PROTECTING YOUR DISPERSED WORKFORCE:

Cyber security in the new normal

ITPro.

IN ASSOCIATION WITH

O2 business

EDITORIAL

Editor
Maggie Holland
maggie_holland@dennis.co.uk

Contributors
Hugh Armitage

Design and layout
Will Haywood

Head of Content Strategy
Riyad Emeran

ADVERTISING & REPRINTS

Advertising Director
Chris Cannon
chris_cannon@dennis.co.uk

LICENSING & SYNDICATION

International Licensing
Dharmesh Mistry

MANAGEMENT

Publisher
Paul Franklin

Chief Revenue Officer
Julian Lloyd-Evans

Chief Executive
James Tye

Company founder
Felix Dennis

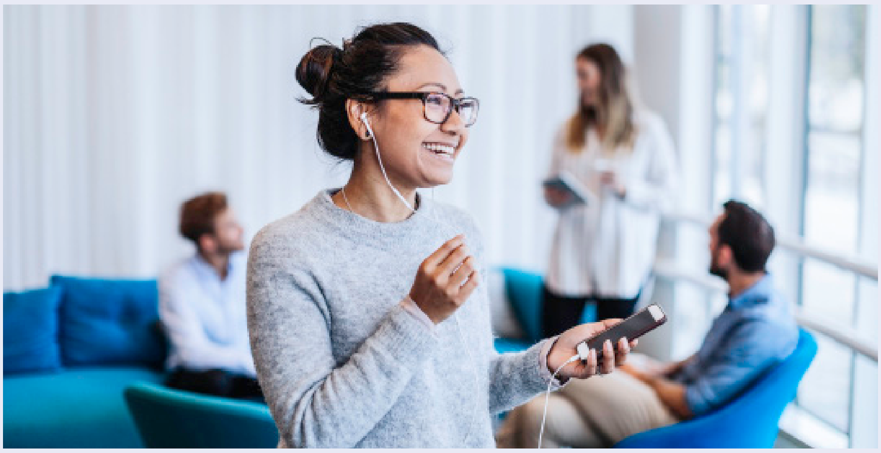
Liability
While every care has been taken in the preparation of this magazine, the publishers cannot be held responsible for the accuracy of the information herein, or any consequence arising from it.

Dennis Publishing Ltd

WELCOME

The events of 2020 have completely changed the way we work with a suddenness greater than anything we have experienced before. With the emergence of COVID-19, the remote-working model immediately pivoted from a slowly emerging option to an essential tool for keeping many business sectors operating during this challenging time. This shift hit hard and fast, and the resulting transformation looks likely to impact the world of work not just for the duration of the pandemic but for years and perhaps decades to come.

These changes bring fresh security risks, as new holes open up in our defences and cyber criminals rush in to exploit them. In this whitepaper, we will assess the new cyber threat landscape and outline the steps to take to protect your organisation.



ABOUT O2 BUSINESS

With greater flexibility and an unrivalled service, O2 helps you stay connected whenever you're doing business. O2 gives your business the coverage, reliability and security it needs to operate effectively. Flexible options include Data Rollover, which automatically rolls over your excess data to the next month, flexible tariffs, and contract lengths that suit you, from 30 days to three years. O2 understands that every business is one of a kind, and therefore provides you with a premium service tailored to your unique business needs.

*Data Rollover: For new or upgrading customers only. Available on selected tariffs of 6GB of data or above, excluding 2GB triple data, 3GB double data and unlimited data tariffs. Up to 100% of unused data from standard monthly data allowance can be rolled over into the following month. Eligible data rolls over for one month only. Any data that cannot be rolled over will expire. Any unused data will not rollover if you decide to change to an alternative tariff. Subject to availability, status, credit check and general terms for business customers apply. Terms apply, see o2.co.uk/terms

THE NEW SECURITY SITUATION

Remote working has become an option for an increasing number of UK employees in recent years, enabled by changing management attitudes coupled with a boom in mobile devices, cloud-based collaboration tools like Microsoft 365 (which is available as a monthly add-on through O2 Business) and other technologies that have made it easy to work in any environment a person chooses. However, until recently it remained a nice-to-have option rather than something deemed a business essential. A survey conducted by the Office for National Statistics (ONS) found that 8.7 million people said that they had worked from home in 2019 – a sizable number, but still less than 30% of the UK workforce.

