Risks for the remote organisation

COVID-19 has made remote working a critical capability, but there are some important risks for technology teams to consider across the themes of resiliency, security, third party and people. These risks are important now and also in the future, as many organisations rely on remote working as a continuity strategy for many scenarios where office facilities are unavailable.

Resiliency Risks

Inadequate access to equipment and systems

Organisations should investigate whether there are enough laptops (and peripherals) to be distributed to desktop workers or whether relocating the desktop computers to their homes is viable. Having a reserve for replacement equipment also ensures flexibility in the event of technical failure. Software licenses and compute capacity are also necessary. Relevant systems to consider include Virtual Private Networks (VPN) and corporate file shares (e.g. SharePoint) and productivity suites (e.g. Office 365).

Insufficient network and bandwidth

Enough data volume and bandwidth are required to access systems and applications remotely, including both for data centres and homes. Household internet plans may often fall short for corporate use, especially considering that multiple members in a household may be required to work from home on the same data plan. That goes for both bandwidth and data caps required to keep staff connected (e.g. via video conferencing).

Considerations:

- Monitor hardware stock levels;
- Higher capacity, datacentre bandwidth and software licence compliance monitoring;
- Optimise VPN routing, and bypass VPN for some activities (e.g. video conferencing);
- Save by downgrading office internet plans;
- Revise internal expense policy to provision for upgraded staff internet plans

Security Risks

Improper technology configuration

Sudden transition into remote working often means less time has been spent considering secure configuration of solutions. Seemingly harmless but publicly accessible tools pave way for opportunistic hijacking and compromise of company assets and time. A simple example recently has been with 'Zoombombing', whereby malicious actors hijack Zoom meeting rooms to screenshare extremely graphic and inappropriate content. Beyond just disrupting meetings, viruses and malware can also easily be sent through the default file-sharing functionality.

The ACSC has recommended these controls to consider for secure web conferencing.

Unsafe ad-hoc workarounds

Hindrance to business-as-usual (BAU) tasks often tempt the desperate worker with 'creative' solutions. When corporate devices are unavailable or unusable, staff may send work to personal emails and even print documents as a workaround. They may also attempt to use unapproved and insecure cloud tools to collaborate on work. Not only is there a risk this could fall into the wrong hands, but what happens when staff no longer needs the data, for example when employment ceases?

Insecure home environments

The physical threat of malicious actors is underestimated, as we consider the differing security standards in homes compared to office buildings. Although it may seem extreme to accuse family members of being malicious, there will be workers who share their common living with non-family members. Taking confidential phone calls in earshot of curious neighbours, leaving sensitive documents displayed on-screen or on the dining table, leaving company assets and devices vulnerable to household theft, and unsecured home Wi-Fi networks all pose unique risks not otherwise experienced in a secure office environment.

Considerations:

- Retrospective security reviews of implemented technologies;
- Heightened monitoring of controls to detect data leakage and unsanctioned cloud use;
- Provide working from home security training and guidance to staff over multiple channels (e.g. team meetings, e-mail etc).

Third Party Risks

Reduced availability of outsourced/offshore services

The ability for suppliers to provide immediate BAU support becomes difficult when remote working infrastructure varies across organisations and borders. Offshore call centre and helpdesk staff may not have adequate home office capabilities and with an increase in helpdesk demands, delays are likely. This may also be the case for local hardware support, where troubleshooting and replacing equipment become challenging and require couriers or travel to homes.

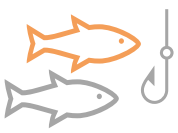
In a remote working environment, suppliers have become more critical and more at risk of supply chain disruption.

Stretched capacity among key software suppliers

As a large proportion of businesses are serviced by a concentration of key suppliers, there is a risk of undersupply. As organisations have shifted to remote working, we've seen a shortage of hardware peripherals such as laptops, webcams and monitors and a significant increase in the use of collaboration tools such as Zoom and Microsoft Teams. In a remote working environment, these suppliers have become more critical and more at risk of supply chain disruption.

Considerations:

- Exploit self-service IT capabilities wherever possible to ease demand, such as self-service password resets, how-to guides etc.
- Review and update supplier contingency plans, with consideration to having redundant agreements with key suppliers for hardware, telephony, support etc.



Since the outbreak, ACCC's Scamwatch has received over a thousand coronavirus related scam reports. These include phishing, online and superannuation scams. Stay updated to stay safe.

People Risk

Key personnel risk

Key personnel risk is a reality for critical IT support and vendors, employees and clients. Along with the spread of COVID-19, Australia is heading into winter and the flu season, which may potentially affect the health and wellbeing of the population. Key individuals being unavailable may lead to delays in projects, troubleshooting of IT issues, as well as put a burden on existing teams.

Low team morale and poor mental health

IT teams may be feeling pressure due to several facets - job security, health concerns, and the uncertainty of when life will revert to 'normality'. Stress associated with adapting to a new way of working and considerable technology change is also likely. The combination of all these factors, as well as prolonged lack of in person connectivity, could possibly have detrimental impacts on mental health.

Considerations:

- Revisit the people aspects of business continuity plans. Identify key person dependencies and ensure critical teams are cross-skilling;
- A split team approach that alternates who needs to physically be in the office;
- Take actions that foster a culture of resilience and wellness. Consult Safe Work Australia for information specific to COVID-19.

Andrew Millward
Director
amillward@amstelveen.com

Romana Bizjak
Senior Manager
rbizjak@amstelveen.com

Obed Oei
Manager
ooei@amstelveen.com

Hima Raj
Senior Consultant
hraj@amstelveen.com

Amstelveen

Amstelveen's team of professionals work on major technology and business change projects, and enhance capability in risk management, internal audit and corporate governance functions. We provide specialist support to the largest public and private organisations in Australia and New Zealand.