Securing the home office: just as important as securing the big business workplace

SOHOs and staff working from home tend to overlook the cyber security risks around their home office, warns Networks Unlimited, distributor of Fortinet.

Anton Jacobz

Small, home offices and corporate staff working from home are typically less security aware and so at greater risk than those working in large corporate environments, says Anton Jacobsz, Managing Director of Networks Unlimited. While larg enterprises generally have remote workforce and mobile device management systems in place, the holiday season often sees employees who don't usually work from home, catching up on outstanding work while on leave.

Small-to-midsized enterprises may well take advantage of the office downtime to get their work in order. And micro enterprises likely won't stop working through the festive season at all.

Jacobsz notes that small, home office environments should be treated as a micro version of a corporate environment wher comes to information security. "Depending on your line of business and the information you have on your PC, laptop and mobile devices, you must take the appropriate measures to secure this environment," he says.

"The problem is that many people have a false sense of security about their home environment. They think that they won't targeted, because they are hard to find at their homes." However, there are numerous information security risks facing hc users. It has become increasingly common for cyber criminals to target individual employees as a channel through which breach the networks of the company they work for, says Jacobsz. Other threats are that a user's devices could become infected and used for DDOS and phishing attacks; or that criminals could use the devices as a means toward identity thef to steal money.

BYOD protocol

While enterprise BYOD protocols may be in place and intended to cover the home office, not all staff abide by them, eithe because of lack of awareness or because staff feel inconvenienced by them. A Fortinet study last year found that among 32 year old employees, more than half would contravene company policies restricting use of own devices, cloud storage a wearable technologies for work. Over 55% indicated they had experienced an attack on personally owned PCs or laptops, but 14% of respondents said they would not tell an employer if a personal device they used for work purposes became compromised.

Awareness and education remain one of the most important aspects of information security.

In addition to a lack of awareness, security weak points at home include a failure to use effective passwords, and even yo own children, says Jacobsz. "You'll often find that while a user has security measures such as a firewall in place, their kid will change the laptop security settings in order to access certain sites.

The home wireless network can also be put at risk when users give the wireless password to their kids and all their friends

And people still use weak passwords, or the same password for every site they need to log in to. This is very risky."

"Effective home office security begins with awareness, and an assessment of the information you work with, and the risks should that information be compromised, advises Jacobsz. "Get advice from security experts," he recommends. "Our partners include security experts and even penetration testing and risk analysis experts."

Based on this, appropriate security measures should be put in place. These might include:

* Effective passwords and access tools to protect each PC, laptop and mobile device, and tools to allow for remote wiping of the device if it should be lost or stolen.
* Secure and effective firewalls and anti-virus tools, preferably from a reputable vendor, offering 24/7 risk updates.

* Company-owned devices could have a VPN installed to allow the user to access secure environments.