dig into the preventative strategies to combat threats, we need to understand what methods cybercriminals are taking to try and penetrate systems.

What's the Cyber Criminal's End Game?

Cyber criminals have countless reprehensible methods of conducting cybercrime, as noted below:

- **Send out phishing emails.** A phishing scam is when a nefarious source targets consumers by sending them an email which appears to be from a reliable source. The hacker asks the consumer to provide personal identifying information. The hacker then uses the information to invade the consumer's accounts or to open new accounts.
- **Collect personal information.** The cyber criminal's goal is to gather personal information to be used for other types of identity theft such as credit card or insurance fraud.
- **Infect a computer with ransomware.** The cybercriminal infects a computer with malicious malware which prevents access to files, systems, or networks, and requires payment of a ransom for their return.
- **Access further accounts within an organization.** Account takeovers can morph from a personal attack on a singular computer as an entry to compromise an entire system or network.

The threat of account takeovers continues to evolve as the number of scenarios cyber criminals can use to gain access to victim's accounts also evolves. It is important for C-suite executives and tech experts to understand their cybersecurity vulnerabilities.

Why Would Global Cybercriminals Target CPA Firms?

CPA firms are prime targets because of the sensitive, confidential, financial information accounting firms amass. Hackers target CPA firms for explicit information and then use the data to steal assets, ransom it, or sell the data to the highest bidder.

- **Obtain confidential, personal data.** Cybercriminals seek client data from CPA firms such as birthdays, Social Security numbers, and other personal information. The data is used to target and steal from specific clients or to sell the data to other

criminals who specialize in identity theft.

- **Attain financial information.** Cyberattacks on accounting firms seek specific account numbers, tax records, credit card information, and employee identification numbers.
- **Gain tax records.** Cybercriminals file fraudulent tax returns from information obtained from CPA firms. They steal tax returns and use the information for additional identity theft.

How to Minimize your Risk of a Cyberattack

It is imperative that CPA firms, regardless of size or composition, have vigorous cybersecurity protections in place. The risk of cyberattacks is disproportionally higher for smaller and medium sized organizations, who tend to be much more reactive than proactive. Below are mitigating steps to help protect your firm from possible cyberattacks:

- **Have a good backup strategy.** Hackers tend to want to go for your backups first, making you more vulnerable during the attack. CPA firms should have multiple backups using different technologies and be physically removed from the network, so in case of a malware infection, the backup data does not become infected.
- **Implement multi-factor authentication for everything.** By requiring multiple factors to prove your identity during the login process, you can drastically reduce the chance of unauthorized access.
- **Train employees about cybersecurity risks.** Educating employees about cybercrime such as phishing, malware, and ransomware attacks is an effective strategy. CPA firms should create a culture of consistent security awareness to reduce the risk of cybersecurity breaches caused by human errors.
- **Use Advanced Threat Prevent Technologies.** Leverage Next Generation Antivirus (NGAV), Endpoint Telemetry Data, DNS Filtering, Intrusion Prevention Systems, Reputation Based Threat Prevention, Data Encryption – the more the better! These security technologies learn users' habits and daily activities using behavioral detection, machine learning algorithms, and exploit mitigation so known and unknown threats can be anticipated, blocked, and immediately prevented.
- **Patch all systems.** Focus on patching any and all known, exploitable vulnerabilities.
- **Store data and information in encrypted databases.** Storing data in an encrypted database can deter cybercriminals from accessing the information.
- **Prepare your organization.** Have a cyber incident response and business continuity plan ready, to ensure critical functions and operations can remain

running if technology systems are disrupted. If your IT systems go down, how will day-to-day account management and communication continue with personnel and clients? Make sure important contacts are up to date & test it regularly!

Accounting firms are prime targets for cybercrime for specific reasons due to all the sensitive, confidential, and potentially lucrative information they have in their systems.

How CPA Firms Can Shift their Risk

Accounting firms have significant responsibilities to protect their clients' information from potential global cybercriminals. Adhering to the CISA guidelines is an important, proactive plan for CPA firms. More specific cybersecurity strategies are examined below:

- **Review cybersecurity insurance.** C-suite executives should determine if specific cybercrime insurance coverage includes state-sponsored cyberattacks such as what might be initiated by outside threats. Check for 1st person vs 3rd party insurance coverage, ransomware coverage, and employ an attorney who understands cybersecurity review your cyber insurance coverage.
- **Encourage a "security mindset" in employees.** Require multifactor authentication, training on data security policies and procedures, and remind personnel that phishing is still the most common cyberattack modality.
- **Enlist the help of IT security professionals.** Engage with cybersecurity experts who can help reduce your level of risk through deploying stronger security technologies, preventative solutions, help guide and enforce evolving security best practices. Having a cybersecurity team available 24x7x365 monitoring threats is a great peace of mind.

At the end of the day, cyberattacks can have a detrimental impact to firms. Don't wait until it's too late to develop an effective data security plan.

=======

Christopher Stark is President & CEO of Cetrom.

Firm Management • Security • Technology

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.