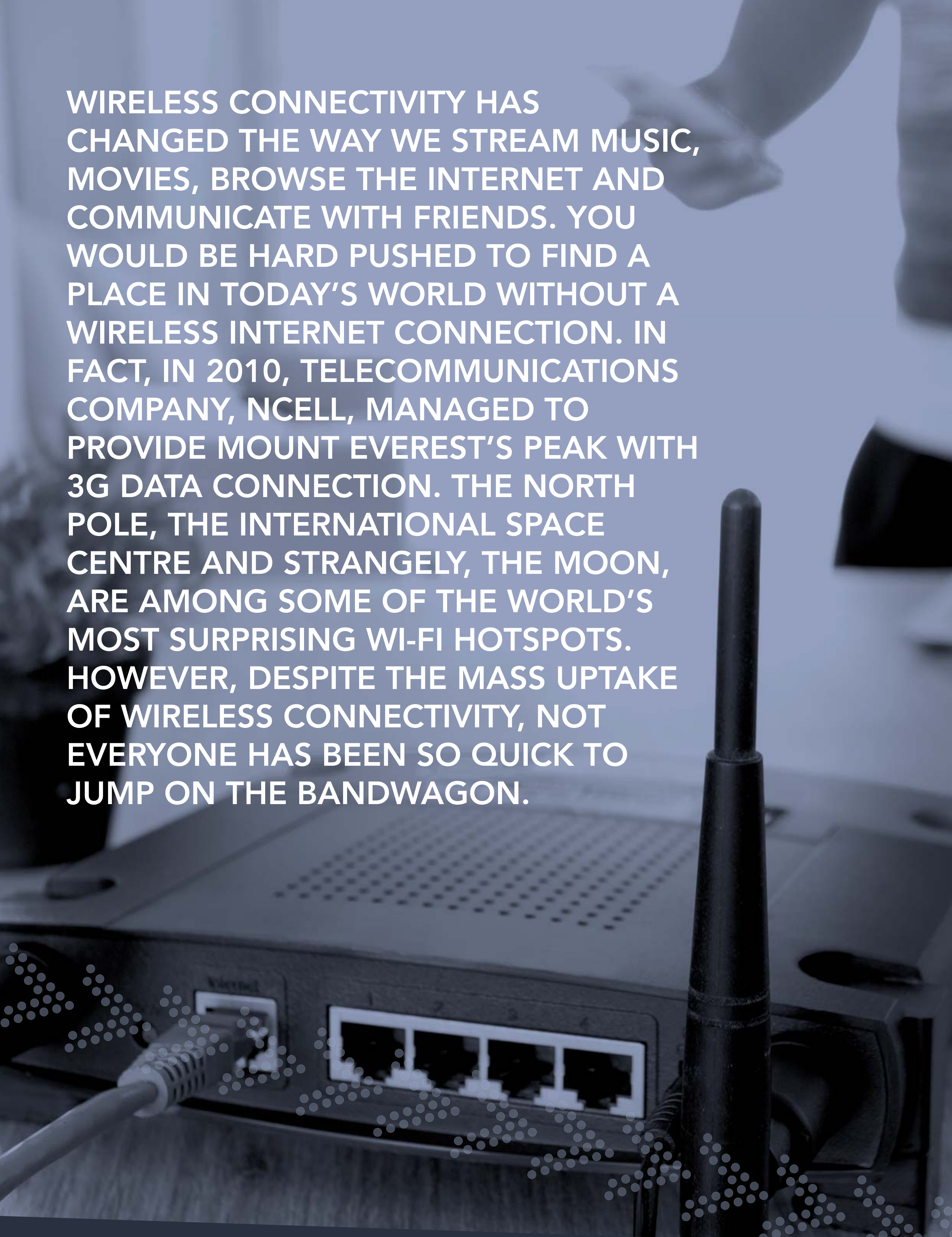
