

SMALL BUSINESS SECURITY HEALTH CHECK

Executive cybersecurity snapshot for a growing professional-services firm

Sample Portfolio Deliverable | Illustrative Price: \$499

FICTIONAL DEMONSTRATION — NOT AN ACTUAL CLIENT REPORT

Executive Summary

Sample client: Northstar Professional Services LLC, a fictional 28-person firm using Microsoft 365, cloud file storage, laptops and several SaaS vendors.

Overall sample posture: MODERATE RISK. The organization has several useful baseline controls, but gaps in identity protection, asset visibility, backup testing and incident-response readiness increase operational risk.

Scope & Method

This demonstration uses a lightweight review aligned to the six NIST Cybersecurity Framework (CSF) 2.0 Functions: Govern, Identify, Protect, Detect, Respond and Recover. It is a practical health check, not a penetration test, certification, audit attestation or guarantee of compliance.

At-a-Glance Scorecard

CSF Function	Sample Rating	What We Observed
Govern	Needs Improvement	Security ownership exists informally; policies and review cadence are not documented.
Identify	Needs Improvement	No complete hardware/software/SaaS inventory or formal risk register.
Protect	Fair	MFA exists for administrators but is not enforced for all users; patching is largely automatic.
Detect	Fair	Cloud security alerts exist but are not centrally reviewed against a documented process.
Respond	Needs Improvement	No written incident-response plan, severity matrix or contact tree.
Recover	Fair	Backups exist, but restore testing and recovery objectives are not documented.

Priority Findings

ID	Risk	Priority	Recommended Action
HC-01	MFA not enforced for every user	High	Require phishing-resistant or strong MFA for all supported accounts, beginning with privileged and remote-access users.
HC-02	No authoritative asset/SaaS inventory	High	Create and maintain an inventory with owner, criticality, data type and lifecycle status.
HC-03	No tested incident-response procedure	High	Create a concise response plan, escalation tree and tabletop exercise.
HC-04	Backups not periodically restored/tested	Medium	Define recovery objectives and perform scheduled restore tests.
HC-05	Vendor security reviews are ad hoc	Medium	Introduce a risk-tiered vendor intake and annual review process.

30-Day Action Plan

- Days 1-7: enforce MFA for all supported users and confirm privileged-account inventory.
- Days 1-14: build hardware, software and SaaS inventory and assign business owners.
- Days 8-21: draft incident-response plan and escalation contacts.
- Days 15-30: test one representative restore and document results.
- By Day 30: classify critical vendors and begin security evidence collection.

Client Deliverables

- Executive security snapshot
- Six-function CSF 2.0 scorecard
- Top-five prioritized findings
- 30-day remediation roadmap
- One 30-minute findings review

Limitations

Findings are based only on evidence supplied within the agreed scope. This service does not constitute legal advice, a regulatory certification, penetration testing, or an audit opinion.