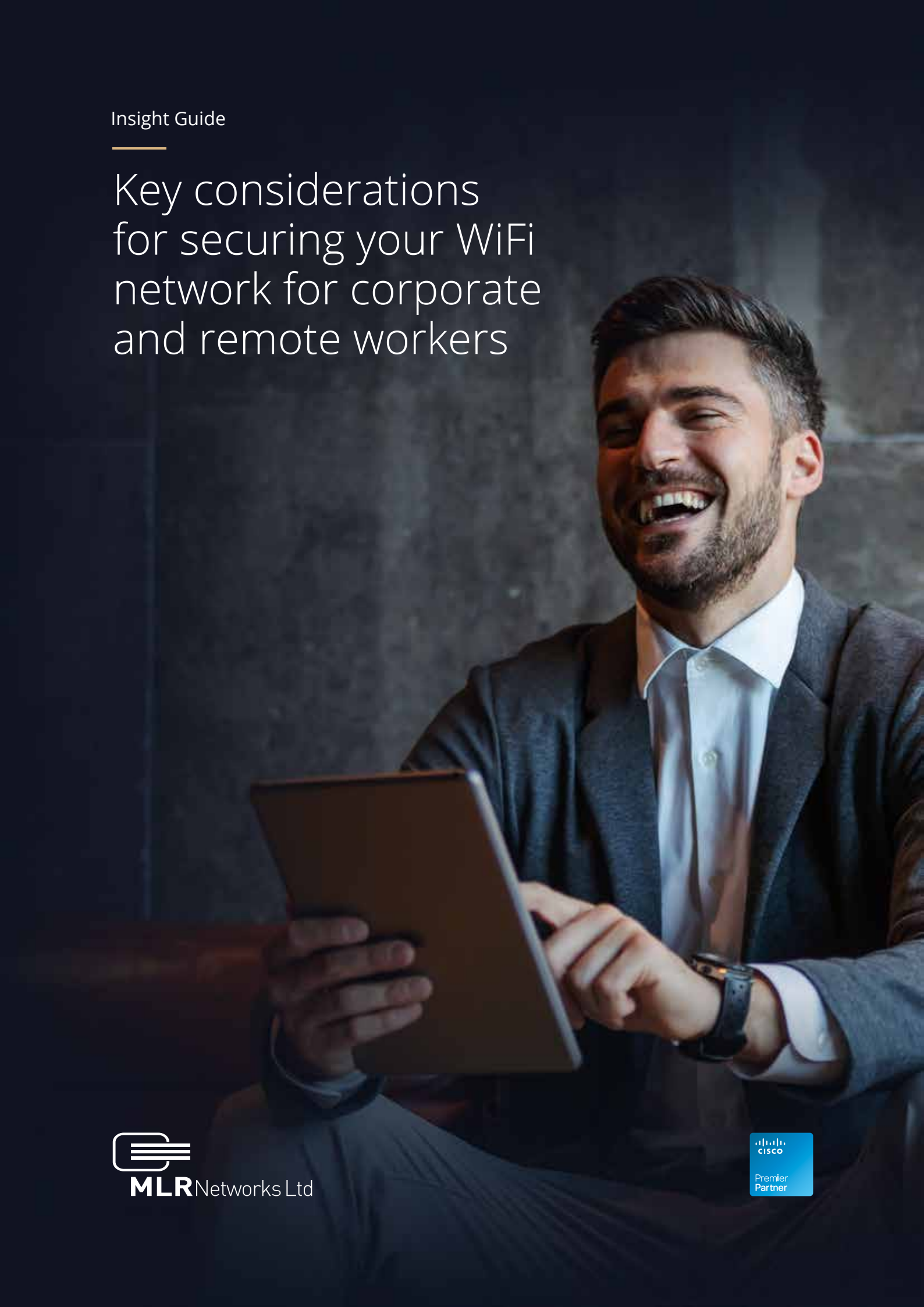
Insight Guide

Key considerations for securing your WiFi network for corporate and remote workers



MLR Networks Ltd

Cisco Premier Partner

Secure your WiFi network for corporate and remote workers

These days, most of your company's data is likely to exist in digital format. However, the fact that WiFi has replaced a large proportion of physical wire boundaries with virtual ones, devices have evolved from static PCs to roaming ones, and more people than ever require remote access to their employer's network can all pose a number of security risks. It's no longer sufficient to rely on your WiFi's default firewall – technology has evolved, and security needs to keep up with it.

