RISK POSTURE REASSESSMENT REPORT (6-MONTH UPDATE)

Small Business Network (Case Study)
Author: A. Brito
Date: March 2026

Note: Based on a real freelance project. Client information anonymized. This report represents a 6-month follow-up to the initial risk assessment conducted in September 2025.

EXECUTIVE SUMMARY

This report presents a 6-month reassessment of the organization's security posture following the initial risk assessment conducted in September 2025.

Over this period, the organization successfully reduced several high-risk exposures through infrastructure modernization, credential hygiene improvements, and removal of legacy systems. Notably, unsupported Windows 10 endpoints were replaced, legacy surveillance systems were decommissioned, and access control policies were improved.

At the same time, business growth and infrastructure changes, particularly the introduction of WiFi-based IoT surveillance systems and expansion of overseas operations introduced new risks related to network performance, identity management, and scalability.

To address visibility gaps identified in the initial assessment, centralized monitoring solutions were implemented using **Wazuh** (endpoint visibility and vulnerability tracking) and **Graylog** (network and IDS/IPS log aggregation). These improvements significantly enhanced the organization's ability to detect and respond to threats.

Overall Risk Trend:

- Legacy/System Risk: Reduced
- Identity & Access Risk: In Progress
- Network & Availability Risk: Increased (new challenges)
- Monitoring & Detection: Significantly Improved

The organization has transitioned from a **static, reactive posture to a more mature, continuously monitored security model**, with ongoing efforts focused on identity security, network optimization, and secure scalability.

ENVIRONMENT OVERVIEW (UPDATED)

Infrastructure Changes (Last 6 Months)

- Replacement of legacy HikVision NVR with WiFi-based camera systems
- Deployment of a secondary ISP connection to support IoT traffic
- Expansion of overseas offices:
    - Increased to ~20 users per office (~40 total endpoints overseas)
- Replacement of legacy Windows 10 endpoints
- Continued use of:
    - Ubiquiti (UniFi) network infrastructure
    - Microsoft 365 with MFA
    - Synology NAS for storage
    - Acronis backup solution

RISK COMPARISON SUMMARY

Risk Area	Initial Status	Current Status	Outcome
VPN MFA (R-01)	Critical	Medium	In Progress
IoT Devices (R-02)	High	Medium	Risk Shifted
Backup Reliability (R-03)	High	Low	Mitigated
NAS Permissions (R-04)	Medium	Low	Mitigated
Overseas VPN Risk (R-05)	Medium	Medium	Increased Exposure
Windows 10 EOL (R-06)	High	Low	Mitigated
Physical Security (R-07)	High	High	Accepted Risk
Legacy NVR (R-08)	High	Eliminated	Resolved
Network Performance	N/A	High	New Risk

REMEDIATION ACHIEVEMENTS

The organization demonstrated strong progress in addressing previously identified risks:

Identity & Access Improvements

- Removal of inactive/legacy user accounts
- Credential rotation implemented
- Preparation for MFA enforcement on VPN via UniFi Identity integration

Endpoint & Infrastructure Security

- Replacement of Windows 10 systems nearing end-of-life
- Planned server upgrade to reduce technical debt and improve security posture

Data Security

- Review and refinement of NAS permissions aligned with least privilege principles

Legacy System Removal

- Decommissioning of legacy HikVision NVR system, eliminating known vulnerability risks

Backup & Recovery Validation

- Backup restore procedures successfully tested
- Increased confidence in recovery capabilities and business continuity

NEW RISKS IDENTIFIED

R-09: Network Congestion & Availability Risk

Description: The deployment of multiple WiFi-based surveillance cameras introduced significant bandwidth consumption, impacting overall network performance.

Impact:
- Degraded user experience
- Potential disruption to business operations
- Increased latency for VPN users

Mitigation Implemented:
- Deployment of a secondary ISP connection to isolate camera traffic

Residual Risk:
- Lack of traffic shaping or QoS may still allow resource contention

R-10: Expanded Overseas Attack Surface

Description: Growth in overseas endpoints increased reliance on VPN connectivity and expanded the attack surface.

