How safe is it to allow employees to work from home?

As Level 4 of the nationwide lockdown kicks in, some companies are still rallying to empower their people to work from home. However, gaps in IT resources and security are set to bite many organisations as they continue to enable remote working strategies.

Mchael Morton

“Some companies are geared to enable remote workforces while for many others this is new and largely unchartered territory. It means allowing employees to access emails, networks, ERM, CRM and other enterprise tools from remote locations. Aside from the obvious challenges associated with allowing them to do this securely while keeping unauthorized eyes out, there is also the security of their WiFi and endpoints such as mobile devices and laptops to consider.

“Additionally, as companies try to retain cohesiveness and collaboration between teams, the use of online meeting apps has risen dramatically. The security of some of these applications is being called into question. There have also been reported breaches of well-known collaboration tools which makes it even more important to properly choose what your employees use and to ensure that these are secured effectively,” says Michael Morton, Solutions Architect at managed IT security company, Securicom.

To protect data wherever it is, companies need a holistic approach, with layers of security solutions to protect data in the most outlying places and on the diversity of endpoints upon which it is found, right to the core, being the network.

Methodical approach to IT security

“Endpoint security is obviously crucial but if employees are using personal devices and computers for work and to access company networks and resources, IT admins have no idea what level of security they have or if they are compromised. Unless companies already have a Bring Your Own Device security strategy, they have no control over the security on these devices. It is not unusual for personal devices to have poor cybersecurity hygiene.”

So what’s the big deal when the priority is to keep the cogs turning during the Covid-19 crisis?

“The big deal is that company data is roaming freely and it is at risk. Essentially, companies’ network perimeters now extend to the homes of every employee working remotely. That’s a massive environment to secure and control.

“There are a few major problems associated with everyone who is anyone working within large, undefined and unsecured environments. Your financial information could be exposed; your business employees and customers are at risk of fraud; you could risk non-compliance with legislation around the protection of information, and you could face litigation if confidential information was to be exposed to unauthorised people. Also, your entire environment could be brought to a halt by a piece of malware.”

Morton concludes: “Certainly, getting employees up and running remotely is the grand prize. Business continuity in these uncertain times is highly prized. However, there are implications associated with not putting the necessary security measures in place. Company data could be compromised and the risk of fraud increases. You can bet that hackers will be taking advantage of companies’ quick and haphazard approaches to allow staff to work remotely.

“The solution is not to stop people from working remotely. In fact, this global crisis is showing us that working remotely can be extremely efficient and productive. It just requires a methodical approach to IT security.”