Cyber security breaches can be deliberate, as in the case of a brute force attack (a trial-and-error method used to crack encrypted data) or unwittingly from the inside, such as being a victim of an 'evil twin' or 'phishing' attack. As WiFi has become commonplace and the use of personal devices widespread, cyber attacks have evolved to take advantage of their inherent weaknesses.

How are Wireless Local Area Networks vulnerable?

For organisations like schools and colleges, hospitals, hotels, large retailers, and office complexes, WiFi comes with significant security problems, while an increasing reliance on IoT (Internet of Things) devices can leave further gaps in protection.

As we've mentioned, wireless Local Area Networks (WLANs) transmit and receive data using Radio Frequency (RF) rather than wires. This makes them vulnerable to a range of cyber security issues, including 'denial of service' attacks, where the network is deliberately overwhelmed by a large volume of traffic, hijacking by assuming the identity of a valid user, or eavesdropping, where 3rd parties intercept data.

Some more of the most common WiFi security risks include:

Piggybacking

The practice of using another subscriber's wireless internet access service without their permission or knowledge. Piggybacking can be done from any wireless-enabled computer. Once a rogue user has gained access, they can easily hack into sensitive information.

Wardriving

Wardriving is very similar to piggybacking. It is carried out by people who know that the broadcast range of a wireless access point makes internet connections available beyond the boundaries of a home. They drive around a given area, searching for unsecured networks, sometimes guided by a powerful antenna.

Evil Twin Attacks

An evil twin attack is where a WiFi signal, stronger than the legitimate one, mimics a public network access point to entrap unsuspecting users. These users will have no idea this is happening. The attacker can then use special tools to read the victim's data, including credit card numbers, passwords, and other personal information.

Distribution of Malware

Malware is software specially designed to damage, disrupt or gain access to a computer system. Hackers use unsecured WiFi connections to distribute malware and infect networks, so it poses a serious threat to your cybersecurity.

Protecting your business from WiFi security breaches

To counter WiFi security issues, whether they take the form of deliberate hacks or unwitting mishaps, you need a future-proof cybersecurity strategy that puts you in the strongest possible position and protects valuable data. Recent improvements in wireless protocols and infrastructure technologies have produced a range of viable WLAN security options.

The first line of defence should be to program personalised passwords on network devices. By eliminating default passwords that are easily hacked, you will give your network a baseline of cybersecurity and protection.

Having two separate Wi-Fi networks for staff and guests will also restrict unwanted access to your business's data and prevent unauthorised users from accidentally viewing sensitive information or infecting your network with malware.

Another strong countermeasure is to encrypt your company's wireless data. This prevents those who have gained unauthorised access from viewing the information within your network. Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA), WPA2, and WPA3 are all options that encrypt information effectively, but WPA3 is the strongest option.

How can remote workers access the company network safely?

