QUANTUM TECHNOLOGIES — CYBERSECURITY ASSESSMENT GUIDE

Is Your Data Actually Secure? A 13-Point Checklist

Quantum Technologies
Managed IT & AI Solutions for Wisconsin Business
quantumtechnologies.com | 920-818-0900

Before You Start

Most Wisconsin businesses assume they're protected because they have antivirus software. Some of them are right. Most of them aren't.

The checklist on the following pages is built on 13 years of cybersecurity assessments across manufacturing, healthcare, professional services, and construction businesses in Wisconsin. Every item on this list is a gap we've found in real businesses — businesses that thought they were covered, businesses that had recently "had IT look at things," and businesses that were paying for managed services that weren't actually managing much.

This isn't a scare tactic. It's an honest inventory. Work through it carefully, check what you're actually confident about (not what you think is probably fine), and use the scoring at the end to understand where you stand.

The 13-Point Security Checklist

ACCESS CONTROLS

- ☐ **Every employee has their own login — no shared passwords.** Shared credentials are the single most common security gap we find. When everyone logs in as "admin" or shares a department password, you have no audit trail, no accountability, and no way to revoke access when someone leaves.

- ☐ **Multi-factor authentication is enabled for email and cloud applications.** Your email is your identity online. If it can be accessed with just a password — through Microsoft 365, Google Workspace, or any other cloud platform — you're one phishing email away from a full account compromise. MFA stops the vast majority of credential-based attacks cold.
- ☐ **Former employees are removed from all systems within 24 hours of departure.** "We'll get to it" is not a process. We've found active credentials for employees who left 8 months prior. In two of those cases, the accounts had been used after departure. Have a documented offboarding checklist with IT included on day one of any employee exit.
- ☐ **Administrative rights are restricted to employees who actually need them.** Not everyone needs to be a local admin on their computer. Not everyone needs access to your accounting system's full settings. Principle of least privilege — giving people exactly the access their role requires and no more — dramatically limits the blast radius of a compromised account.

BACKUPS & RECOVERY

- ☐ **Backups run automatically, not manually.** Manual backup processes fail. Someone gets busy, someone goes on vacation, someone assumes someone else ran it. Automated backups with verified completion alerts are the only backups you can actually count on. Bonus: do you get an alert when a backup fails?
- ☐ **You have actually tested a restore within the last 90 days.** A backup you've never restored is a backup you don't actually have — you have an archive of files that you hope can be restored under pressure. Test restores are the only way to know your recovery process works before you desperately need it to.
- ☐ **At least one backup copy is stored offsite or in the cloud.** If your backups live on a NAS in the same building as your servers, a fire, flood, or ransomware attack that encrypts your network can take both your primary data and your backup simultaneously. Offsite or cloud-based backup copies are non-negotiable for real recovery capability.

EMAIL & ENDPOINTS

- ☐ **Email has dedicated spam filtering and phishing protection — not just built-in spam.** Gmail and Microsoft 365's built-in spam filters catch a lot. They don't catch everything. Dedicated email security platforms analyze link destinations, attachment behavior, and sender reputation at a level that built-in filters simply don't match. Business email compromise starts with a convincing phishing email that slipped through.
- ☐ **All devices are patched and updated within 30 days of patch release.** The majority of successful cyberattacks exploit known vulnerabilities — vulnerabilities with patches that had been

available for months. Patch management isn't glamorous, but it closes more attack surface than almost anything else on this list.

- ☐ **You have endpoint protection beyond basic antivirus.** Traditional antivirus looks for known malware signatures. Modern endpoint detection and response (EDR) tools watch for behavioral anomalies — things that look like an attack even when no known malware signature is present. If your endpoint security hasn't been updated in the last few years, it likely isn't keeping pace with current threats.

COMPLIANCE & AWARENESS

- ☐ **Your team has received security awareness training within the past year.** Technology is only part of your security posture. Your employees are the most targeted attack surface in your business. Phishing simulations and security awareness training — even a 30-minute annual session — measurably reduce the click rate on malicious emails. This is one of the highest-ROI security investments a small business can make.
- ☐ **You know which regulatory frameworks apply to your business.** Depending on your industry and customers, you may have compliance obligations under HIPAA (healthcare data), PCI DSS (credit card processing), CMMC (defense contracts), or other frameworks. "We don't handle that kind of data" is often incorrect. If you're not sure which frameworks apply to you, that's worth a conversation.
- ☐ **You can answer your cyber insurance questionnaire accurately and confidently.** Cyber insurance questionnaires have become significantly more detailed and technical over the past three years. Insurers are asking about MFA, EDR, backup testing, and privileged access management. Businesses that answer inaccurately — even unintentionally — may find their claims denied. If you're not sure what's in your environment, you shouldn't be signing that form.

How to Read Your Score

11 – 13
Solid foundation. You've done the work. An annual review keeps you current.

7 – 10
Meaningful gaps. These are addressable — but worth a real conversation soon.

Under 7
Real risk right now. Don't wait for an incident to be the motivation.

What to Do Next

If this checklist surfaced gaps, the most practical next step is a no-pressure security assessment with Quantum Technologies. The assessment takes about an hour, covers your full environment — not

just a questionnaire — and gives you a prioritized list of what to fix first, along with honest cost estimates.

There's no sales pitch at the end. If we look at your environment and you're in good shape, we'll tell you. If there are gaps worth addressing, we'll show you exactly what they are and give you options — including ones you can address on your own.

Free security assessment — no pressure: ***quantumtechnologies.com*** | *920-818-0900*