CPA
Practice Advisor

COVID-19

Firm Cybersecurity Measures Must Be Proactive and Forward-Looking in Uncertain Times

CPA firms that can strengthen their IT networks, improve their team's ability to work from anywhere securely and enhance their data protection tools with the future in mind will come out the other side of the coronavirus pandemic stronger than ever before

May. 08, 2020

The coronavirus pandemic has knocked many market sectors for a loop, including the CPA industry. CPA firms, like other companies across the globe, have had to pivot on the fly to transition to near 100% remote work environments while trying to maintain operational continuity and client relationships.

It's natural and necessary for CPA firms to be reactive during the COVID-19 crisis; but strong, decisive action around telework capabilities, cybersecurity and other critical risk management areas cannot be shortsighted. Lessons learned from building out a telework ecosystem and improving data security during the pandemic need to be applied to longer-term solutions that go beyond the current uncertainty of these unusual times.

CPA firms that can strengthen their IT networks, improve their team's ability to work from anywhere securely and enhance their data protection tools with the future in mind will come out the other side of the coronavirus pandemic stronger than ever before.

It doesn't matter, really, where your CPA firm stood from a cybersecurity and telework standpoint prior to COVID-19. The current crisis and its consequences should be a mandate for all CPA organizations to raise the bar when it comes to IT performance and security. Firms that had already adopted the cloud, had started leveraging AI for security and had functional remote work environments obviously had a less radical transition to make than CPA firms that were lagging behind the tech curve.

All CPA firms should now know fundamentally where they need to be at this time and in the future. How firms get to the same end will differ. The important point is that the spark that was COVID-19 doesn't dim as the curve flattens and life gets back to normal in the months ahead.

There are fundamental, proactive measures that all CPA firms need to build on now to ensure a less risky IT and data security future.

Understand the New Cyber Threat Environment

All CPA firms, regardless of their telecommuting preparedness, now face new data and cybersecurity threats that have emerged due to more and more of the workforce operating online remotely.

Many organizations are operating with the majority of their workforces using remote means. IT resources, both internal and external, are being stretched thin due

to the demand for help enabling remote work environments. Connectivity and bandwidth issues are being tested, and employees have been forced to perform more work on personal devices, which creates additional security risks. Therefore, data privacy risks have increased exponentially in this environment.

The key is for CPA organizations to build a remote work policy that can instruct employees on how to stay safe, as well as hold them accountable for putting the company at risk.

The bottom line is that CPA firms have to take the actions they can right now to protect their employees, sensitive data and their clients. Whatever CPA firms do now to stay safe has to be part of a long-term plan to be prepared for unexpected crises like the coronavirus pandemic.

AI Isn't Just for the "Big Four" CPA Firms Anymore

In order for CPA firms to keep their valuable client and company data secure, automation and Artificial Intelligence are a must to mitigate potential risk. New technology is now available that will enable CPA firms to automate security measures and integrate a more behavioral, always-on approach to keeping data secure.

AI and automation of time-consuming, error-prone manual processes can help create space for innovation. AI's always-on, 24/7/365 security scanning and monitoring is more secure than relying only on human security surveillance and slow-to-react antivirus software.

Partnering with a cloud service provider with deep data and information security expertise and current experience leveraging AI, machine learning and automation can literally be a company-saving strategic effort.

Educate and Train Continuously on Security Best Practices

Your staff represents one of the gravest cybersecurity risks out there; it is also possibly the most difficult to prevent. Human error, ignorance of possible threats, and poorly communicated internal protocols can very easily lead to network breaches.

The most effective solution: constant education and training of your staff.

A cybersecurity educated and trained workforce is your best line of defense against security breaches during COVID-19 and into the future. Heightened states of alert and

awareness cannot only exist in a time of crisis; they need to be steady states during normal times as well.

Training should be an ongoing professional development requirement that will reinforce company-wide security policies, such as requiring clear, enforced password rules, restricting access and permissions, making sure all devices are protected, requiring multi-step identity verification, and creating an IT policy with an Incident Response plan.

The coronavirus crisis most certainly evoked some of these actions across the CPA industry, but the transition from a reactive to a perpetual state of effective and proactive risk management is the key.

Adopt a New Mindset

The cloud, Artificial Intelligence, and automation are no longer mysterious or the musings of futurists; these tools are now best practices.

Building remote work ecosystems that include Virtual Desktop Solutions, deploying synchronous and asynchronous communication and sharing channels, and using virtual meeting technologies, to name just a few tools, are all IT elements that prepare CPA firms to remain agile during a crisis and to scale up when they enter growth mode.

To be able to react quickly and set a company up for future change and growth, CPA firms need to invest more heavily in IT tools and systems that enable this kind of environment.

New cyber threats are always emerging and COVID-19 won't be the last crisis your firm faces. Now is the time to keep the momentum going when it comes to upgrading your IT environment; utilize the lessons learned from COVID-19 while you move ahead with investing in the future of your company.

Take These Other Key Steps

In addition to altering your thinking on your cybersecurity approach, there are pragmatic steps you can take to enhance security.

- **Augment Your Data Backup Processes.** Implement multiple daily backups using different methods like the cloud and hard drive backups, for example. Backups should live outside your network, outside your physical office space and should

not be virtually connected to your network. The key is diversity of backup types and consistency.

- **Secure Home Networks.** More people are working from home because of the coronavirus, which means an increased risk of security breaches via home networks working with your CPA firm's data. Here are some tips for securing home networks:
    - Use a wired connection
    - Review equipment that's being used by staff at home
    - Run updates, patch and reboot until all updates are made
    - Subscribe to antivirus software
    - Use two-factor authentication (2FA)
    - Remain vigilant both about updates and staff behaviors/education about the threat environment
- **Establish Company-Wide Security Policies.** Technology like AI will not solve security issues. People remain a huge factor in the success of any cybersecurity system. Therefore it is critical that CPA firms build out, distribute and update an enterprise security policy that is clear and promotes accountability. This policy should include:
    - Clear, enforced password rules
    - Restricted access and permissions
    - Protection for all devices
    - Two-factor authentication
    - Documentation disseminated to all staff
    - Remote work/Bring Your Own Device Policy
    - A security emergency response plan
- **Stay Informed and Educated.** The cyber threat environment is constantly changing, so keeping abreast of the latest reports and threats is critical to keeping your data safe. Following IT security related resources like MSSP Alerts, Crowdstrike, Cybersecurity SmartBrief, and Tech Republic for cybersecurity updates.

IT augmentation and improvement is a never-ending commitment that needs to be made proactively so that your CPA firm can react skillfully in times of crisis and intelligently as it builds for the future.

Cetrom can help you achieve this dual mission of being prepared for the unexpected while planning meticulously for the future of your CPA firm.

========

Christopher Stark is the President and CEO of Cetrom, an industry-leading provider of custom cloud hosting solutions for CPA Firms. With more than 25 years of experience in all facets of the IT industry, and holding some of the industry's most prestigious technical certifications, Stark keeps his finger on the pulse of the IT industry and eyes toward the future.

COVID-19 • Firm Management • Technology • News • coronavirus accounting • coronavirus accounting firm • COVID-19

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.