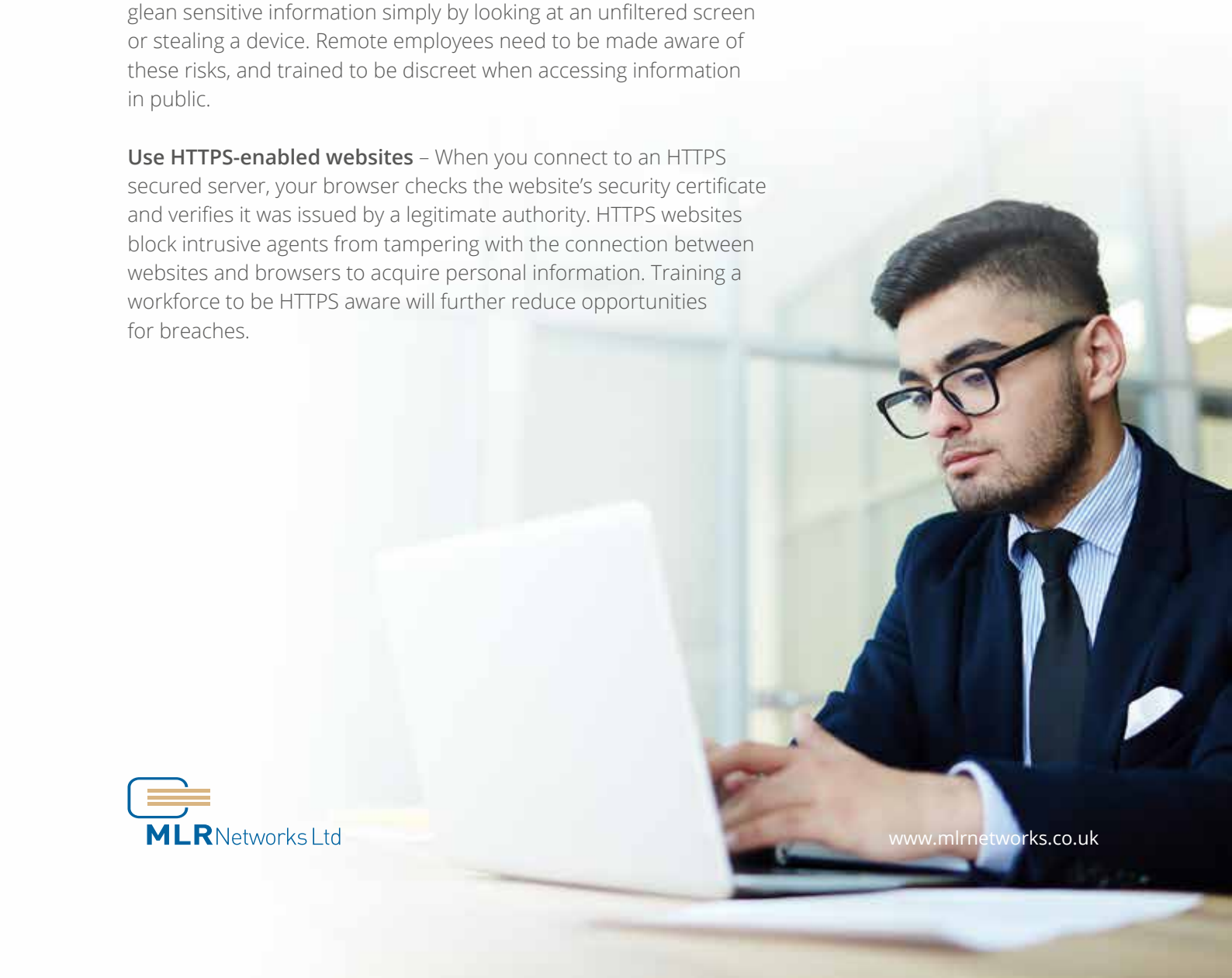
Your company's network will need additional security measures to protect its integrity as the remote workforce grows. Developing a comprehensive remote access policy including both technical and practical measures, will ensure remote employees are not a weak link in the network's cybersecurity:

Set up a VPN – A Virtual Private Network (VPN) allows remote workers to connect securely to the company network even when they're away from the office. VPNs encrypt transmissions at the start and endpoints and keep out unidentified traffic.

Employ strong encryption and enhance user authentication – External security threats can be mitigated by encrypting data and using enhanced authentication. This will help to protect the confidentiality and integrity of communications and securely verify identities.

Update public usage terms – In public settings, it's possible to glean sensitive information simply by looking at an unfiltered screen or stealing a device. Remote employees need to be made aware of these risks, and trained to be discreet when accessing information in public.

Use HTTPS-enabled websites – When you connect to an HTTPS secured server, your browser checks the website's security certificate and verifies it was issued by a legitimate authority. HTTPS websites block intrusive agents from tampering with the connection between websites and browsers to acquire personal information. Training a workforce to be HTTPS aware will further reduce opportunities for breaches.



Use Specialist Cyber solutions

There are now multiple, purpose-built cybersecurity programs on the market that are specially designed to deal with the complexities of WiFi, remote working and multiple devices. They can both protect the network and prevent unauthorised, malicious access to your data.

And today, network and device management doesn't even need to be tied to the office. Secure, cloud-based systems facilitate easy-to-operate remote networks that can be run from anywhere and almost any device, keeping WiFi networks secure wherever your workforce is based.

MLR Networks Ltd

www.mlrnetworks.co.uk

Connecting your business

Powerful, agile solutions for all
your infrastructure requirements.

MLR Networks Ltd

Head Office
Unit 9 & 10
Beeston Ct
Runcorn
Cheshire
WA7 1SS

0151 423 3633
sales@mlrnetworks.co.uk

www.mlrnetworks.co.uk