But come 2020, a new ONS report revealed that in April – at the very height of lockdown – 46.6% of people in employment in the UK did at least some work from home. With travel restrictions in place and town centres practically deserted, it seems safe to assume that a large proportion of that 46.6% did all their work from home. As restrictions change and ease, some workers will head back to the office, but for others the benefits of remote working have been established and they are unlikely to want to give them up (according to O2 Business report, The flexible future of work, 45% of people want flexible working to strike a better work-life balance). With the technology to achieve this in place and its efficacy demonstrated, it will be hard for businesses to say no. A hybrid model of office and remote working is likely here to stay.

But this dispersed working model poses challenges as well as opportunities. While security perimeters had already been growing increasingly porous thanks to the emergence of the cloud and the multiplying of internet-enabled devices connecting to business networks, remote working has greatly accelerated the process. A company may find that the majority, if not all, of their workforce is operating beyond the safe confines of its on-premises network. Many organisations will have had to adopt 'bring your own device' (BYOD) policies – where employees work from their personal computers, laptops, tablets and other devices – in order to make the quick pivot to remote working. Ensuring that these devices are properly protected with antivirus software is a challenge, not to mention simply maintaining oversight of all the devices workers are using to connect to your network. Vulnerabilities can easily multiply in this environment, and any one of them can be exploited by a malicious actor.

And all the while, the cyber threat landscape is not standing still. These threats continue to evolve. Securing your organisation against these cyber criminals while compensating for the new vulnerabilities created by our new working practices is a challenge, but there are steps that you can take to keep your company safe.

KNOW THE RISKS

The first step towards securing your business is to understand the threats you are facing and the potential vulnerabilities of your systems. Armed with that understanding, you will be best placed to choose the right methods for shoring up your defences.

A key issue for maintaining cyber security is one we've touched on already – the profusion of devices attached to your network, otherwise known as 'endpoints'. Each endpoint represents a potential route by which a malicious actor can access your critical systems and data. There may also be more endpoints than you realise – it's not just a question of laptops and smartphones, but also printers and a huge variety of Internet of Things (IoT) devices (which are especially worth bearing in mind as workers begin to transition back into the office).

It only takes one unsecured device to allow cyber criminals into your network, and no organisation is immune. NASA learned this when it discovered that 500MB of data, including information regarding the international transfer of restricted military and space technology, had been stolen from its Jet Propulsion Lab over the course of 10 months. The culprit? A simple Raspberry Pi that an employee had attached to the network without informing IT. Endpoints pose two key challenges: gaining full visibility of every endpoint connected to your network and properly securing them against malware, ransomware and other attacks and intrusions. This has become even more difficult now that the majority of the workforce is not operating on the same premises as your IT department.

The story doesn't end once your network perimeter has been breached. Once inside, an attacker will move laterally through your network, assessing it to identify valuable targets such as financial or personal data, or critical systems. Using compromised or stolen credentials and leveraging privileged access and trusted paths within the network, malicious actors can do serious damage without ever being detected. With the new working models making our perimeters ever more porous, it is more important than ever to consider not only how to keep attackers out, but how to contain any that are able to gain access to your network.

Many security breaches are not down to technical issues but simple human error, so your work culture is an area that shouldn't be forgotten. Workers need to be wary of risky online behaviour, seductive phishing scams and any other activities that could leave your network vulnerable, such as exposing or failing to secure login credentials. Organisations must ask themselves whether remote workers are receiving sufficiently clear, consistent and regular messaging about the behaviours and risks that could leave the business open to cyber attacks.

PLAN YOUR DEFENCE

Armed with an understanding of the sort of threats and risks facing your business, the next step is to take action to mitigate them. It's important not to forget the basics. Password security is unglamorous, but it shouldn't be ignored. IT teams might be the security experts, but even they aren't immune to reusing the same passwords, sharing them too freely and not updating them regularly. Take time to ensure that WiFi networks are secured, encrypted and not left on default password settings, and any other routine measures and upkeep that can go neglected.

Firewalls have long been a standard tool to protect your on-premises network from outside attackers by monitoring and controlling incoming and outgoing traffic, but these new working models mean many of our devices now fall outside of that protection. Fortunately, there are various solutions that can step into this gap, with innovative technologies to defend your workforce.