Impact:
- Increased vulnerability exposure
- Greater difficulty in monitoring and patching
- Potential for inconsistent security enforcement

R-11: Incomplete MFA Enforcement on VPN

Description: While Microsoft 365 enforces MFA, VPN authentication still relies partially on username/password.

Current Initiative:
- Integration of Microsoft Entra ID with UniFi Identity (RADIUS) to enforce MFA

Risk:
- Misconfiguration could lead to authentication bypass

R-12: Future SD-WAN / Fabric Deployment Risk

Description: Planned deployment of UniFi UCG devices with SD-WAN introduces new trust relationships between sites.

Potential Risks:
- Lateral movement between offices
- Misconfigured routing policies
- Overly permissive inter-site access

CONTINUOUS MONITORING & DETECTION IMPROVEMENTS

To address visibility gaps identified in the initial assessment, the organization implemented centralized monitoring solutions:

Wazuh (Endpoint Visibility & Vulnerability Management)

- Deployed for endpoint monitoring and vulnerability tracking
- Provides visibility into:
  - System vulnerabilities
  - Security events
  - Endpoint activity

Impact:
- Enables validation of remediation efforts
- Supports continuous risk assessment

Graylog + UniFi IDS/IPS (Network Monitoring)

- Centralized ingestion of IDS/IPS logs from UniFi infrastructure
- Provides visibility into:
  - Port scans
  - Suspicious external traffic
  - Potential intrusion attempts

Key Outcome
The introduction of centralized logging and monitoring transformed the environment from a reactive posture to a more proactive and observable security model.

CONTROL MATURITY IMPROVEMENT

Control Area	Before	After
Logging	Minimal	Centralized (Graylog)
Endpoint Visibility	Limited	Wazuh deployed
Threat Detection	Reactive	IDS/IPS + log monitoring
Risk Tracking	Static	Continuous
Backup Validation	Unverified	Tested & validated

ACCEPTED RISKS / CONSTRAINTS

Physical Security (R-07)

- Recommendation: Implement badge/PIN access controls
- Current Status: Not implemented due to budget constraints

Risk Decision:

- Risk formally accepted by the business

LESSONS LEARNED

- Security improvements can introduce operational challenges (e.g., IoT deployment impacting network performance)
- Removing legacy systems reduces risk but may introduce new infrastructure dependencies
- Visibility is critical monitoring significantly improves security decision-making
- Identity remains a central control point across all environments
- Not all risks can be mitigated immediately; business constraints must be considered

RECOMMENDATIONS (NEXT 6 MONTHS)

Identity & Access

- Fully enforce MFA on VPN access
- Implement conditional access policies via Microsoft Entra ID

Network Security

- Implement QoS / traffic shaping for IoT devices
- Monitor outbound traffic from camera VLAN
- Segment inter-site traffic for SD-WAN deployment

Monitoring & Detection

- Expand alerting capabilities (SIEM use cases)
- Monitor VPN login behavior and anomalies
- Correlate endpoint and network events

Backup & Recovery

- Continue periodic restore testing
- Document recovery time objectives (RTO) and recovery point objectives (RPO)

Infrastructure & Scalability

- Complete server upgrade
- Secure SD-WAN deployment with least privilege routing policies

CONCLUSION

Over the past 6 months, the organization has made measurable improvements in reducing legacy risks and strengthening its overall security posture. Key achievements include system modernization, improved access control hygiene, and the introduction of centralized monitoring.

However, business growth and infrastructure expansion have introduced new challenges, particularly in identity management, network performance, and scalability.

The organization has progressed from a **basic to intermediate level of security maturity**, aligning more closely with continuous monitoring principles outlined in modern security frameworks. With continued focus on identity security, network optimization, and proactive monitoring, the organization is well-positioned to further reduce risk and support secure growth.