IS YOUR BUSINESS PROTECTED FROM CYBERATTACKS?

Manawa Cybersecurity Scorecard Grades Your Potential Risk in Seven Critical Areas
Find out where your business may be most vulnerable to cyberthreats
— whether it's the network, email, web, or employee education —
and then prioritize the activities that can mitigate your risk.

manawa

www.manawa.ca

CYBERSECURITY SCORECARE

To find your Manawa Cybersecurity Score, place a check next to the questions you can answer in the affirmative. Each checkmark is worth four points, for a maximum score of 100. A score below 80 indicates a need for improved security.

SCORE 0

EMPLOYEE TRAINING & POLICIES

- ☐ Do you hold regular employee training that covers the latest in cybersecurity?
- ☐ Does your IT Team/MSP actively test your employees to identify cyber hygiene gaps via phishing simulations?
- ☐ Do you have a well-documented Acceptable Use policy (including Internet access, passwords, email, passwords, devices, and remote work)?

DATA SECURITY

- ☐ Do you perform regular backups of data and configurations, as well as test restore?
- ☐ Do you have a formal policy for disaster recovery?

EMAIL SECURITY

- ☐ Do you have an email security filtering solution that protects against malicious emails landing in your inbox?
- ☐ Do you have a formal policy that bars employees from sending sensitive data (such as passwords and financial information) by email?

WEBSITE SECURITY

- ☐ Is your website's SSL certificate up to date?
- ☐ Does your website hosting plan include regular site updates? Is your website hosted on a secure server?

END POINT SECURITY

- ☐ If your organization was hit by malware, would your IT Team/MSP be able to identify the threat within hours? (This includes off hours such holidays and in the middle of the night.)
- ☐ Would your IT Team/MSP be able to identify the root cause, or what is known as the initial point of compromise (IOC)?

NETWORK SECURITY

- ☐ Do you use up-to-date software and regularly apply security patches?
- ☐ Are your firewalls next generation devices covered under a support agreement and running the latest firmware with UTM features like Anti-Malware and Intrusion Detection enabled?
- ☐ Do you regularly scan your network for vulnerabilities, such as malware and unauthorized devices?
- ☐ Do you password-protect your router and make internal Wi-Fi accessible to employees only? (Configure guest networks separately.)
- ☐ Do you use a VPN (virtual private network) for remote access? Is Multi-factor Authentication used for remote connections such as VPN and RDP?
- ☐ Are work devices set up to automatically lock the screen and require logging back in after a period of inactivity?
- ☐ Do you limit and log access to the physical locations or rooms containing network devices (such as switches) and any in-house servers?
- ☐ Do you store data securely in cloud software, using password best practices for accessing this data?
- ☐ Are your external ports actively reviewed, monitored, and alerted on?
- ☐ Is Multi-Factor Authentication used for cloud environments such as O365, Azure, or AWS?

USER SECURITY

- ☐ Do you require employees to use complex passwords and update them regularly?
- ☐ Do you audit and disable outdated accounts?
- ☐ Do you avoid shared accounts and passwords?
- ☐ Do employees know to check that all websites are secure (https://) when sharing company information or passwords?

85 Scarsdale Road, Suite 202, Toronto, Ontario, M3B2R2 866.996.2629 www.manawa.ca

manawa