Understanding and mitigating the new cyber security risk from remote workers

should be top of the agenda for HR professionals

In a rush to keep the 'lights on', many firms have moved their entire workforce out of the office to remote working as soon as lockdown became imminent and not prioritised the greater likelihood of a successful cyber attack on their remote workforce

For many, the shift has been a revelation as remote workers prove to be at least as productive as they were in their previous office-bound life, with employees enjoying the freedom and flexibility that comes from ditching the office commute and the need to be in the office at prescribed times.

Of course, it's not all plain sailing as people rely on the robustness and bandwidth of their own wi-fi, the ability to find a suitable (and quiet) space to work at home, while also coping with partners and children at home. The assumption that people would be working less hours remotely, or no more than usual has also been debunked with many working more hours.

More IT traffic, more chance of an accident

Given there is so much more IT traffic in the form of emails, web conferencing and other electronic communications however, the potential for employees and their organisations to fall victim to a cyber-attack has grown significantly. IT teams report seeing more traffic from cyber criminals who have recognised that remote working exposes office networks to a greater chance of being hacked and are targeting businesses with phishing scams and misinformation.

The human error element around cyber has increased and consequently companies are challenged with reminding people to be careful in their basic cyber security hygiene such as clicking on links in emails and password management in the hope of avoiding a successful attack and all the damage that it can inflict on an entire company.

Reputation lost

Take a recruitment consultant and the sensitive information they would hold in terms of payroll data for example. From a reputational perspective, loss of this type of confidential data can be hugely detrimental to their brand, while a loss of systems following a successful ransomware attack would be financially devastating – without their IT infrastructure they cannot operate.

Given these exposures, how aware are HR professionals of their enhanced remote working exposure? Surprisingly, perhaps, awareness varies. Some firms have a good handle on the risk and are taking additional steps to mitigate the problem. But there are still those who have been focusing on keeping systems up and running, and not yet accounted for their increased exposure.

CyQu offers a window into the increased risk

One solution is to employ a tool like Aon's online risk assessment platform CyQU (Cyber Quotient Evaluation). Designed to assess cyber security exposures across a number of domains such as data security, access control and third parties, a new additional domain has been added to look at remote working. In ninety minutes or less, businesses can receive a snapshot of their cyber maturity and get clear, actionable strategies to help strengthen their cyber resilience.

It's a simple way for professional services firms to get a handle on their remote working exposure particularly as it becomes more likely that, even though firms might be considering a return to the office, some degree of remote working will become a permanent fixture for most employees. In turn, this means the increased cyber exposure is unlikely to diminish, placing the emphasis on firms to be proactive in how they manage the risk.

By taking a decisive step against cyber criminals targeting a remote workforce, a tool like CyQu could be the critical difference between business as usual or a damaging data loss and system outage.

Find out how Aon's CyQu can help your business assess its remote working cyber exposure.

Aon's online risk assessment platform CyQU

AON
Empower Results®