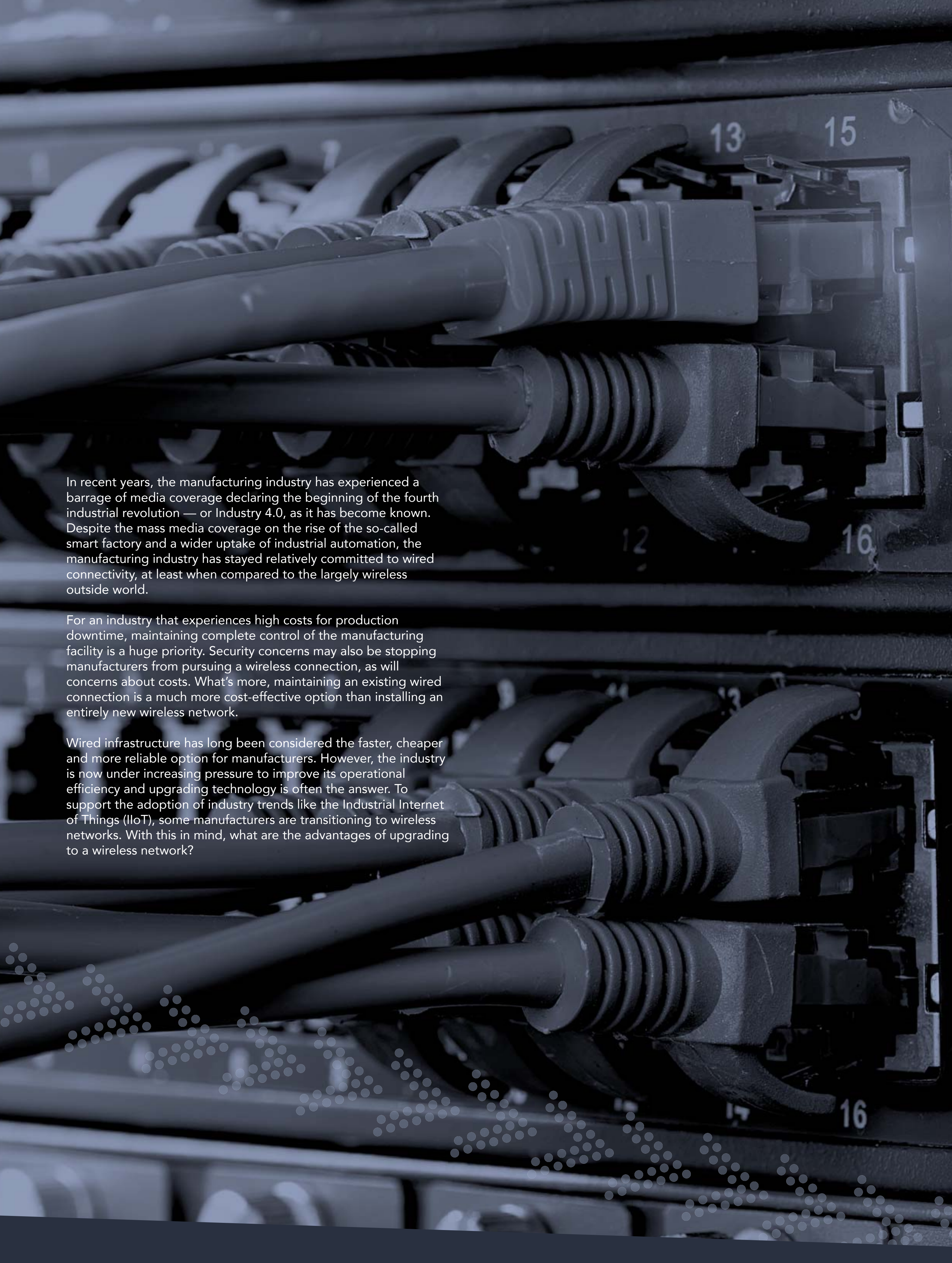
WIRED VERSUS WIRELESS

