The 2021 Guide to

Hybrid Working Cyber Security

How to keep your business safe from anywhere, on any device

engeneum

Contents

The Move to Hybrid Work

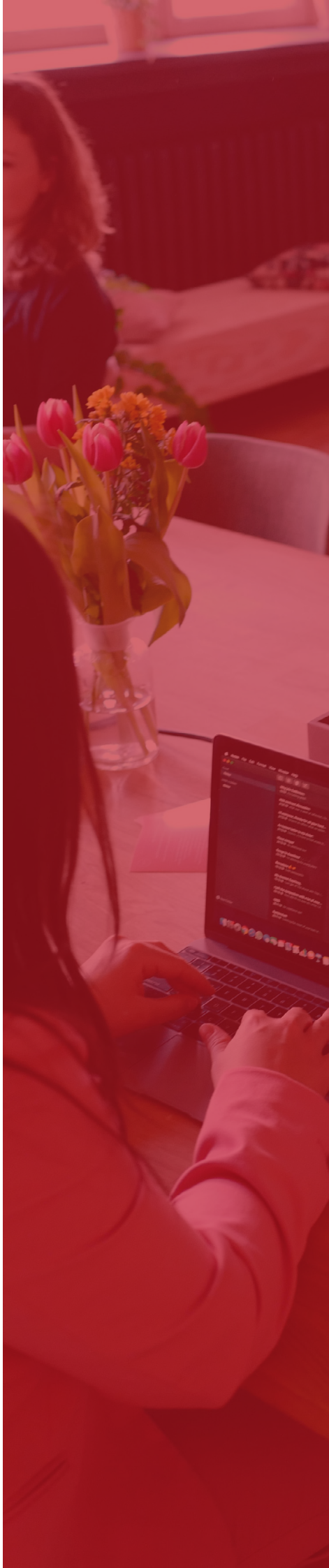
The Future is Hybrid

After months of working from home, restrictions have now eased, and many businesses have implemented a hybrid work model whereby employees work both in the office and remotely. This comes as no surprise as a recent survey found that 47% of employees would be likely to look for another job if their employer failed to offer flexible working arrangements.

Hybrid work has many variations, and employees share differing views on what is the right approach to the new workplace, however, one thing is certain, the future of the modern workplace is hybrid!

47%

of employees would likely look for another job if their employer doesn't offer flexible working arrangements



Benefits of Hybrid Work

Flexibility

One of the key benefits of hybrid working is that it allows greater flexibility for employees. Allowing work from a blend of office and home allows businesses to empower the employee to decide which environment suits them best, while maintaining office-time for easier collaboration and teamwork where required.

Research has shown that employers offering a hybrid working solution see a rise in productivity from their employees and hybrid work models have already been introduced by 63% of high-growth companies. Having this increased flexibility promises to create more productive employees, leading to better business efficiencies.

Better Work-Life Balance

For some, being able to work from home and avoid long commutes into work has made them realise that working in the office 5 days a week led to a poor work/life balance. Conversely, whilst working from home some employees struggled to set clear boundaries between their home life and their work life. Implementing a hybrid work model aims to ensure that regardless of the employee, they will be able to have a healthy work-life balance.

Cost Savings for Employees and Employers

For employees, working in a hybrid arrangement may result in decreased expenditure on fuel from commuting and opens the possibility to move to better value housing as they won't need to commute as often. For employers, hybrid working may allow them to downsize their office spaces and use a hot desk system if not all employees will be working every day.

How COVID-19 and Remote Work Has Affected Security

Ransomware Attacks

Many of most devastating cyberattacks of the past 18 months have been ransomware attacks. Between August 2020 and August 2021, ransomware attacks have increased by 64% year on year. The majority of these attacks have been led by a number of high-profile ransomware gangs. These attacks have shut down gas pipelines in the US, health services in Ireland, and hundreds of smaller businesses in all industries.

The move to remote and hybrid work has been a factor in this massive increase in ransomware. The swift change to working from home meant that many businesses had not appropriately prepared for how to manage security policies when employees were not in the office. Most of these ransomware attacks started from a phishing email, which have also seen an upward trend since the widespread advent of COVID-19 and remote/hybrid working.

