7 ways to escape a hacker's paradise

Your cybersafe hybrid workplace checklist

BUSINESSICT AUSTRALIA

business **nbn**™
accredited adviser

Hybrid working is one of the biggest shifts to hit workplaces in the past 20 years. While previously only an option for a small number of businesses, it's expected that 35% of Australian companies[1] will maintain a degree of hybrid working post-pandemic.

Hybrid working offers great advantages for business growth, opening up the talent pool to regional areas and improving employee satisfaction.

Despite the many advantages of hybrid work set-ups, businesses face a major security challenge, as the 'surface area' for risk becomes much larger with a distributed workforce.

35% of Australian companies
will maintain a degree
of hybrid working

1 - http://1u0b5867gsn1ez16a1p2vcj1-wpengine.netdna-ssl.com/wp-content/uploads/2021/10/Telstra_HybridWorkingReport_Final.pdf

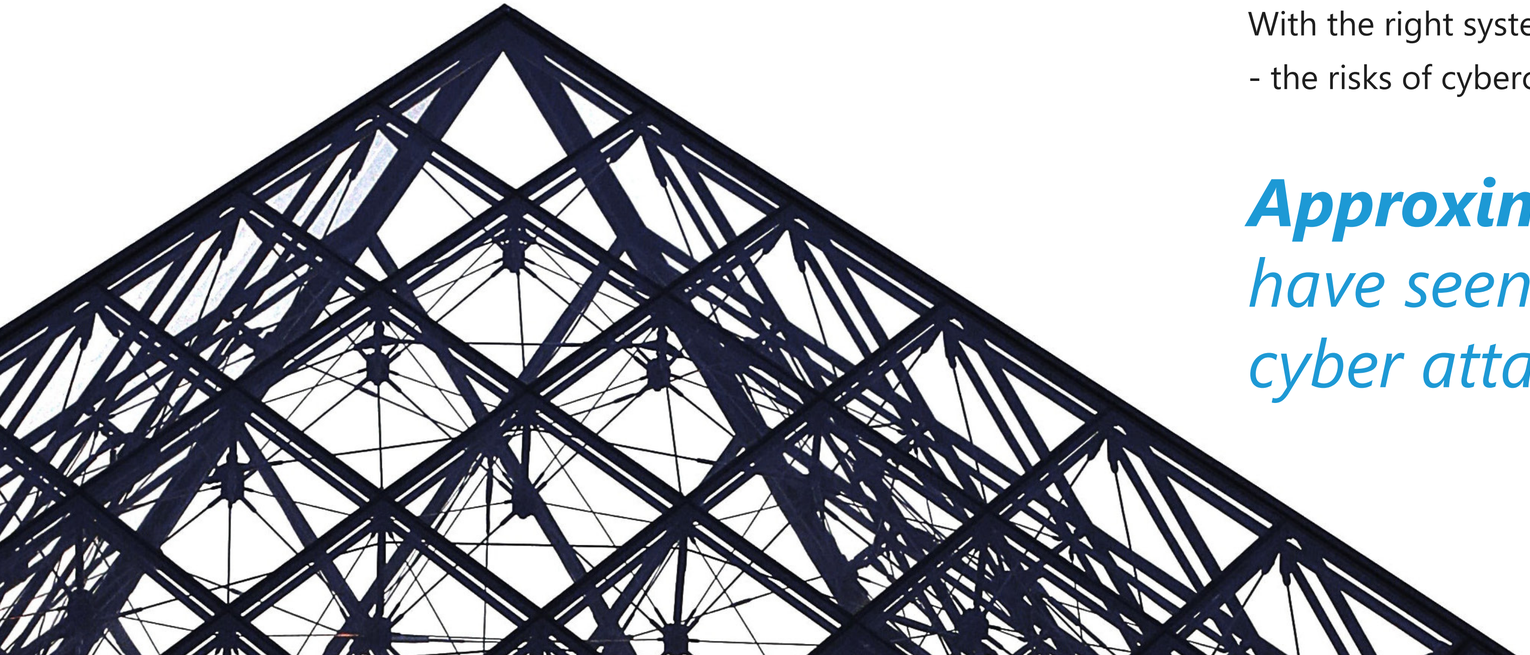
Cybersecurity: the biggest risk to hybrid workplaces

Simply put, without protections in place, remote workers create a hacker's paradise.

