MARSH

Cyber Checklist for Continuing Care Clients

Aged Care, Disability Care and other care environments have been particularly susceptible to cyber attacks. To help you be prepared, our cyber team has developed a check list aiming to minimise any cyber exposures, keep your employees up to date on cyber risks and identify areas of weakness.

Please note: The checklist should be reviewed in conjunction with the personnel responsible for managing the IT infrastructure of the organisation eg the CTO as it uses IT-specific language.

Risk and Governance

- [ ] Update and communicate acceptable use policies for employees.
- [ ] Identify functions requiring secure IT environments.
- [ ] Anticipate how entities on which your business 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.
- [ ] Review your BYOD policy for an appropriate employee exit action.
- [ ] Consider Behaviour Detection training for Managers and Supervisors.

IT Infrastructure

- [ ] Offer security protection on endpoints.
- [ ] 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.

Cyber Operations

- [ ] Ensure that cybersecurity alerts and audit logs of critical systems — for example, VPNs, firewalls, endpoint security tools, and critical business 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 tunnelling 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 company 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.
- [ ] Confirming screen locks are enabled to ensure workstations are secured when not in use.
- [ ] Never leaving laptops and mobile devices unattended in public spaces.
- [ ] Using company-approved cloud services or data centre 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.