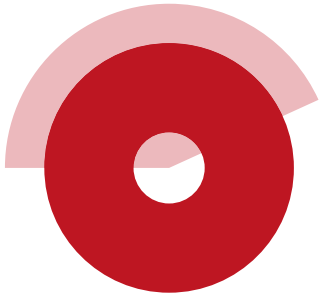
Ransomware attacks have increased 64% year on year

Insider threats

An insider threat is an individual with legitimate access to company's systems and data, that use that access, either maliciously or unintentionally, to cause harm to the organisation. During remote work, insider threats were more common, and often these were unintentional breaches of security policy that lead to other forms of attack. This increase in prevalence was often due to employees having to find work-arounds to get IT systems to function, or from employees lowering their guard in respect to security, as they are no longer working from an office space.

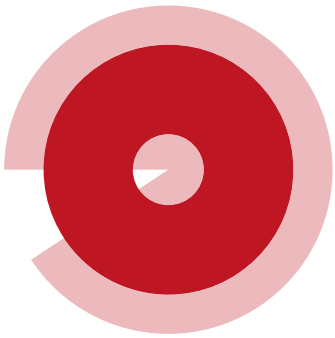
Phishing

In the past 12 months 4 in 10 businesses reported having some form of security incident and from these 83% were phishing attacks. Throughout the pandemic many phishing emails were focused on COVID-19 and remote working, and unfortunately these had a high success rate. These phishing attempts were not confined to email, as throughout 2020 and 2021 there were many SMS phishing attacks around COVID-19, lockdown fines and false COVID-19 benefit payments. These attacks aimed to deceive users into clicking malicious links or files that would lead to data breaches, ransomware attacks or RDP attacks.



40%

of business reported some form of attack in 2021



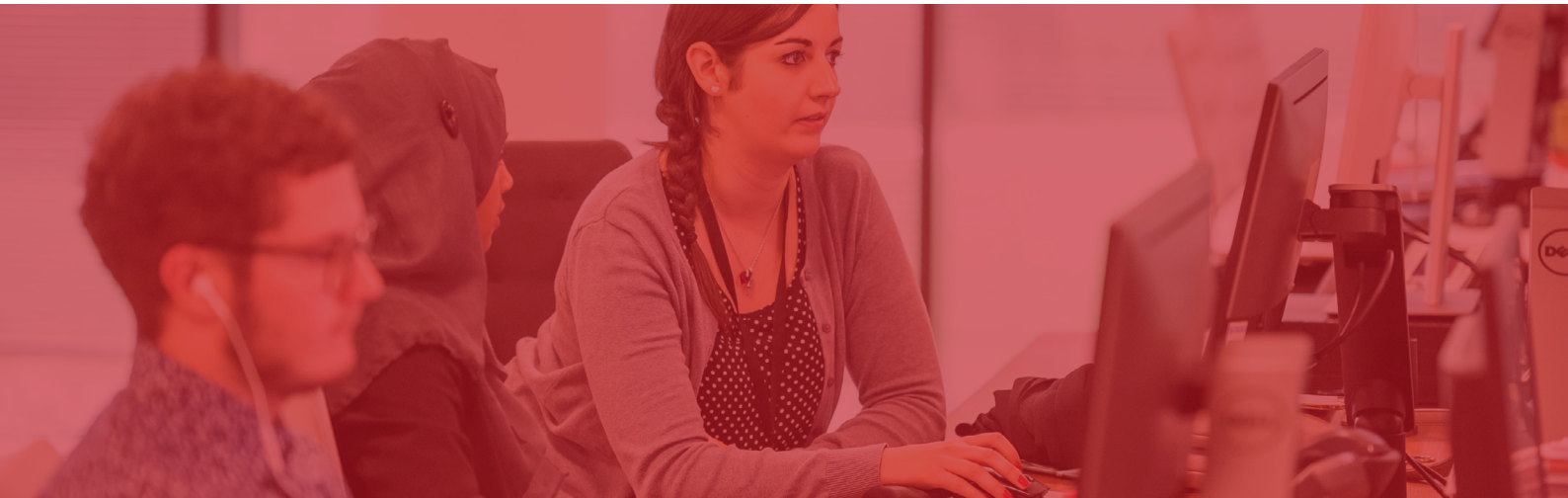
84%

of these attacks were phishing attacks

Business Email Compromise Attacks

Business email compromise attacks are a form of spear phishing whereby the cybercriminal attempts to deceive senior executives into transferring funds or revealing sensitive information. These are social engineering attacks that rely on the cybercriminal to thoroughly research the target and their vendors in order to craft convincing phishing emails.

