Working from home? Be alert to cyber threats

The world is in chaos and everyone is vulnerable, this is the ideal situation for opportunistic cyber attackers who are constantly infiltrating networks and accessing large volumes of data, putting millions of people at risk. The threats are real and the attackers are always on the prowl.

John Mc Loughlin, CEO at J2 Software

Most businesses are implementing emergency plans to cope with the coronavirus and they are facing many new challenges outside the office environment. They are shuffling around to accommodate their staff and many are now allowing employees to work from home, but this could mean more disaster.

John Mc Loughlin, a cybersecurity expert and CEO at J2 Software, has warned companies to ensure they are protected from outside threats.

“Unsecured home networks, default passwords and excessive social media sharing are opening up holes in business cybersecurity. With many employees working from home for the first time, there will be many new problems that might not have been addressed or maybe not even thought of."

“Most businesses have just started to realise the magnitude of the cyber risk and many started making changes in their traditional setups to match the threat. Many are doing quite a good job in traditional cybersecurity and have been adequately protecting the perimeter. Now they have been thrown a massive curveball and are facing challenges that they never saw coming,” he adds.

7 tips to reduce the cyber risk of remote workers

Priyanka Naidoo 23 Mar 2020

At the office, these people are protected by secure WiFi and they sit behind company firewalls. The sudden move to home often means that the same people are now using laptops and desktops that have no firewalls and access systems using open remote desktop sessions.

“The simple truth is that simply picking up and moving people home without looking at the risks of remote connectivity can result in even more business disruption. There are simple steps to take and this could be an opportunity for a rapid and secure move to the new normal. Virtual work environments, collaboration and a remote workforce are now a reality. You can either do this safely and embrace the new normal or find yourself falling behind, or worse,” he warns.

With many more workers outside the corporate boundaries, it is key to ensure compliance around data security. This includes issues like data encryption and remote backups. The process and need for improved cyber resilience is something that requires even greater vigilance as staff move out of the business and access corporate networks remotely.

Cyber risk during Covid-19 outbreak

Rosalind Lake and Priyanka Naidoo 19 Mar 2020

Mc Loughlin says effective cyber risk management requires a comprehensive approach employing risk assessment, measurement, mitigation, transfer, and planning, and the optimal program will depend on each company’s unique risk profile and tolerance.

Security challenges can manifest whenever new technology is integrated into business infrastructure, bringing new and additional complexity to the company's technology footprint. The risks and exposures presented by new technologies must be weighed against the potential transformative business effects, and risk tolerance varies both by industry and by an individual company.

“There are tools to ensure security, compliance and allow you to confirm that the work is being done and completed within policy. These tools will assist management without infringing on the user’s ability to complete their work," he concludes.