RISK ASSESSMENT REPORT

Small Business Network (Case Study)

Author: A. Brito

Date: September 2025

Note: Based on a real freelance project. Client information anonymized.

EXECUTIVE SUMMARY

Scope: A mid-sized distribution company (~60 PCs, tablets, and servers across HQ, local branch offices, and overseas sites).

Objective: Assess risks in the hybrid Ubiquiti-based network, VPN, Microsoft 365, and physical environment.

Key Findings:

- Strong segmentation and MFA on Microsoft 365.
- Risks identified in VPN access, IoT devices, Windows 10 end-of-life, backup testing, physical access controls, and legacy systems.
- Recommendations provided to strengthen resilience across IT and physical security domains.

ENVIRONMENT OVERVIEW

Headquarters: Sales, Logistics, Marketing, and warehouse operations.

- 25 Windows computers, 7 tablets (Logistics on Enterprise Wi-Fi)
- 1 on-prem server (Sales software)
- 3 Network printers accessible via VPN VLAN
- Ubiquiti network: UDM Pro, 4 switches, 10 APs, VLAN segmentation

Branch Offices (local):

- Office 1: 4 Windows computers (Accounting + warehouse)
- Office 2: 1 Windows computer (Sales + warehouse)
- Office 3: 1 Windows computer (Sales)
- All connect via VPN

Overseas Offices:

- Office 4: 13 Windows computers (Sales Support)
- Office 5: 13 Windows computers (Logistics Support)
- VPN connectivity to HQ

Cloud/Storage:

- 40 Microsoft 365 accounts (MFA enabled)
- Synology NAS for shared storage (segmented by department)
- Acronis backups (daily to NAS, weekly to cloud)
- Legacy HikVision NVR system in use

RISK REGISTER

Risk ID	Description	Likelihood	Impact	Rating	Mitigation
R-01	VPN users may not all be using MFA	High	High	Critical	Enforce MFA on VPN login, not just O365
R-02	IoT VLAN (cameras) may have weak/default credentials	High	Medium	High	Apply strong passwords + firewall rules
R-03	Backup restore testing not documented	Medium	High	High	Implement quarterly recovery drills
R-04	Shared drive permissions broad in some areas	Medium	Medium	Medium	Refine least privilege access by department
R-05	Overseas VPN latency → users bypass controls	Low	High	Medium	Improve monitoring & enforce VPN-only access
R-06	Several PCs still running Windows 10, which will reach end-of-support in Oct 2025	High	High	High	Plan phased upgrades or hardware refresh; isolate legacy systems if needed
R-07	No access control on building doors, risk of unauthorized entry	Medium	High	High	Implement badge/PIN system or enforce visitor logs
R-08	Legacy HikVision NVR with potential unpatched vulnerabilities	High	Medium	High	Replace with supported system or isolate on IoT VLAN

RISK ANALYSIS (NARRATIVE)

VPN & MFA: While O365 accounts had MFA, VPN access relied on username/password. This gap exposes risk if credentials are stolen.

IoT VLAN: Cameras and IoT gear are isolated but may have default credentials; these are often exploited for lateral movement.

Backups: Daily/weekly backups exist but recovery testing is infrequent. Without proof of restore, reliability is uncertain.

File Sharing: NAS shared folders are segmented, but some groups have broad access that could lead to data leakage.

Windows 10 End-of-Life: Several endpoints remain on Windows 10, which will no longer receive security updates after Oct 2025. This presents a high risk of unpatched vulnerabilities. Recommended phased replacement plan and compensating controls.

Physical Access: No access control on building doors increases risk of unauthorized entry and tampering with IT assets. Suggested implementing basic access control or visitor.

Legacy HikVision NVR: Outdated NVR system may have known vulnerabilities. Recommend upgrading or fully isolating on IoT VLAN with no external access.

RECOMMENDATIONS & NEXT STEPS

1. Extend MFA to VPN users.
2. Harden IoT VLAN with firewall rules + credential rotation.
3. Schedule quarterly backup restore testing.
4. Review NAS permissions against least privilege.
5. Enhance VPN monitoring for remote/overseas offices.
6. Create phased plan to replace or isolate Windows 10 machines.
7. Implement building access control measures (badges or visitor logs).
8. Replace or isolate legacy HikVision NVR system.

CONCLUSION

Current security posture = Moderate (segmentation + MFA on cloud accounts are positives). By implementing recommendations, posture would move toward Low Risk, aligning with NIST CSF (Identify, Protect, Detect, Respond, Recover). Addressing Windows 10 EOL, physical access, and legacy NVR concerns will further strengthen resilience and compliance.