Brian Colpak Explains How Remote Work Could Leave Companies Vulnerable to Cyber Attack

Tech expert Brian Colpak believes remote work will be here to stay long after the pandemic ends. Here's why that increases the likelihood of cyberattacks.

BOSTON, MASSACHUSETTS, UNITED STATES, November 5, 2021 /EINPresswire.com/ -- When the COVID-19 pandemic began, companies worldwide had no choice but to adjust to a new work environment. Essential services shifted online as employees were forced to work from home.

As the pandemic has eased, many businesses have allowed employees to continue working remotely, at least part of the time. But, as tech entrepreneur Brian Colpak explains, remote work could leave companies vulnerable to cyber-attacks.

IT is well organized when employees are located in a central office -- or a few main offices. It's an infrastructure with a hub-and-spoke design, where all technology feeds into a major point of security.

All video meetings, documents, emails, messaging, and other essential data are managed and monitored through this central system. When employees work remotely, this hub-and-spoke design breaks down, increasing the potential for cyber-attacks.

A company's IT infrastructure is only as strong as its weakest link. Unfortunately, in a small working world, the IT department doesn't have complete control over all these links -- creating the potential for many weak spots.

Employees work on their home internet networks and potentially even public WiFi hotspots in libraries, restaurants, and coffee shops. These networks are not as secure as in-office networks, typically protected by the most up-to-date firewalls and other security features.

Routers on even home networks can be outdated and not as secure, especially if the internet service provider provides them. It's also more difficult for IT departments to ensure all devices have the latest security patches and firmware updates when employees work remotely.

These weak points in the remote work IT infrastructure provide an increased opportunity for hackers to steal passwords and gain access to a company's critical systems and data.

These challenges are not likely to go away anytime soon, as Brian Colpak says. So, what can companies do to protect themselves in this "new normal" of remote work?

First, all companies should provide basic security training to all employees working remotely. This training should include information on protecting passwords, installing security and patch upgrades when available, and avoiding using vulnerable networks.

Second, companies should consider moving as many systems to the cloud as possible. By moving vital systems and information to reputable cloud-based systems, businesses can add an extra layer of security.

Finally, all IT teams need to have systems in place to recognize potential cyber-attacks quickly, so measures can be put into action to prevent significant damage from being done. And, just in case a bad actor does gain access, companies need to have robust backup and recovery plans, so they aren't devastated.

Remote work is likely here to stay for the long haul. Brian Colpak says companies need to recognize this fact and the increased threat of cyber-attacks that come with it and implement in-depth security and planning measures to prevent what could be a devastating event.

About Brian Colpak
Brian Colpak is a tech entrepreneur and founder of Continental Global. After spending most of his career in managerial positions, he founded and led a company recognized as one of the top 100 fastest growing companies in Massachusetts before starting his current company. These days his main focus is on an upcoming project in Dubai.

Jessica Brown
Mercury News Media
email us here