SECURITY RISK ASSESSMENT SUMMARY

Executive Overview — Internal Operations & IT Infrastructure

Organization	Acme Manufacturing LLC [Sanitized — Client Confidential]	**Date**
Industry	Manufacturing / Light Industrial	Q1 2026
Assessor	Kevin Leverett | Converged Security Consulting	
Framework	NIST Cybersecurity Framework (CSF) v2.0 | NIST SP 800-30 Risk Assessment Guide	

1. Organization Overview

The assessed organization operates a light manufacturing facility with approximately 85 employees across two sites. IT infrastructure includes a centralized internal network, a mix of Windows workstations and servers, an internally-hosted HR web application, and remote access via VPN for approximately 20 users. No formal information security program is currently in place.

This assessment evaluates the organization's current security posture across six risk domains and provides prioritized recommendations suitable for executive decision-making and resource planning.

2. Current Risk Posture — At a Glance

Risk Domain	Risk Level	Key Finding
Access Control & Authentication	Critical	Default credentials on firewall; no MFA on admin accounts
Patch & Vulnerability Management	High	Unpatched RCE on Windows Server; 60% of endpoints outdated
Network Security	High	SMBv1 enabled; no network segmentation between IT and OT
Data Protection & Encryption	Medium	Internal HR application transmits data over unencrypted HTTP
Logging, Monitoring & Incident Response	Medium	No centralized logging; no documented IR plan; no SIEM in place
Security Awareness & Policy	Low	No formal security policy; no employee awareness training program

3. Risk Narrative

The organization's most significant exposure is in access control and patch management — two foundational controls that form the basis of any secure environment. The combination of default administrative credentials on network infrastructure and an unpatched critical vulnerability on a production server creates conditions where a single network-connected attacker could achieve full administrative control without needing advanced techniques.

The absence of multi-factor authentication, centralized logging, and a documented incident response plan means that a breach could occur and persist undetected. Industry data suggests the average dwell time for an undetected attacker in an SMB environment exceeds 100 days.

These findings are not unusual for organizations at this stage of security maturity. The good news: the highest-priority risks are addressable quickly and at low cost relative to the potential impact of a successful attack.

4. Priority Recommendations

Priority	Timeline	Action	Estimated Effort
1	24 hrs	Change default firewall credentials; enable MFA on all admin accounts	2–4 hours (internal IT)
2	24–48 hrs	Patch Windows Server (critical RCE); isolate if patch not immediately available	1–3 hours (patch deployment)
3	7 days	Disable SMBv1; deploy centralized endpoint patch management	4–8 hours (configuration)
4	30 days	Enable HTTPS on internal HR portal; implement password complexity policy	Low — policy + cert deployment
5	60 days	Deploy SIEM (Splunk Free or Microsoft Sentinel); begin log aggregation	Medium — platform setup
6	90 days	Develop written security policy; launch employee phishing awareness training	Low — policy drafting + training platform

5. Recommended Next Steps

The following actions are recommended to move from assessment to active risk reduction:

- Schedule a 30-minute debrief with your IT lead and key stakeholders to walk through findings and confirm remediation ownership
- Assign a remediation owner and target date for each Priority 1 and Priority 2 item
- Request a follow-up verification scan 30 days after remediation of Critical and High findings
- Consider engaging a managed security service provider (MSSP) if internal IT capacity is limited
- Schedule a quarterly reassessment to track posture improvement over time

This summary is designed for executive and operational decision-making. A full technical findings report with CVE details, CVSS scores, and MITRE ATT&CK mappings is available upon request.

Prepared by: Kevin Leverett | Converged Security Consulting

k.leverett32@gmail.com | (850) 774-2218 | Charlotte, NC (Remote Available) | linkedin.com/in/kevin-leverett-8b1828128

All assessments performed under signed authorization agreement only. Unauthorized security testing is prohibited under the CFAA.