WORKING IN PARTNERSHIP WITH Paradigm CONSULTING

MITIGO CYBERSECURITY

HOW TO REDUCE YOUR EXPOSURE TO CYBERATTACKS AS A RESULT OF REMOTE/HOME WORKING

Remote working is helping to get control of the coronavirus emergency and mitigate the economic impact to business. However, without exception, we find that remote working is one of the top three critical vulnerabilities which can result in a serious cyber incident. There are a lot of things to consider and guidance will vary by business, but the following is our advice to proportionately reduce this risk of a cyber breach.

Cyber vigilance increased.

Staff behave differently in a home-based environment and cybercriminals are actively creating new attacks to exploit the change in business arrangements.

1. Acceptable use of a company laptop – business and personal life should not be blended. The starting position should be work use only.
2. Unattended machines – be conscious of who can see your work and lock your machine when unattended. Set auto lock to max 5 mins.
3. Phishing attacks – increased vigilance is vital especially as fraudulent emails and infected videos, related to coronavirus, are already proliferating.

Tip – Staff should re-do cyber training and tests when they start remote working. A simulated attack may be appropriate for a prolonged period of home working.

Effective controls maintained.

Important technical controls which are run centrally in the office network environment do not operate when working away from the office network. They simply fall into disrepair. It is important to get work laptops properly set-up otherwise they will become increasingly vulnerable.

1. Anti-virus – make sure that the application is up to date and configured to proactively scan device, attachments and downloads. You should consider upgrading to a version with a cloud portal so that control and alerts can be maintained centrally.
2. Operating systems (Windows or Mac typically) – this is usually centrally managed when connected to the office network, but remote working prevents this. Machines need to be reconfigured to update independently, and staff shown what role they must play in that update.
3. Back-up – this will vary hugely by business setup. Seek advice on the new configuration setup required.

Tip – a periodic check on a sample of devices, to check these three controls are working, is a simple way to get some comfort in this area.

Defensive configuration reviewed.

The change in working arrangements requires a change in the configuration of the laptop's defences. So, the machine settings on remote devices will need new configuration.

1. Encryption (e.g. BitLocker) – needs to be enabled, without exception, to protect in the instance of a lost machine.
2. Local admin – make sure any local admin rights have been removed from the user's profile.
3. Wi-Fi – laptops should be configured only to allow secure wi-fi connections.

Tip – Seek appropriate advice on the changes required to keep all devices safe. Please make sure you think carefully about where to keep the encryption recovery keys.

Remote connection secured.

This can go horribly wrong if done incorrectly. Our advice will vary dramatically depending on your business processes, your IT set-up and the third-party software you rely on. If in doubt, please seek support.

1. Update the remote connection software – services need to be brought up to the latest version to ensure they are patched against known cyber vulnerabilities.
2. Don't allow personal devices. Where at all possible remote machines should be work devices, configured to the points above. Seek advice before connecting home and personal computers to your secure network.
3. Strong authentication – enable these settings on the cloud applications you use. E.g. MFA on Office 365, 2 step verification on G suite. Most of the applications, where you log on via a web page, should have something that is stronger than just relying on a password.

Tip – if you must rely on a password make sure it is strong and unique (not shared or reused), oh and don't store it in plain sight.

We really hope this has proved useful and please be in contact if you need help.

Stay safe with our best wishes.

Mitigo team