EUA AUTOMATION

SPECIAL REPORTS



WIRELESS CONNECTIVITY HAS CHANGED THE WAY WE STREAM MUSIC, MOVIES, BROWSE THE INTERNET AND COMMUNICATE WITH FRIENDS. YOU WOULD BE HARD PUSHED TO FIND A PLACE IN TODAY'S WORLD WITHOUT A WIRELESS INTERNET CONNECTION. IN FACT, IN 2010, TELECOMMUNICATIONS COMPANY, NCELL, MANAGED TO PROVIDE MOUNT EVEREST'S PEAK WITH 3G DATA CONNECTION. THE NORTH POLE, THE INTERNATIONAL SPACE CENTRE AND STRANGELY, THE MOON, ARE AMONG SOME OF THE WORLD'S MOST SURPRISING WI-FI HOTSPOTS. HOWEVER, DESPITE THE MASS UPTAKE OF WIRELESS CONNECTIVITY, NOT EVERYONE HAS BEEN SO QUICK TO JUMP ON THE BANDWAGON.



In recent years, the manufacturing industry has experienced a barrage of media coverage declaring the beginning of the fourth industrial revolution — or Industry 4.0, as it has become known. Despite the mass media coverage on the rise of the so-called smart factory and a wider uptake of industrial automation, the manufacturing industry has stayed relatively committed to wired connectivity, at least when compared to the largely wireless outside world.

For an industry that experiences high costs for production downtime, maintaining complete control of the manufacturing facility is a huge priority. Security concerns may also be stopping manufacturers from pursuing a wireless connection, as will concerns about costs. What's more, maintaining an existing wired connection is a much more cost-effective option than installing an entirely new wireless network.

Wired infrastructure has long been considered the faster, cheaper and more reliable option for manufacturers. However, the industry is now under increasing pressure to improve its operational efficiency and upgrading technology is often the answer. To support the adoption of industry trends like the Industrial Internet of Things (IIoT), some manufacturers are transitioning to wireless networks. With this in mind, what are the advantages of upgrading to a wireless network?

BENEFITS OF WIRELESS CONNECTION

Manufacturers are under constant pressure to improve operational efficiency. Wired infrastructure has long been considered the faster, cheaper and more reliable option, but to support the adoption of industry trends like the Industrial Internet of Things (IIoT), some manufacturers are moving towards wireless networks instead.

The introduction of new internet protocols appears to be bridging the benefits gap between wired and wireless connectivity. For the most part, industry is beginning to move away from traditional and proprietary technologies and instead, is recognising the emerging wireless options that could rival their wired predecessors.

