SURA PROFESSIONAL RISKS

Managing a remote workforce?

Protect your employees and your business from cybersecurity risk

More than ever before in these unprecedented times; companies of all sizes are enabling their employees to work remotely. Unfortunately, some organisations are not fully prepared for this sudden change to remote working which can potentially put the company at an increased risk of a cyberattack.

Many companies offer remote working and have company-owned and managed devices and robust security defences to protect remote access. Until recently, some smaller organisations might have thought that they did not need – or lacked the opportunity – to develop this type of infrastructure. This does not have to be the case: businesses of every size can take proactive steps to enhance their information security immediately.

Protect your business

For businesses of all sizes, we recommend these basic steps to help ensure your transition to remote working goes as smoothly as possible:

- Ideally, employees working remotely should use only company-issued or approved devices to securely access company resources. If employees generate business records on their personal devices and outside the company's control, it may not only lessen their security but also complicate your company's compliance functions, privacy legislation, trade secret protection, non-disclosure agreements, record retention policies, and legal process, among other things.
- For company devices, consider prohibiting personal email or other non-business use.
- All devices should be equipped with up-to-date anti-virus and anti-malware solutions, and follow regular software updates and security patch schedules.
- All data should be encrypted, whether in transit or at rest. Since remote workers may be operating on less secure networks at home or on the road, implementing a virtual private network (VPN) with multi-factor authentication protects these connections.
- If personal devices are used for business purposes, consider ways to educate and require employees to strengthen their security settings and firewall configuration. For example, require strong passwords, preferably 8-20 characters with combinations of capital and lower case letters, numbers and special characters. You may also consider a password manager solution.

Best practice cyber tips for employees overleaf

Protect your employees

Employees also need to be vigilant and follow best practices when remote working. These guidelines may help protect data confidentiality:

- When working from home, individuals should exercise responsibility for their own personal electronic hardware like Wi-Fi routers, cable modems, printers, scanners, and portable devices. A backdoor into their home network may be a backdoor into the company network. Consider asking them to follow your company guidelines (or, if your company does not want to undertake to issue such guidelines, then their devices' manufacturers' guidelines) for keeping their software and firmware up to date, for using strong passwords and security settings, and for patching device operating systems regularly.
- Employees should keep electronic work files on company systems or on company-issued hardware, and not on their personal devices.
- Don't leave sensitive information in plain view – on paper or onscreen.
- Make sure your device has a lockout feature after a short period of inactivity.
- Shred all paper containing sensitive information once it's no longer needed.
- Use care before clicking on links or attachments in emails. Even if the sender looks legitimate, when in doubt utilise "out of band verification", call the sender from a known good phone number to verify the messages authenticity.
- If you receive a phone call or email asking for your personal or financial information, do not share.
- Never share any user ID or password.
- Verify any charity or community group's authenticity before making a donation.

The ultimate goals of information security are confidentiality, integrity and availability – ensuring that remote communications are private and unaltered, and resources are available when needed. By following these guidelines, you can help move your organisation towards achieving those goals and creating a safer, more functional remote working environment – helping your organisation stay connected.

To talk to an underwriter about insurance for your technology clients, to include cyber coverages, please contact Paul Brown on 0438 729 886 or Estelle Smith on 0407 334 679 for a friendly chat.

SURA PROFESSIONAL RISKS

Sydney
Level 14/141 Walker Street North Sydney NSW 2060
P O Box 1813 North Sydney NSW 2059
Telephone. 02 9930 9500

Melbourne
Level 9, 99 william Street Melbourne Vic 3000
GPO Box 1281 Melbourne Vic 3001
Telephone. 03 8823 9400

sura.com.au/professional-risks