ChannelLife
AUSTRALIA

Guides

cloud services # cybersecurity # it distributors # microsoft # partner programmes

Security risks plague SMEs in shift to remote working

cybersecurity # malware # covid-19

Fri, 8th Mar 2024

By Kaleah Salmon, Journalist

Follow us

The proliferation of remote working in the wake of the COVID-19 pandemic has led to an increase in security challenges that threaten this burgeoning business model. Start-ups and small businesses, an integral part of today's business tapestry, are particularly affected by their ecosystem, which inherently embraces flexibility, reduced costs, and a wider talent pool.

While the remote working industry undeniably offers enhanced opportunities, including improved collaboration and better work-life balance, it simultaneously opens the doors to nasty security risks such as unauthorised access, theft of company intellectual property, and malware. These issues, unfortunately, pose a looming threat to businesses, especially small and mid-size enterprises (SMEs), that have enabled remote work.

Remote work, which surged in popularity during the COVID-19 pandemic, has become a double-edged sword. On one side, it has promoted a paradigm shift in workforce management, benefiting both employers and employees. Companies can curtail operating expenses while employees relish the freedom of working from home and experience an improved work-life balance. However, the flip side of the coin is considerably darker, with the rise of security challenges that have the potential to damage companies financially and reputationally.

There has been a noticeable rise in security breaches in recent years, orchestrated through unauthorised access, theft of company intellectual property, and the introduction of malware into company systems. The threats are real and demand immediate attention if the benefits of remote work are to be fully realised. These threats could impact the financial standing of many student businesses and their prized reputation, which are hard to rebuild.

According to Paul Oppong, a thought leader in project and portfolio management, while these problems are startlingly real, they are not insurmountable. The solution lies in the adoption of greater security practices that provide robust protection to both employers and employees. This will create an environment where the possibilities of remote working can truly blossom without the constant shadow of security threats.

Mr Oppong said securing company IP utilised in remote areas is the first integral consideration. "Using a VPN (Virtual Private Network), which encrypts data transmitted over the internet, helps protect against unauthorised access by, for example, other people in the same location at the same time." He also suggests regularly updating software and providing employee training on identifying and avoiding potential security threats.

According to Mr Oppong, another way to combat security threats is to implement network segmentation and segregation, which involves dividing a network into smaller subnetworks to limit the spread of malware and unauthorised access. Additionally, remote access VPN clients can connect to an organisation's VPN gateway to gain access to its internal network, but not without authenticating first.

Regarding specific projects, Mr Oppong said business owners should consider workflow specifically for individuals who work remotely. He said, "It is important to ensure that employees use secure networks and devices. This can include using two-factor authentication and strong passwords, as well as ensuring that all devices are up-to-date with the latest security patches and software updates."

SMEs' ability to thrive in a remote-working model amidst security threats depends largely on how well they adapt and respond to these challenges. Armed with the right resources and foresight, SMEs can embrace remote working as a mainstay business model that champions flexibility, cost savings, and a worldwide talent pool while keeping security threats at bay.

While the rise of remote work has brought mixed blessings, SMEs can reap the benefits through diligent planning, robust security measures, and continuous vigilance while ensuring they are not susceptible to the associated risks. By addressing these challenges head-on, the remote work framework can be resilient and flexible enough to endure and thrive in this new world order.