

A SELF-ASSESSMENT CHECKLIST

How secure is your business?

How to use this checklist: You don't need to be a technical expert to work through this. These questions are designed to help you take an honest look at where your business stands. If you're unsure of an answer, that's worth paying attention to.

1 Access & Identity

Who can get into your systems, and should they?

- Do you require multi-factor authentication (a second verification step beyond a password) to access company email, VPN, and remote systems?

- When an employee leaves, is their access to systems and accounts removed promptly?

- Are passwords for shared or system accounts regularly reviewed and updated?

- Do employees have access only to the systems and data they need for their role, nothing more?

2 Your Environment & Configuration

Are your systems set up to protect you?

- Do you know what devices, applications, and cloud services are connected to your network?

- Has anyone reviewed your cloud environment (Microsoft 365, Azure, AWS, etc.) for overly permissive settings in the past year?

- Are there systems set up years ago that no one has reviewed since, and is anyone responsible for making sure their settings are still secure?

3 Updates & Maintenance

Are you keeping the door closed on known risks?

- Are operating system and software updates applied consistently across your organization?

- Do your firewalls, VPNs, and network appliances receive regular updates, or do they fall outside your normal IT process?

- Do employees have access only to the systems and data they need for their role, nothing more?

4 Awareness & Preparedness

Does your team know what to do?

- Have your employees received security awareness training in the past year?

- Do you have a documented plan for what to do if a breach or ransomware incident occurs?

- Have you ever tested that plan, even informally?

Where to Go from Here

No environment is perfect, and this checklist isn't meant to grade yours. It's meant to start a conversation.

If you worked through this and feel good about where you stand, a **vulnerability assessment** can validate that and surface anything worth a second look.

If some questions surfaced uncertainty, that's useful information. Knowing where the gaps are is the first step to closing them, and it's a lot less disruptive to find them proactively than during an incident.

Either way, we're here to help you think it through — not hand you a report and walk away.

Ready to Take a Closer Look at Your Business?

Contact your High Point Networks account manager, or reach our team online. Expect a real conversation, not a sales pitch.

highpointnetworks.com/cybersecurity

Talk with a Security Expert