to avoid group gatherings, some offices went remote for the whole of the year and ...

Amy Vetter • Feb. 26, 2021

If you didn't begin 2020 relying on cloud-based technology to allow you to work from anywhere, you almost certainly ended it that way. With a global pandemic forcing us to avoid group gatherings, some offices went remote for the whole of the year and aren't thinking of returning anytime soon. Even if you plan to reopen fully once it's safe to do so, it's unlikely you'll ever go back to an environment where work-from-home (WFH) isn't an integral part of your operations. As such, it's probably time to ensure that your cybersecurity meets your current needs.

There are many ways to ensure that your sensitive data is kept safe from prying eyes, and the best plan of action will vary depending on the nature and size of your organization. That being said, there are a number of strategies that are worth

exploring for all firms. You're probably doing some of the items listed below, but it

airport. And they should never, ever open unsolicited links, whether they come via email, social media, text, or any other format. If they receive a dubious email, such as one purporting to be from a bank that doesn't feel quite right, it's always better to exercise caution. You don't want to end up with a phishing scam on your hands. You can even run fake phishing scams in order to test the vigilance of your team. While you're at it, it wouldn't hurt to encourage your clients to engage in these practices as well.

Virtual Protected Networks (VPNs) and Multi-Factor Authentication (MFA)

VPNs and MFA are two of the easiest ways to add enhanced security layers to your firm. A VPN requires users to sign onto a specific network in order to access certain applications. In other words, a user wouldn't be able to access their company data by simply being online; they must sign onto your network in order to do so. MFA requires users to verify their identity in at least two ways as a means of ensuring that a single lost password can't compromise a network. Under the best MFA systems, at least one authenticating factor will be randomly generated and time-sensitive, such as a code sent to a phone or accessed through an app like Duo. Stacking these technologies, making a VPN accessible only through MFA, makes them even more secure.

Zero Trust Security

If you want to have the highest level of security currently available, you may choose to go with a Zero Trust architecture. In a Zero Trust system, no devices are ever considered to be inherently safe. All devices and users must prove their authenticity at all times, use the most updated patches of all software, with security assessing threats in real-time. If you want to read more about the specifics of Zero Trust, you can follow the work of John Kindervag, the thought leader who coined the term. Microsoft also offers a helpful diagram explaining the system.

The most important part of any security system is making sure it is implemented

CPA Practice Advisor 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.