GoWest TOP TEN

tasks to mitigate cyber risk 2018

1 Identify where your data resides

and how it is accessed. Capture all locations including servers, PCs, laptops, mobile devices, web applications, cloud services, and personal devices.

2 Backup your data, period

Ensure that backups for valuable and sensitive information reside in secure, redundant storage. Restoring from backup is the **ONLY** way to recover from a ransomware attack.

3 Defend your perimeter

Use a Unified Threat Management appliance from a reputable vendor, lock down application access controls, encrypt your WiFi and control who can use it

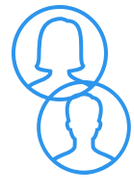
4 Implement malware and virus protection

for email, gateways, and endpoints (PCs, laptops, tablets).

5 Harden your email platform

Disable unnecessary and potentially vulnerable "features", configure security controls, employ anti-spoofing technology, and routinely review user access.

6 Implement user access and account management controls



Eliminate shared accounts. Enforce strong, unique passwords. Use SSO (Single Sign On) and multi-factor authentication wherever possible. Define controls for your admin-level accounts, and review regularly.

7 Train your users

Do not assume they know how to recognize a social engineering attack. Teach them to identify phishing attempts, and test them regularly to determine where additional training is required.

8 Maintain a thorough hardware and software inventory

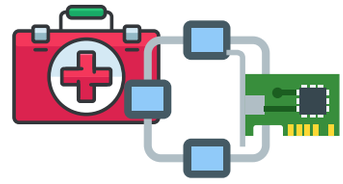
Eliminate unnecessary hardware and software to reduce your vulnerability footprint.

9 Routinely patch hardware and software

Including operating systems, line of business applications, firmware, and third party applications (Adobe, Java, Flash...)

10 Conduct routine health checks

Conduct regular vulnerability scanning and remediation. Routinely assess risks.



Go West IT, Inc. *info@gowestit.com* **303-795-2200**