Endpoint protection is an important tool in this arsenal. As already noted, endpoints are a key area of attack for hackers, and it is next to impossible to manually maintain a comprehensive catalogue of endpoints across a dispersed network. Thankfully, there are many tools and systems available to help protect your endpoints from infiltration, from the standard antivirus software services to identify and block malware, ransomware and other attacks, to those that will detect if an endpoint has been compromised and quarantine it to protect the rest of your network. Cloud-based services can easily be installed remotely on devices, including personal hardware being used under a BYOD policy. Security experts Sophos (whose services can be bundled with O2 Business) offer Intercept X Endpoint, one of a variety of newer solutions that also employ

machine learning to identify emerging threats, so that they protect not only against established malware but previously unidentified attacks. This is especially valuable in confronting an ever-evolving threat landscape, offering proactive protection that is less likely to fall behind and leave your network vulnerable.

Emails are a common method of infiltration, particularly in the form of phishing attacks that attempt to trick the recipient into handing over login credentials and other sensitive information. These attacks have surged in 2020, with the NHS reporting in August that it had received 43,108 malicious emails at the height of the COVID-19 pandemic and the BBC claiming that coronavirus-related phishing attacks had resulted in a loss of £2 million in the UK as early as April. Services like Sophos Email Advanced can combat these threats by scanning incoming emails and highlighting and quarantining threats as well as blocking suspicious accounts altogether.

For the malicious actors that are able to infiltrate your perimeter, privileged access management (PAM) is a solution that can help mitigate the damage they can wreak inside your network. It is good practice to limit access whenever you can, as the more employees able to access your critical systems and data, the more opportunities there are for a hacker to take advantage of those privileges. It's always worth considering who does and doesn't require privileged access. PAM tools can make this process much easier to manage by giving oversight of all the accounts on your network and limiting the extent and duration of special privileges and helping to keep the most vital parts of your network safe.

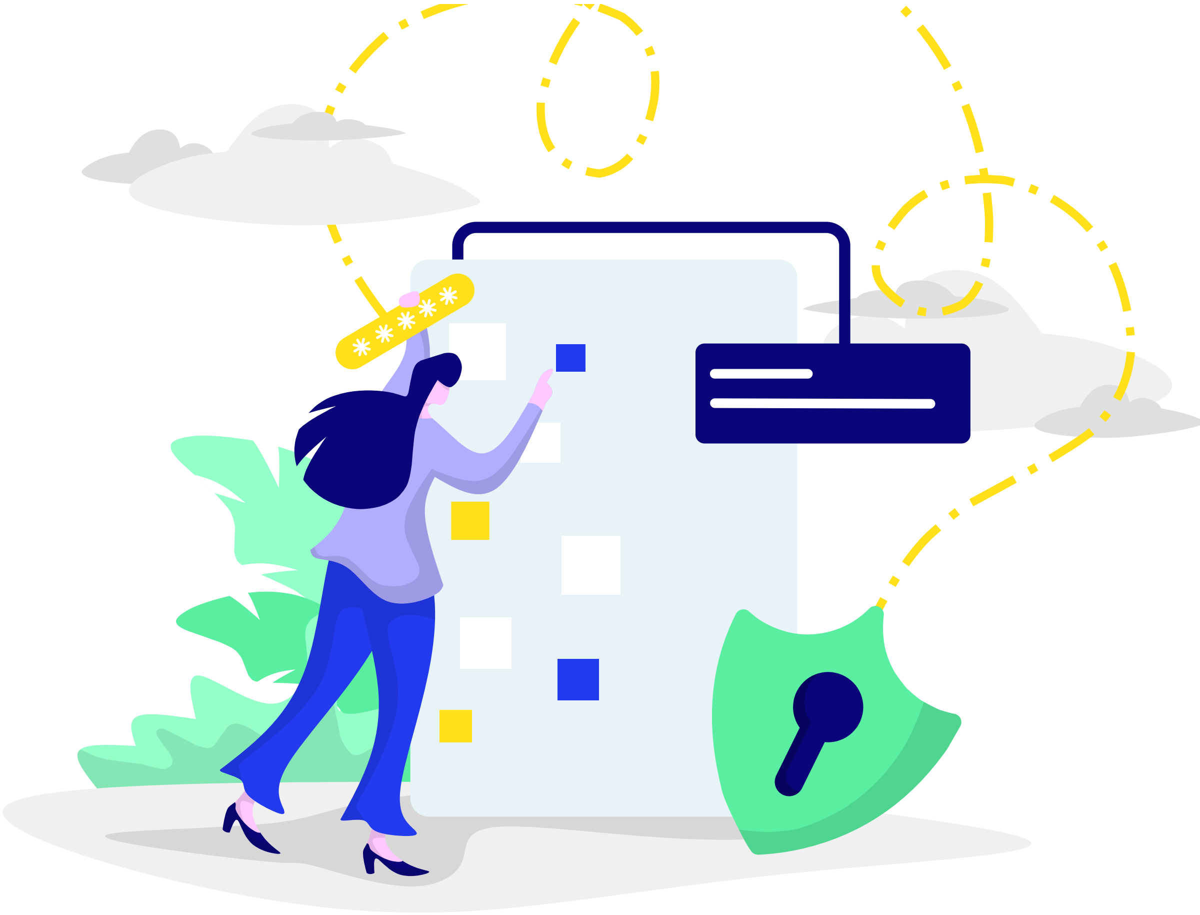
Multi-factor authentication will also help by limiting access your network via compromised employee credentials. Requiring workers to enter a code sent to a verified email address or phone number prevents unauthorised users from accessing the network even if they are in possession of a stolen username and password.

