RISK POSTURE REASSESSMENT REPORT (1-YEAR UPDATE)

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

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

EXECUTIVE SUMMARY

This report presents a 1-year reassessment of the organization's security posture, building upon the initial risk assessment conducted in September 2025.

While the 6-month milestone saw the successful removal of legacy systems and the introduction of centralized monitoring, business growth and overseas expansion introduced new challenges regarding network congestion, identity management, and VPN reliance. Over the past six months, the organization has aggressively mitigated these operational risks by transitioning from a small-business infrastructure model to an enterprise-grade SD-WAN architecture.

Key achievements in this phase include the elimination of high-overhead client VPNs in favor of a hardware-backed SD-WAN fabric, the segmentation of IoT surveillance traffic via a dedicated Starlink WAN connection, and the strict enforcement of multi-factor authentication (MFA) across all remote access points. Furthermore, M365 security hardening and centralized Splunk SIEM deployments have demonstrably reduced successful phishing incidents and enhanced threat correlation capabilities.

Overall Risk Trend:

- **Network & Availability Risk:** Reduced (Mitigated via dual-WAN and policy-based routing)
- **Identity & Access Risk:** Resolved (MFA fully enforced)
- **Overseas Exposure:** Significantly Reduced (Transitioned to SD-WAN)
- **Monitoring & Detection:** Advanced (Splunk SIEM in production)

ENVIRONMENT OVERVIEW (UPDATED)

Infrastructure Changes (Months 6 to 12)

- Deployment of UniFi Cloud Gateway (UCG Ultra) appliances at overseas offices.
- Transition from individual client VPNs to a 4-node Hub-and-Spoke SD-WAN fabric (UniFi Site Magic).
- Implementation of a secondary Starlink ISP connection specifically for routing IoT and WiFi camera traffic.
- Integration of Microsoft Entra ID with UniFi One-Click VPN for identity management.
- Migration of network logging to a Dockerized Splunk SIEM, monitoring the UDM Pro and UCG Ultra infrastructure, running alongside Wazuh for endpoints.

RISK COMPARISON SUMMARY

Risk Area	6-Month Status	1-Year Status	Outcome
Network Congestion (R-09)	High	Low	Resolved via Starlink WAN2
Overseas Attack Surface (R-10)	High	Low	Resolved via SD-WAN Fabric
Incomplete VPN MFA (R-11)	In Progress	Eliminated	Resolved via Entra ID
SD-WAN Deployment Risk (R-12)	New Risk	Low	Successfully Deployed

REMEDIATION ACHIEVEMENTS

1. Network Congestion & IoT Traffic Isolation (R-09)

The deployment of WiFi-based surveillance cameras previously introduced significant bandwidth consumption, leading to degraded user experiences and VPN latency. To resolve this resource contention, a secondary Starlink ISP connection was provisioned. Policy-Based Routing (Traffic Routes) was configured on the UniFi gateways to strictly enforce all IoT and camera traffic out through the Starlink WAN2 interface. This physical segmentation completely eliminated network congestion on the primary business line while maintaining high-fidelity video streams for the overseas Quality Assurance and Loss Prevention teams.

2. Overseas Attack Surface & SD-WAN Implementation (R-10 & R-12)

The expansion to ~40 overseas endpoints previously increased vulnerability exposure due to a heavy reliance on individual VPN connectivity. To modernize this architecture, UCG Ultra gateways were deployed at both overseas branches. The network was transitioned into a 4-node Hub-and-Spoke SD-WAN utilizing UniFi Site Magic, with an Imperial-Decora UDM Pro serving as the central hub. This fabric deployment eliminated the need for legacy VPN clients for internal access. Additionally, custom WireGuard policy-based routes were engineered to selectively bypass regional website blocking for overseas staff, ensuring business continuity without exposing the broader network to misconfigured routing policies.

3. Identity & Zero-Trust VPN Authentication (R-11)

While Microsoft 365 previously enforced MFA, the VPN still relied partially on vulnerable username/password authentication. This gap was closed by deploying UniFi One-Click VPN integrated directly with the organization's Microsoft Entra ID instance. All remote access now requires mandatory MFA and is governed by conditional access policies, completely eliminating the authentication bypass risk.

4. M365 Hardening & Phishing Reduction

Building upon the established Microsoft 365 environment, custom security hardening measures were introduced. Automated spoofing detection and logic-based custom banner alerts were engineered via the Defender portal. These administrative controls have yielded a measurable, sustained decrease in successful phishing attempts across the organization.

5. Advanced Continuous Monitoring

The organization previously utilized Graylog for centralized IDS/IPS log ingestion. To expand alerting capabilities and SIEM use cases, the network monitoring infrastructure was migrated to a Dockerized Splunk SIEM. Splunk now ingests advanced syslog telemetry from the centralized Imperial-Decora UDM Pro and the three regional UCG Ultra gateways. Combined with Wazuh for continuous endpoint visibility, this unified monitoring approach has significantly matured the organization's threat hunting and correlation capabilities.

CONTINUOUS MONITORING & DETECTION IMPROVEMENTS

To address the visibility requirements of the expanded SD-WAN architecture, the organization standardized its centralized monitoring solutions:

Wazuh (Endpoint Visibility & Vulnerability Management)

- Maintained as the primary tool for endpoint monitoring and vulnerability tracking across the ~40 overseas endpoints and domestic systems.
- Enables rapid validation of remediation efforts and supports continuous risk assessment for remote staff.

Splunk (Network SIEM & IDS/IPS Log Aggregation)

- Deployed as a Docker container to centralize network telemetry.
- Ingests logs across the entire SD-WAN fabric (1x UDM Pro, 3x UCG Ultras).
- Provides deep log correlation, visibility into port scans, external traffic anomalies, and centralized intrusion detection alerts.

CONTROL MATURITY IMPROVEMENT

Control Area	6-Month Status	12-Month Status
Network Logging	Graylog (Basic Ingestion)	Splunk SIEM (Advanced Correlation)
Remote Access	Client VPN (Username/Password)	SD-WAN Fabric + One-Click VPN
Identity Security	Partial MFA	Full Entra ID Conditional Access
Traffic Management	Congested Single WAN	Segmented Dual-WAN (Starlink IoT Routing)
Threat Detection	Reactive / Fragmented	Proactive / Centralized

LESSONS LEARNED

- **Hardware-Backed Routing Outperforms Client VPNs:** Transitioning to a Hub-and-Spoke SD-WAN using UCG Ultras significantly reduced administrative overhead and eliminated the performance bottlenecks of managing 40+ individual VPN connections.
- **Physical Segmentation Solves IoT Contention:** Utilizing a dedicated secondary WAN (Starlink) with policy-based routing is highly effective for isolating high-bandwidth IoT surveillance traffic without disrupting core business operations.
- **Centralized Identity is Non-Negotiable:** Integrating network access with Microsoft Entra ID streamlines onboarding and ensures conditional access and MFA are uniformly enforced across all perimeters.
- **Log Aggregation Must Scale with the Network:** Moving to a Splunk SIEM environment provided the necessary correlation depth to effectively monitor the new multi-site SD-WAN fabric.

CONCLUSION

Between month 6 and month 12, the organization successfully executed complex architectural upgrades that transitioned the network from an intermediate, reactive state to a highly scalable, enterprise-ready environment. By deploying a robust SD-WAN fabric, utilizing a dedicated Starlink connection for high-bandwidth IoT devices, and strictly enforcing Entra ID MFA across all access layers, the previously identified risks regarding network availability and identity exposure have been thoroughly mitigated. The environment now fully embodies continuous monitoring principles and secure scalability.