Throughout remote work, cybercriminals often researched employees within a business, spoofed their email address and sent emails to senior leadership teams in an attempt to steal/gain access to customer data or company funds. This was more prevalent during remote work as it was not an option to check with an employee in person to ensure the email was from them.



The Security Challenges of Hybrid Work

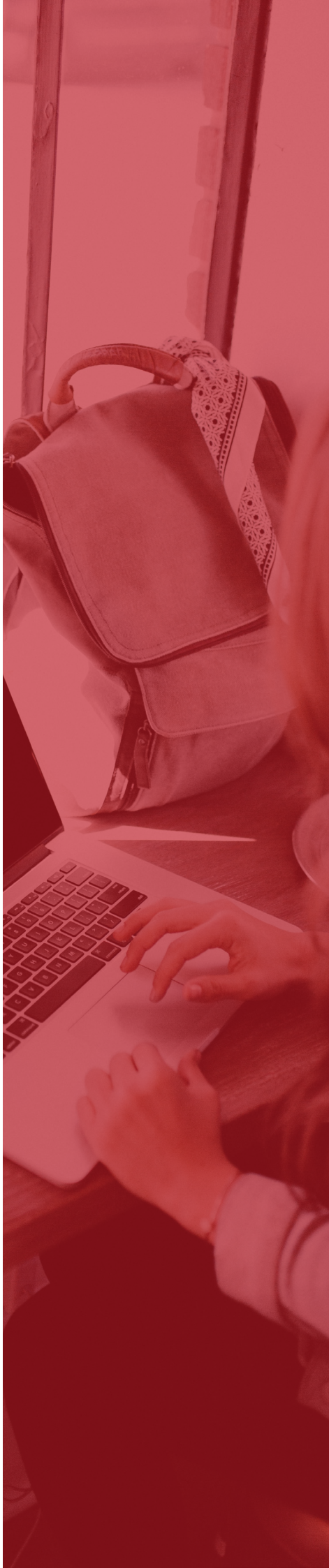
Poor Employee Security Behaviour

If IT systems and the subsequent security policies are not adapted to suit hybrid work, employees will likely create workarounds to combat the shortcomings of the systems. This is evidenced as 36% of employees stated they have picked up poor cybersecurity behaviours and found 'security work-arounds' since working remotely.

A common security issue associated with hybrid and remote working is the unauthorised sharing of data between work devices and home devices. Employees may share this data as they want to print a file, however their work device is not connected to their home printer. This forces employees to take data off a secure system and move it to a potentially unsecure device.

Another security challenge associated with hybrid work is an increase in the amount of shadow IT. Shadow IT is the use of IT hardware or software used by a department or individual without the knowledge of the IT department or IT/security provider. Shadow IT software may include productivity tools or cloud file storage that employees use or install without realising it carries potential security risks.

36% of employee state they have picked up poor security behaviours since remote working



Less Defined Network Boundaries and Poor Home Network Security

Securing a network that spans over an office space, employees' homes, as well as multiple cloud services such as SaaS, IaaS and PaaS is extremely complex in comparison to securing a network that has clear boundaries within an office. Having employees working from home introduces the challenge of ensuring that their home network is secure, to prevent the introduction of malware or spyware from an infected home network.

In the past, a simple way to stop unauthorised access to IT systems was to add geolocation conditional access. This would not allow access to a system if the IP address of the device was not in the same geolocation as the business. This does not work for remote or hybrid work, especially if the employee uses a personal VPN on their home network.

