ADVANTAGE LEADERSHIP CONSULTING

SMB SECURITY SELF-ASSESSMENT

Is Your Business Security-Ready?

A 27-question diagnostic for small and mid-sized business owners

SECURE • IMPROVE • INNOVATE

v1.0 | July 2026

BEFORE YOU BEGIN

How to Use This Assessment

Work through each of the 7 sections below and score your business honestly on every question. Terms that may be unfamiliar are explained in plain language as you go, with a full glossary at the end. There are no wrong answers — only an accurate picture of where you stand today.

0	1	2
NOT IN PLACE	PARTIALLY IN PLACE	FULLY IN PLACE

What You'll Cover

01 **Access & Identity** — *Who can get in, and how tightly that access is controlled.*

02 **Data Protection** — *Where sensitive data lives, and how well it's safeguarded.*

03 **Cyber Awareness** — *How prepared your people are to spot and stop an attack.*

04 **Network & Endpoint** — *The technical foundation protecting your systems day to day.*

05 **Incident Response** — *What happens in the first hours after something goes wrong.*

06 **Leadership & Governance** — *Whether security is treated as a business priority, not an IT chore.*

07 **Remote Access & Data Handling** — *Where modern breaches start, and whether you'd catch one in time.*

01 ACCESS & IDENTITY

Who can get in, and how tightly that access is controlled.

QUESTION	0	1	2
1. Do you use multi-factor authentication (MFA) on all business email and key systems?	○ 0	○ 1	○ 2
2. Are employee accounts deactivated within 24 hours of departure?	○ 0	○ 1	○ 2
3. Do you use unique passwords and a password manager across your team?	○ 0	○ 1	○ 2
4. Is admin/privileged access *(accounts with elevated system permissions)* limited to only those who need it?	○ 0	○ 1	○ 2

CATEGORY SCORE ..... _____ / 8

02 DATA PROTECTION

Where sensitive data lives, and how well it's safeguarded.

QUESTION	0	1	2
5. Do you know where your sensitive business and customer data is stored?	○ 0	○ 1	○ 2
6. Is sensitive data encrypted at rest and in transit *(protected both while stored and while being sent)*?	○ 0	○ 1	○ 2
7. Do you have a current, tested backup of critical business data?	○ 0	○ 1	○ 2
8. Do you have controls limiting who can access or export sensitive data?	○ 0	○ 1	○ 2

CATEGORY SCORE ..... _____ / 8

03 CYBER AWARENESS

How prepared your people are to spot and stop an attack.

QUESTION	0	1	2
9. Have your employees received security awareness training in the last 12 months?	○ 0	○ 1	○ 2

10. Do employees know how to identify and report a phishing email?	○ 0	○ 1	○ 2
11. Do you have a process for verifying wire transfer or payment requests?	○ 0	○ 1	○ 2
12. Have you conducted a simulated phishing test?	○ 0	○ 1	○ 2

CATEGORY SCORE ..... _____ / 8

04 NETWORK & ENDPOINT

The technical foundation protecting your systems day to day.

QUESTION	0	1	2
13. Is your business Wi-Fi separated *(kept on its own isolated network)* from guest networks and any IoT or cloud-managed devices?	○ 0	○ 1	○ 2
14. Are all endpoints (laptops, desktops) running up-to-date antivirus/EDR *(software that actively detects and responds to threats, beyond basic antivirus)*?	○ 0	○ 1	○ 2
15. Is your firewall configured and actively maintained?	○ 0	○ 1	○ 2
16. Do you patch operating systems and software regularly?	○ 0	○ 1	○ 2

CATEGORY SCORE ..... _____ / 8

05 INCIDENT RESPONSE

What happens in the first hours after something goes wrong.

