GoWest
GO BOLDLY.

THE CYBER RISK CHECKLIST

10 Cyber Risk Mitigation Tasks for Small + Medium Sized Businesses

Most small and medium sized businesses struggle to adequately mitigate cyber risk. Act today by following the steps below to protect your business. Each step you take will reduce the likelihood that your business is the victim of a cyber-attack.

01

❑ **Harden your email platform.**

- » Validate all active users. Eliminate accounts for separated employees.
- » Limit the number of admin users and make sure that administrators use separate and unique credentials to administer your email hosting platform.
- » Implement multi-factor authentication (MFA) for 100% of users, starting with Admin users. No excuses! This is an absolutely necessity.
- » Review existing mail forwarding rules and block the addition of any new mail forwarding rules without management approval (criminals use forwarding rules to exfiltrate mailbox data and perpetrate financial crimes).

02

❑ **Install good business class (not free) antivirus and antimalware software on 100% of servers and workstations.**

- » Make sure it configured to routinely update definitions and that virus scans are conducted on a routine basis.
- » Make sure a qualified technical resource is timely reviewing antivirus alerts and notifications for all systems on a regular basis.

03

❑ **Identify where your business critical and sensitive data resides (workstations, servers, cloud storage, email…) and implement a business class backup solution.** Recovery from backup is the ONLY way to recover from a ransomware attack without paying the ransom.

04

❑ **Get control of your endpoint hardware (workstations, servers, firewalls).**

» Inventory all the systems that are used to store, manage, and access your systems and data.

» Patch your hardware and software. Workstation and server operating systems should be patched no less frequently than monthly. Third party software (Microsoft Office, Adobe, browsers, Java…) should be patched no less frequently than monthly. Firewall firmware should be updated no less frequently than quarterly. Hypervisors and network appliance (switches, NAS devices, wireless access points…) firmware should be updated no less frequently than annually.

05

❑ **Conduct routine phishing testing of your people.** Determine who needs training to prevent falling victim to a phishing attack, the most common and effective cyberattack vector.

06

❑ **Conduct routine and ongoing user awareness training to reduce the risk of social engineering attacks, including phishing.**

07

❑ **Implement a solid password management platform.** It should provide your users a safe place to store credentials and promote good credential hygiene (long, strong, and unique passwords).

08

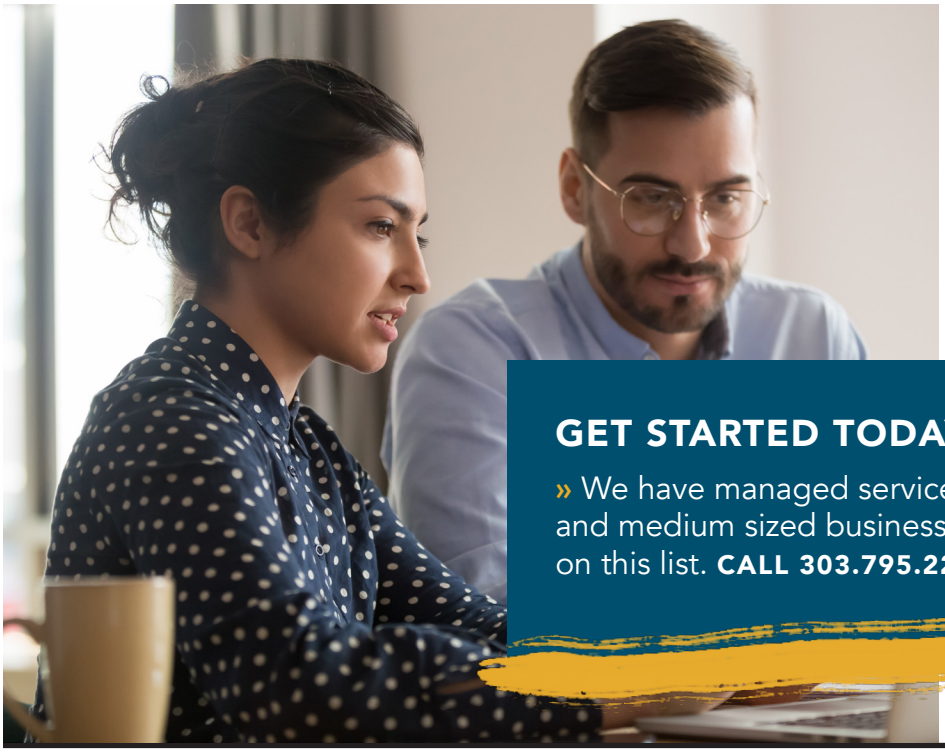
❑ **Remove local administration rights where possible and encrypt workstations.**

09

❑ **Conduct regular health and security assessments of your email hosting platform.**

10

❑ **Conduct regular Information Technology business reviews and assessments.** Evaluate the operational effectiveness, health, and security of your information technology infrastructure.



GET STARTED TODAY

» We have managed service solutions tailored for small and medium sized businesses to address 100% of the tasks on this list. **CALL 303.795.2200 TO BEGIN.**