The Risks Involved with Bring Your Own PC

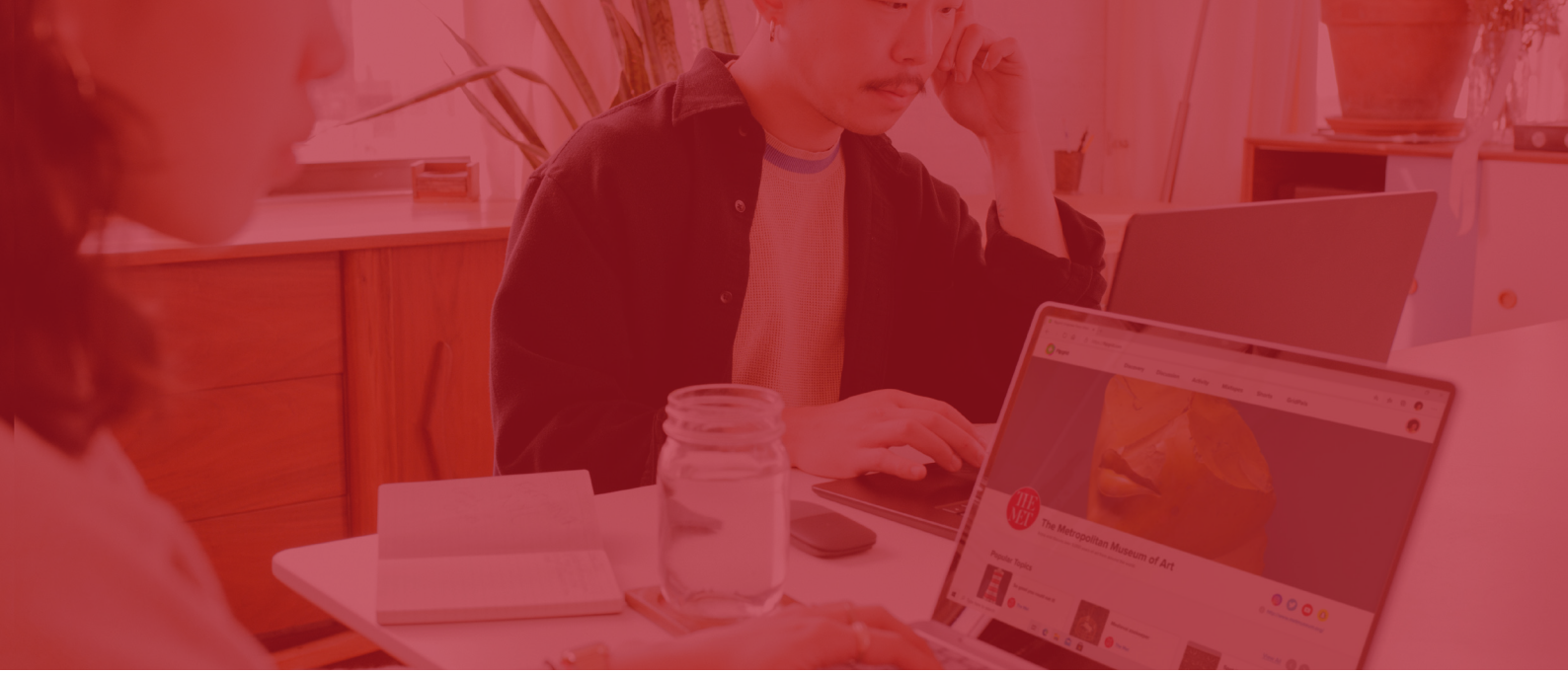
Bring Your Own PC (BYOPC) programmes can be an effective method for a business to reduce overall hardware costs, and a positive experience for employees as they are able to have a single device for both home and work use. It is predicted that by 2022 more than 50% of enterprises will enable a BYOPC programme. This sort of programme is well-suited to hybrid work, however if not correctly implemented it can present a worrying security risk. Employees are more likely to engage in risky security practices whilst using their personal devices, and if there is no separation between the work device and personal device it may lead to a security incident.

By 2022, more than 50% of enterprises will enable an BYOPC programme

Finding the Balance of Flexibility and Security

Securing a business's IT systems and infrastructure is a complex procedure, and hybrid work heightens this complexity. Unfortunately, when businesses improve their security posture it often comes at the cost of flexibility for the employee. As some of the main benefits of hybrid work are increased productivity and flexibility, it is important that businesses do not negate these benefits through difficult security policies and procedures.

The key to a successful hybrid work scheme is ensuring that employee experience is at the forefront of decisions making, and the same is true for improving security posture. It is important to consider the end-user experience and ensure that there is a balance of flexibility and security.



How Businesses Can to Stay Secure Whilst Hybrid Working

Add an Extra Layer of Authentication

Most employees understand the best practices for password hygiene, and it is important to have a long, complex password that has no personal connections to the user. However, cybercriminals have many tools at their disposal to crack a password, including keystroke loggers, brute force attacks and through previous data leaks. If a hacker is able to gain access to an employee's email account, this can act as the launch pad for many other devastating attacks. For this reason, a password should never be the only line of defence. Multifactor authentication (MFA) adds another layer of security that prevents 99.9% of account compromise attacks.

