COVID-19: CYBERSECURITY CHECKLIST FOR REMOTE WORKING

Written by Kelly Butler 21 April 2020

The COVID-19 pandemic has created an abrupt and unforeseen need for entire workforces to be moved out of regular offices or facilities and into virtual environments. For many Councils, a shift of this magnitude would normally require long-term IT transformation efforts. Due to the pandemic's speed, however, many IT departments have come to appreciate the military adage: "You must fight with the army you have."

At the moment, there is no time for Councils to create the armies they need. While many Local Governments are now reconfiguring networks and systems to serve the needs of remote workforces, the success of these transformations is often being limited by less-than-optimal technology capabilities.

While your IT infrastructure may be stressed by a significant increase in demand, cyber threat actors are actively seeking to exploit weaknesses that may exist in your newly implemented or temporary IT infrastructures. Below are some recommended steps, considerations, and tips to help protect your Council from malicious cyber threats.

Note that this is an inclusive, but not exhaustive, list of recommendations.

RISK AND GOVERNANCE

- Update and communicate acceptable use policies for employees and address the use of home computing devices.
- Identify functions requiring secure IT environments that remote working may not provide, and develop ways of performing them.
- Anticipate how entities on which your Council depends – cloud, network infrastructure providers, and others – may be affected by COVID-19 disruptions, and develop resiliency options.
- Refresh and update cyber incident response and disaster recovery plans to address current operational needs.
- Regularly communicate cybersecurity awareness messages to employees to reinforce security procedures.

IT INFRASTRUCTURE

- Provide secure access solutions with sufficient capacity for the increased number of remote users.
- Offer security protection on endpoints.
- Enforce software updates to remote workers.
- Reassess rules such as geo-blocking that could prevent remote access.
- Increase IT help desk capacity and hours of operation to handle the increase in services required by remote workers.

CYBER OPERATIONS

- Ensure that cybersecurity alerts and audit logs of critical systems – for example, VPNs, firewalls, endpoint security tools, and critical applications – are centrally collected and analysed to detect and respond to suspicious/malicious activity.
- Review/update VPN profiles and firewall rules to ensure employees are assigned appropriate privileges based on their roles.
- Implement procedures requiring approval from data/ system owners for provisioning and de-provisioning of remote VPN and other accounts related to critical business applications.
- Enable multi-factor authentication for VPN and critical information systems.
- Disable split tunneling for VPN profiles to ensure that remote employees cannot access the internet directly from their laptops while using VPNs to access corporate information systems.
- Create a shared channel – for example, #phishing-attacks – or email address where employees can report suspicious emails.

ADVICE FOR YOUR EMPLOYEES

Develop tailored cybersecurity awareness messaging for remote workers and deliver it online to all employees. Include topics such as:

- Detecting and avoiding elevated phishing threats, including COVID-19 scams and fraudulent websites.
- Ensuring secure use of Wi-Fi, both at home and in public.
- Not using Council computers for personal email, file sharing sites, or social media without approval.
- Saving and securing needed printouts of work files or emails and shredding others.
- Not copying work files or information to personal devices, including home network drives and personal online storage.
- Muting or shutting down in-home digital assistants that may continuously record nearby conversations.
- Not permitting family members or others to use Council-provided equipment, including laptops and phones.
- Eliminating default home Wi-Fi router passwords and performing other home security checks.
- Confirming screen locks are enabled to ensure workstations are secured when not in use.
- Never leaving laptops and mobile devices unattended in public spaces or unlocked at home.
- Using Council-approved cloud services or data center storage instead of local storage, particularly for sensitive information such as personally identifiable information, protected health information, financial data, and trade secrets.
- Avoiding the use of USB sticks and other removable storage.

Although the COVID-19 pandemic has created enormous and swift changes, Councils cannot ignore the cyber challenges associated with a largely or entirely remote workforce. The recommendations above related to risk and governance, IT infrastructure, operations, and employee education can help Councils work more securely and efficiently through these challenging times. In the long run, changes made in response to the pandemic should ultimately be viewed through a resiliency lens, with an eye on building to more flexible and secure future states.

KELLY BUTLER
Cyber Leader – Marsh Pacific

The information in this document is general in nature and is not intended to be relied upon as advice regarding any individual situation and should not be relied upon as such.

This information is based on sources we believe to be reliable but we make no representation or warranty as to its accuracy.