new data and cybersecurity threats that have emerged due to more and more of the workforce operating online remotely.

Mar. 24, 2020

Businesses of every size and industry — including CPA firms of all shapes and sizes — are being upended and pushed into telecommuting work environments. Some CPA firms that have already invested in powerful, efficient and user-friendly telecommuting infrastructures powered by cloud computing have had an easier transition than those that are behind the curve.

However, 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.

What's Changed Due to the COVID-19 Pandemic?

- Many organizations will be operating with the majority of their workforces using remote means
- IT resources, both internal and external, will be stretched thin due to the demand for help enabling remote work environments
- Connectivity and bandwidth issues will be tested
- The national and international supply chains will be disrupted so sourcing hardware and other IT necessities will be challenging
- Employees might be forced to perform more work on personal devices, which creates security risks
- Data privacy risks will increase exponentially in this environment

What Are the New Threats Emerging Because of the COVID-19 Pandemic?

The cybersecurity field has already identified several ongoing security threats that have been sparked by the coronavirus outbreak. There are also many unknowns at this stage and potential threats that have not yet been labeled; knowledge of the vulnerabilities of business networks operating in pure remote work ecosystems is evolving and will continue to do so for the foreseeable future.

Here's what we do know right now:

- The World Health Organization (WHO) has issued an alert about coronavirus-based scams where the bad actor is posing as the WHO

- Misinformation campaigns are being deployed as phishing scams posing as

leveraged the coronavirus to penetrate IT networks across multiple industries. Phishing emails, malware, and ransomware attacks have also sought to take advantage of the coronavirus pandemic.

What Can CPA Firms Do to Keep Their Data and Networks Secure?

Cetrom is here to help during times like these where uncertainty leads to reassessment and then corrective action. Agile businesses will think differently about the way they operate after the coronavirus threat fades in the coming months.

For now, however, CPA firms should take the following into consideration:

- Add remote work standard operating procedures into your IT policy, or amend your existing remote work processes to consider the coronavirus factor
- Plan for more personal devices connecting to your business network
- Take into consideration that these personal devices might be connected to your network through less secure Wi-Fi home networks. The following is recommended to help secure your data while exercising BYOD
    - Use a wired connection (more secure and better connection)
    - Run updates on your PC, patch and reboot
    - Subscribe to an antivirus – most ISP offer free programs
    - Use Two-Factor Authentication for everything
- Educate your team about new threats and engage in open, transparent communication and cybersecurity training
- Amend incident response plans with a 100% remote workforce in mind

Take the Steps You Can Now But Plan for the Future

they also provide significant risk mitigation against the unexpected, like a pandemic.

We are experts at building cloud solutions that will enhance your CPA firm’s performance and elevate its ability to remain agile and pivot when confronted with the unpredictable. We offer Virtual Desktop services and capabilities as part of our overall menu of cloud solutions. Cetrom’s Virtual Desktop, also known as VDI or Desktop as a Service (DaaS), provides CPA firms the capability to stay up and running in the midst of an unexpected crisis, delivering peace of mind to the business, security to its team, and protection for the bottom line.

Whether your CPA firm needs quick fixes right now to deal with these unprecedented times or you’re exploring longer-term cloud-based solutions, Cetrom is here to help you navigate this crisis and future risks to business continuity and data privacy.

For accurate and trustworthy information on the coronavirus/COVID-19, please turn to these reputable sources about COVID-19:

- World Health Organization
- The Center for Disease Control and Prevention
    - Download the guide to keeping workplaces safe
- Johns Hopkins University

==========

Christopher Stark is President & CEO of Cetrom.