With MFA enabled, when an employee enters their password, they are prompted to provide a second form of identification to login to their account. This may be using an authentication app with passcode or biometrics, or for particularly security-conscious organisations this may be a hardware key. MFA can be easily enabled within a Microsoft 365 subscription to greatly increase security and address some of the challenges involved with having less defined network boundaries whilst hybrid working.

MFA prevents 99.9% of account compromise attacks

Implement Virtual Desktops or Cloud PCs

As mentioned previously, a BYOPC programme is perfectly suited to hybrid work, however it carries significant security risks. One way to mitigate these risks is to implement virtual desktops or cloud PCs. Both of these solutions can be deployed through Microsoft Azure and allow users to access Windows 10 and all necessary applications, from anywhere, on any device. As the security policies are set by the administrator, employees can safely use their own devices without putting the business at risk of a cyberattack.

Microsoft has two virtual desktop solutions, Azure Virtual Desktop (AVD) and the recently released Windows 365.

Azure Virtual Desktop is optimised for flexibility and suits businesses that require full control over the configuration and management of the virtual machines. With AVD it is possible to run multi-session Windows virtual machines, as well as remote app streaming. This is particularly useful when workloads require high levels of compute or are GPU intensive. The pricing for AVD is flexible consumption-based pricing and the level of compute and storage can be optimised for cost and experience.

If AVD is optimised for flexibility, Windows 365 is optimised for simplicity. It is a complete end-to-end Microsoft service with predictable per user, per month pricing. If a business is wanting to deploy cloud PCs, they do not need any VDI experience or skills, and if compute or storage requirements change, it is simple to scale each cloud PC to meet these requirements. Administration and management of cloud PCs is also simpler with Windows 365 as it offers a direct self-service model for the Business edition and one-stop administration in Microsoft Endpoint Manager for the Enterprise edition.

Both solutions provide a secure method of launching a BYOPC programme that can reduce a business's hardware costs whilst providing a better experience for remote or hybrid employees.

Employee Education for a Strong Security Culture

A large component of a strong security culture is employee education and awareness of cybersecurity fundamentals. A business cannot expect employees to report a threat or unsafe behaviour if they do not understand the cybersecurity threat landscape, or best practices. As there are different challenges associated with hybrid work, in comparison to traditional office work, the training and education should reflect this.

When implementing education and training it should be a constant process to ensure employees retain the information and it should be delivered in an engaging manner. The training should include common attack methods and how to recognise them, the potential cost of a data breach or cyberattack, and the policies and procedures to follow if employees believe they have detected an attack attempt or breach of policy. This in itself will not stop all potential attacks, but it provides the foundation of a security culture within an organisation. A strong security culture decreases the risk of a security incident and leads to more involved employees, both in regard to cybersecurity and the wider business.

Identity and Access Management

A core cybersecurity principle is ensuring that only authorised users are able to access IT systems and the information contained in these systems. This is identity and access management, and it includes how individuals are identified in a system and what level of access they have. This should stop cybercriminals gaining access to secure systems and launching an attack or stealing sensitive data.

Many of the security challenges associated with hybrid work can be overcome by introducing zero-trust security concepts. The zero-trust security model assumes that there are malicious actors both inside and outside a network. Therefore, no users or machines are automatically trusted, and all requests must be authenticated and authorised. This verification is based on multiple data points, including user identity, device health, service or workload, classification and anomalies. Another key principle of the zero-trust security model is least-privilege access. This states that users should only be able to access the data they need to do their job, and nothing more.

Least-privilege access greatly reduces the fallout of a data breach, as even if a cybercriminal gains access to an employee's account, they are only able to access a small amount of information. Implementing the zero trust security model within a business is a lengthy process, and it needs to be managed carefully to ensure the balance of flexibility and security is maintained. However, the concepts within the model suit hybrid work as it ensures quality of service and consistent security across all applications and systems.

Conclusion

The move to hybrid work should bring many benefits to businesses and employees with an increase in flexibility and productivity. This new era of work presents some worrying security challenges, and businesses need to address these before it is too late.

An investment of time and money into a comprehensive security solution now, may prevent a costly ransomware attack or data breach in the future.

If you want to find out more about how to protect your business whilst hybrid working, or are interested in technology that can support the move to hybrid work, get in contact with us today.

engeneum

www.engeneum.com

+44 1159 058 523

info@engeneum.com