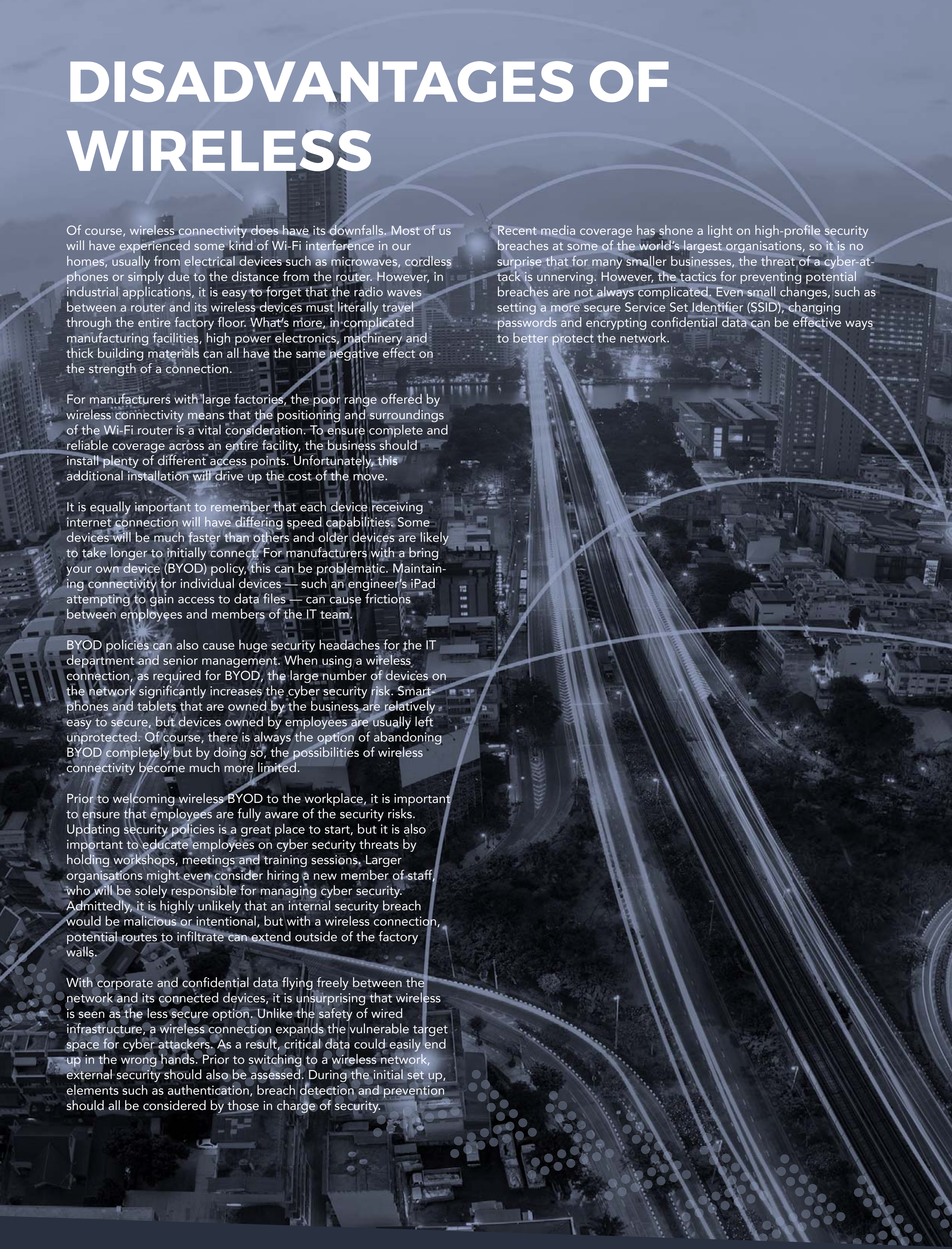
6LoWPAN technology, for example, is the first wireless network specially designed for use within the Internet of Things (IoT). As a new application, 6LoWPAN uses internet protocol version six (IPv6), whereas the consumer internet is largely based on its predecessor, internet protocol version four (IPv4). IPv4 allowed space for around 4.2 billion unique IP addresses, but in 2011 this capacity proved insufficient and it was exhausted. In contrast to IPv4's limitations, IPv6 holds space for an incomprehensibly large amount of IP addresses. In fact, enough space for the internet – the IoT and the IIoT - to grow for decades to come.

Upcoming 3G-based protocol High Speed Downlink Packet Access (HSDPA), could be another factor to swing faith in favour of the wireless camp. Impressively, HSDPA will support wireless download speeds of up to 14.4mbps surpassing the speed of many wired networks. Following the HSDPA introduction, the next logical stage would be to introduce High Speed Uplink Packet Access (HSUPA). HSUPA aims to improve uplink speeds to an impressive 2 megabytes per second. In fact, some large telecommunications companies have tested this protocol with great success.

Wireless advancements are impressive and according to a report by market analyst firm Berg Insight, the number of active wireless devices in the industrial automation market has already surpassed 10.3 million. With the estimated annual growth rate at 27.2 per cent, this figure is expected to reach 43.5 million by 2020.

However, it is not just technological capabilities that are persuading some businesses to cut the cord on wired infrastructures. In contrast to the wired model, wireless networks are less affected by outdoor terrain and poor weather. This tolerance for extreme conditions make wireless an ideal option for the oil and gas industry — particularly for those operating offshore. Wireless networks can provide connectivity when both fixed and mobile. This improved flexibility can supply internet connection across much wider geographical locations, where a wired infrastructure would not have been viable.

Despite common delusions, moving from a wired infrastructure to a wireless network is not hugely complicated. In truth, the process can be incredibly fast. Following the initial set up, deployment times are almost instant and require no additional set-up or extra installation costs. Instant deployment provides businesses with the opportunity to expand and adapt freely, without having to completely rewire the facility.



