3 CYBERSECURITY MISTAKES BUSINESSES ARE MAKING DURING COVID-19

huonit
A KYOCERA GROUP COMPANY

Many organisations successfully shifted to a sudden work-from-home arrangement when COVID-19 struck. This change saw new technology adopted at unprecedented speeds, and thankfully allowed many organisations to survive and keep their staff in employment.

However, in that rush, what new cybersecurity vulnerabilities were created?

Working away from a secure, private office network opens the door to many cyber risks. Even as offices re-open as COVID-19 restrictions are lifted, the ‘new normal’ will likely be a combination of office and home based arrangements.

These risks are here to stay, and it is now more important than ever to assess your security posture.

In this article, we explore the three most common security risks of a dispersed workforce, and recommend best practice solutions to ensure your business data remains safe.

1 SENSITIVE DATA OUTSIDE OF THE CORPORATE DOMAIN

Keeping company information in centralised, managed and secure repositories is key to any solid data management strategy. However in many cases, the sudden pivot to working from home has led to a loosening of these policies.

IT may have had to relax remote access configuration policies, such as allowing quick access to enterprise applications. If any such changes were made during the transition, a full review of all configurations should be conducted with urgency to mitigate those risks.

And from the users’ perspective, they may be using “workarounds” to get by from home. For instance if your company doesn't have easy and accessible filing & document sharing tools, then they may develop bad habits such saving copies locally, or using convenient (yet unapproved) methods of file sharing, e.g. Dropbox. This can even occur during web conferences (such as Zoom) where content is shared or discussed during unsecure calls.

Both of these scenarios could mean a serious lack of management control over data., putting your business at risk of cyber attack and in potential breach of data privacy laws.

Ensure systems are in place where copies of files are not permitted to be saved elsewhere, and must remain in your company's approved systems – either company cloud repositories (e.g. OneDrive) or document management systems, such as SharePoint or iManage. File sharing methods must also be secure and traceable by IT.

2 UNMANAGED DEVICES & OUTDATED SECURITY POLICIES

In order to provide staff with rapid remote access, many companies pulled together a combination of existing workstations, new laptops, and sometimes even relied on employees using their personal devices.

In too many cases however, not all were set up in line with best practice management in mind, meaning that company data is now located on unprotected, uncontrolled and unmonitored devices.

Connection methods can also be a risk, if staff are operating on Wi-Fi without a password, or connecting to VPN or other systems without security controls such as multi-factor authentication (MFA). VPN and remote services are currently primary targets for hackers, and many companies have not put enough emphasis on properly securing them.

Ensure that IT policies are reviewed holistically, with new emphasis on remote working to cater for new and BYO devices, and that best practice security features such as MFA and identity access management controls are in place to maximise control of company data.

3 INCREASED VOLUME OF PHISHING ATTACKS & ONLINE SCAMS

In addition to the plethora of online scams regularly hitting inboxes, hackers are now also preying on COVID-19 fears - posing as health or government officials, or even internal IT department or senior staff members - to steal personal information or gain access to company data.

Even with the most secure backend IT systems in place, staff remain a key point of vulnerability. In addition to industry leading email-filtering solutions to reduce the likelihood of such emails actually reaching your staff, it is also imperative to educate all users on how to recognise and deal with a scam.

Regular education via online training tools and simulated phishing tests helps to raise this awareness, and all companies should have an official process to report suspicious messages.

LEARN MORE

If you need help reviewing or securing your remote office environment, read about our Cybersecurity Portfolio of services, or get in touch with our team.

T: 1300 HUON IT (4866 48)
E: info@huonit.com.au
www.huonit.com.au

huonit
A KYOCERA GROUP COMPANY