QUESTION	0	1	2
17. Do you have a written incident response plan *(a documented step-by-step guide for what to do during a breach)*?	○ 0	○ 1	○ 2
18. Do you know who to call if you experience a ransomware attack?	○ 0	○ 1	○ 2
19. Have you tested your incident response plan in the last 12 months?	○ 0	○ 1	○ 2
20. Do you have cyber liability insurance?	○ 0	○ 1	○ 2

CATEGORY SCORE ..... _____ / 8

06 LEADERSHIP & GOVERNANCE

Whether security is treated as a business priority, not an IT chore.

QUESTION	0	1	2
21. Does your leadership team treat cybersecurity as a business priority?	○ 0	○ 1	○ 2
22. Do you conduct an annual security risk assessment?	○ 0	○ 1	○ 2
23. Do you have a vendor/third-party security review process?	○ 0	○ 1	○ 2
24. Do you have written security policies in place?	○ 0	○ 1	○ 2

CATEGORY SCORE ..... _____ / 8

07 REMOTE ACCESS & DATA HANDLING

Where modern breaches start, and whether you'd catch one in time.

QUESTION	0	1	2
25. Do you require secure VPN access *(an encrypted connection for staff working outside the office)* for all remote or RDP *(a common tool for remotely controlling a work computer)* access to business systems?	○ 0	○ 1	○ 2
26. Do you have logging or monitoring in place to detect unauthorized activity on your network?	○ 0	○ 1	○ 2
27. Do you have documented controls for handling customer payment data (credit card, ACH, bank details)?	○ 0	○ 1	○ 2

CATEGORY SCORE ..... _____ / 6

RESULTS

Your Total Score

CATEGORY	SCORE
Access & Identity	_____ / 8
Data Protection	_____ / 8
Cyber Awareness	_____ / 8
Network & Endpoint	_____ / 8
Incident Response	_____ / 8
Leadership & Governance	_____ / 8
Remote Access & Data Handling	_____ / 6
TOTAL SCORE	_____ / 54

INTERPRETING YOUR RESULTS

What Your Score Means

SCORE	TIER	WHAT IT MEANS
45 – 54	**Security Leader**	Strong posture with minor gaps to close. You're ahead of most SMBs.
31 – 44	**Building**	Solid foundation with meaningful gaps. Risk is manageable but real.
18 – 30	**Significant Exposure**	Reactive security posture with high-risk gaps. Action needed.
0 – 17	**Urgent**	Immediate attention required — your business is currently exposed to high-probability, high-impact events.

Using Your Results

Your score is a starting point, not a verdict. The categories where you scored lowest are the ones most worth addressing first — a single zero in a critical area can matter more than a high total score. Bring this completed assessment to your Security Review and we'll turn it into a prioritized, practical action plan.

REFERENCE

Glossary of Terms

MFA (Multi-Factor Authentication)	Requiring a second proof of identity — like a code on your phone — in addition to a password.
Privileged Access	Accounts with elevated permissions, such as the ability to install software or change system settings.
Encrypted at Rest / in Transit	Data that is scrambled and unreadable both while stored on a device and while being sent over a network.
EDR (Endpoint Detection & Response)	Software that actively watches for and responds to threats, going beyond traditional antivirus.
Segmented / Separated Network	Keeping different types of devices (e.g., guest Wi-Fi, IoT devices) on isolated networks so a breach in one can't spread to the other.
Incident Response Plan	A written, step-by-step guide for what your business does in the first hours and days after a security incident.
VPN (Virtual Private Network)	An encrypted connection that lets staff safely access business systems from outside the office.
RDP (Remote Desktop Protocol)	A common tool for remotely controlling a work computer — a frequent target for attackers if left unsecured.

READY TO KNOW WHAT TO FIX FIRST?

Your score tells you where you stand.

A Security Review tells you what to do about it.

Book a free 30-minute Security Review with Adam Campbell at Advantage Leadership Consulting. We'll walk through your highest-risk gaps and give you a prioritized action plan — no sales pitch, no obligation.

BOOK YOUR FREE SECURITY REVIEW →

ADVANTAGE LEADERSHIP CONSULTING

Secure. Improve. Innovate.

adam@advantageleadershipconsulting.com • (402) 799-1090 • advantageleadershipconsulting.com