DISADVANTAGES OF WIRELESS

Of course, wireless connectivity does have its downfalls. Most of us will have experienced some kind of Wi-Fi interference in our homes, usually from electrical devices such as microwaves, cordless phones or simply due to the distance from the router. However, in industrial applications, it is easy to forget that the radio waves between a router and its wireless devices must literally travel through the entire factory floor. What's more, in complicated manufacturing facilities, high power electronics, machinery and thick building materials can all have the same negative effect on the strength of a connection.

For manufacturers with large factories, the poor range offered by wireless connectivity means that the positioning and surroundings of the Wi-Fi router is a vital consideration. To ensure complete and reliable coverage across an entire facility, the business should install plenty of different access points. Unfortunately, this additional installation will drive up the cost of the move.

It is equally important to remember that each device receiving internet connection will have differing speed capabilities. Some devices will be much faster than others and older devices are likely to take longer to initially connect. For manufacturers with a bring your own device (BYOD) policy, this can be problematic. Maintaining connectivity for individual devices — such an engineer's iPad attempting to gain access to data files — can cause frictions between employees and members of the IT team.

BYOD policies can also cause huge security headaches for the IT department and senior management. When using a wireless connection, as required for BYOD, the large number of devices on the network significantly increases the cyber security risk. Smartphones and tablets that are owned by the business are relatively easy to secure, but devices owned by employees are usually left unprotected. Of course, there is always the option of abandoning BYOD completely but by doing so, the possibilities of wireless connectivity become much more limited.

Prior to welcoming wireless BYOD to the workplace, it is important to ensure that employees are fully aware of the security risks. Updating security policies is a great place to start, but it is also important to educate employees on cyber security threats by holding workshops, meetings and training sessions. Larger organisations might even consider hiring a new member of staff, who will be solely responsible for managing cyber security. Admittedly, it is highly unlikely that an internal security breach would be malicious or intentional, but with a wireless connection, potential routes to infiltrate can extend outside of the factory walls.

With corporate and confidential data flying freely between the network and its connected devices, it is unsurprising that wireless is seen as the less secure option. Unlike the safety of wired infrastructure, a wireless connection expands the vulnerable target space for cyber attackers. As a result, critical data could easily end up in the wrong hands. Prior to switching to a wireless network, external security should also be assessed. During the initial set up, elements such as authentication, breach detection and prevention should all be considered by those in charge of security.

Recent media coverage has shone a light on high-profile security breaches at some of the world's largest organisations, so it is no surprise that for many smaller businesses, the threat of a cyber-attack is unnerving. However, the tactics for preventing potential breaches are not always complicated. Even small changes, such as setting a more secure Service Set Identifier (SSID), changing passwords and encrypting confidential data can be effective ways to better protect the network.

WIRED AND WIRELESS: BETTER TOGETHER?

There are valid arguments on both sides of the wireless vs wired debate. There is no denying that wireless networks are becoming more popular and advanced, but equally, they are a long way away from becoming the industry standard. For the manufacturing industry, there is far too much legacy infrastructure in place to simply rip out wired networks and replace them with a wireless set up. Clearly, this would not be a sensible option. So, could a combination of the two be the answer?

Maintaining both wired and wireless connectivity means that businesses can experience the advantages of both. Some applications are undoubtedly better off when connected to a wired network. Vital factory equipment for example — which could cause halts in production when internet connection fails — is much safer and more reliable when connected to a wired infrastructure. On the contrary, the implementation of BYOD policies and IIoT relies on the adoption of wireless internet. Similarly, businesses cannot satisfy the needs of mobile workers just by using a wired connection.

From the point of view of management, this combination may seem like a logistical nightmare. However, that does not have to be the case. Leaders in technology are already developing ways to make this process easier. IT giant, Cisco, has already unveiled its answer to this problem by creating a combination platform which will bring wired and wireless connections together, in one simple switch.

The ongoing debate on the superiority of each option is not a conclusive one. Managing both together, businesses should expect to feel significant advantages, while also reducing the negatives associated with either installation. For the time being at least, a combination of wired and wireless networks is the way forward.