A myriad of personal devices, connected by private VPN lines and lacking security can easily become vulnerable to malware, DoS attacks and phishing attempts that compromise the security of the entire organisation. In the 2020-21 financial year, a cyber attack was reported every 8 minutes in Australia[2]. Approximately 30% of organisations have seen a spike in the number of cyber attack attempts since 2020, and this number is expected to rise.

With the right systems in place, however - and an experienced IT provider - the risks of cybercrime can be greatly reduced. Here's how.

Approximately 30% of organisations *have seen a spike in the number of cyber attack attempts since 2020*



2 - https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

Your **seven-step guide** to cyber security in the hybrid workplace

1 Start with a plan

Work with your IT partner to audit your existing security capabilities and map the network of users and devices connecting to your network - remote and in office. Set up a plan to address each vulnerability, as well as a schedule for regular maintenance tasks, such as computer security updates. Review the plan every 6 months.

2 Build cyberawareness

Unfortunately, human error is the leading cause of cyber attacks. Cybersecurity awareness training is essential for all employees, especially when working from home. Cover from understanding what a phishing attempt looks like to teaching them the importance of using 2-factor authentication on all devices. Ideally, training should be conducted when onboarding new employees and refreshed regularly.

3 Manage the endpoints

Endpoint management software, also known as remote monitoring and management services (RSS) help businesses manage and control internet-enabled devices from a single interface. This allows IT administrators to have a centralised view of all endpoints, aiding efficiency by enabling remote working policy updates, security patches and other device management approaches.

4 Adopt a zero-trust security strategy

Zero Trust is a holistic approach to network security. Put simply, where traditional IT network security trusts anyone and anything inside the network - a Zero Trust architecture trusts no one and nothing.

Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

Your network provider should make sure zero trust security is built in from the start when you install business-grade **nbn**™. This may include security strategies such as multifactor authentication when accessing important web apps and data.

5 Avoid ‘shadow IT’

Unsanctioned or unapproved hardware or software, also known as Shadow IT, is a huge cybersecurity risk. Employees have become comfortable downloading and using apps and services from the cloud to assist them in their work, not knowing that cloud apps on personal phones and computers can be a huge security risk. Studies by Gartner have identified that between 30 and 40% of IT spending in large enterprises goes on shadow IT. To combat it? Train staff on the risks of shadow IT and adopt software-defined governance, in the form of specific IT policies.

*30 and 40% of IT spending in large enterprises goes on **shadow IT***

6 Upgrade to fibre internet

Cybercriminals typically take advantage of business vulnerabilities to gain unauthorised access to data. Those vulnerabilities could even include the type of connection you’re using. Fibre internet is not just more secure than traditional copper cable, it’s also less susceptible to interference. Plus, the super-fast speeds of a service like business **nbn**™ Enterprise Ethernet enable more secure cloud storage of sensitive data, in addition to fewer delays and faster access to critical data and systems.

7 Automatic threat detection and live networking monitoring

When a security threat breaches your network, immediate detection can minimise the impact. Take control of the situation with real-time network reporting available on a number of robust and user-friendly reporting platforms like Unifi and Observium, which allow you to see the health and status of your network at a glance. Other innovations like Cisco Meraki can provide you with the tools to allow, block or prioritise traffic on your network.

"Cybercrime, not competitors, may be the **biggest threat to small to medium enterprises in Australia.** Cybercrime costs SMEs time and money, and causes lasting damage to the reputation of a business. It's time to **make cybersecurity a priority.**"

Nick Kennedy

GM - Product & Technology

Business ICT

Talk to Business ICT about how you can **protect your business from the threat of cybercrime** while successfully managing a hybrid working strategy.

Contact Us

1300 988 505

info@businessict.com.au

BUSINESSICT AUSTRALIA

business **nbn**™
accredited adviser