The new dispersed working model has the potential to be a physical security nightmare as well as a digital one. Gone are the days when all business devices were locked up overnight in one building with a security guard stationed at the door. It only takes one successful home burglary or a laptop left on a train to put business hardware in the hands of criminals. Fortunately, "find my device" systems are widely available – such as the show location option available as part of the Sophos Mobile solution – and full disk encryption services like Sophos Device Encryption can prevent malicious actors accessing critical data stored on a hard drive in the case of loss or theft.

There are many security options and services available for your organisation, but it is advised to choose a single centralised solution if possible to avoid leaving gaps in your security or having services working against or disrupting each other. It is also much easier to deploy a single solution. Sophos security services can be operated from one cloud-based portal, enabling oversight of your entire security system, synchronising your defences and also helping maintain compliance. What's more, all the aspects of Sophos work together to create stronger, unified protection for your entire network.

Every situation is different, so assess your company's particular circumstances, vulnerabilities and strengths to determine what you need from your security policy. Cyber security experts can assist you in this and help to tailor a strategy and package that is best suited to your organisation.

A SECURITY-MINDED CULTURE



It isn't only tools and systems that are necessary in the fight against cyber threats. 90% of UK data breaches in 2019 were the result of human error, according to analysis by CybSafe and the Information Commissioner's Office. It's not enough to have the tools to protect your network – you need to foster a business culture that reduces risky behaviour. There is a danger of falling victim to an "out of sight, out of mind" mentality, so it's vital to make sure that you are emphasising the importance of security in the new working model, where employees working from home are more likely to blur the lines between personal and professional – and perhaps forget the key tenets of cyber security.

Cyber security good practice has a habit of being forgotten at the best of times, and in these times of change many workers are likely to require training and reminders of good digital hygiene. Consider regular refresher courses on issues like password safety and phishing awareness, and keep workers informed about new and emerging threats. Encourage your staff to take steps that will help to secure their personal networks and hardware, like changing default home router passwords and ensuring that they have the most secure WiFi encryption – simple steps that they might not have considered but can be walked through with relative ease.

At the same time, it's important to remember that security might not be at the forefront of the minds of stressed employees struggling to get to grips with the changes wrought by 2020. Patience is needed to build a robust security culture, alongside an understanding that workers may be distracted at times. It's important to consider your messaging around security and training, focusing on informing and supporting your staff rather than lecturing, criticising or overwhelming with information and clunky training courses. Little and often is likely to have better long-term effects on security awareness than bombarding them, and empowering them by outlining actions they can take to protect your business is more productive than trying to frighten them with the potential threats you face.

A security-minded culture is something that needs to be built carefully and continually reinforced. Combined with a good awareness of the threats and a robust, cohesive package of security systems and tools, your business will be ready to face the cyber security challenges brought about by our new working models – as well as those that await in the future.