Pinnacle Manufacturing Inc.

Industrial Manufacturing | 1,200 Employees | Columbus, OH | $85M Revenue

74
RISK SCORE
HIGH RISK

EXECUTIVE SUMMARY

This target presents material cyber risk requiring purchase price adjustment and post-close remediation. External reconnaissance identified an undisclosed ransomware incident (Q2 2024), 312 compromised employee credentials, and 14 active infostealer infections indicating ongoing compromise. The attack surface includes exposed RDP, unpatched VPN infrastructure, and weak email security controls. Estimated remediation cost: $1.8M-$2.4M. Recommend 5% escrow holdback and 100-day remediation plan as closing conditions.

312	14	1	23	$2.1M
EXPOSED CREDENTIALS	INFOSTEALER INFECTIONS	UNDISCLOSED INCIDENT	CRITICAL CVES	EST. REMEDIATION

CREDENTIAL EXPOSURE ANALYSIS

312 Records

SOURCE	COUNT	RISK	DETAILS
Infostealer Logs	14	CRITICAL	Active infections with session cookies for M365, Salesforce, ERP system. MFA bypass possible. Indicates ongoing compromise.
Breach Databases	198	HIGH	LinkedIn (2021), Dropbox (2012), industry-specific breach (2023). Includes plaintext passwords.
Combolist Exposure	87	MEDIUM	Credentials in aggregated lists used for credential stuffing. 67% password reuse detected.
Executive Accounts	13	CRITICAL	C-suite and VP-level accounts exposed including CEO, CFO, VP Engineering. High-value targets for BEC.

INCIDENT HISTORY

Undisclosed Event Detected

Q2 2024 — CRITICAL **Ransomware Incident - BlackCat/ALPHV Affiliate**
Dark web intelligence indicates data exfiltration and encryption event. Target company name appeared on ransomware leak site (subsequently removed, suggesting payment). Not disclosed in management representations. Financial records, employee PII, and customer data potentially compromised.

2022 — HIGH **Business Email Compromise Attempt**
Wire fraud attempt targeting accounts payable. Unclear if successful. Indicates weak email security controls and employee training gaps.

2019 — MEDIUM **Third-Party Breach Exposure**
HR vendor breach exposed employee PII. Disclosed and remediated.

DEAL IMPACT ANALYSIS

$1.8M - $2.4M	5%	100 Days
ESTIMATED REMEDIATION	RECOMMENDED ESCROW	REMEDIATION TIMELINE

Valuation Impact: Undisclosed ransomware incident and ongoing infostealer infections represent material cyber risk. Recommend purchase price adjustment of $2-3M or equivalent escrow holdback. Reps & warranties should include cyber incident disclosure with indemnification for undisclosed events.

EXTERNAL ATTACK SURFACE

47 Assets Discovered

ASSET TYPE	COUNT	RISK	FINDINGS
Remote Access	6	CRITICAL	RDP exposed on 3 hosts (no NLA). VPN gateway running Fortinet with CVE-2024-21762 (actively exploited). Citrix ADC with known vulnerabilities.
Web Applications	18	HIGH	Customer portal with SQLi indicators. Exposed admin panels. WordPress instances with outdated plugins. Staging environment with prod database.
Mail Infrastructure	4	HIGH	Exchange server missing recent security updates. Open relay on dev server. Autodiscover misconfiguration.
Cloud Resources	12	MEDIUM	AWS S3 buckets with weak permissions. Azure blob storage enumerable. Shadow SaaS applications detected.
IoT/OT Systems	7	HIGH	Industrial control systems accessible from internet. SCADA interfaces with default credentials. Building management exposed.

EMAIL SECURITY POSTURE

SPF	WEAK	Too permissive (+all), allows spoofing
DKIM	OK	Configured for primary domain
DMARC	NONE	No DMARC record - BEC risk

BEC Risk: Missing DMARC enables email spoofing attacks. Combined with exposed executive credentials, this creates significant wire fraud risk.

THIRD-PARTY EXPOSURE

Critical Vendors	4 identified with elevated risk
Shadow IT	23 unauthorized SaaS services
Data Exposure	Customer data in 3rd party breach

Supply Chain: Primary ERP vendor (Acme Software) appeared in recent breach disclosure. Credential overlap detected.

Investment Committee Recommendation: PROCEED WITH CONDITIONS

This target presents addressable cyber risk that should not be a deal-breaker but requires material adjustments.

Required Conditions:
1. Purchase price reduction of $2.5M OR 5% escrow holdback for cyber remediation
2. Cyber incident disclosure rep with 24-month indemnification tail
3. 100-day post-close remediation plan with defined milestones
4. Immediate engagement of IR firm to assess ongoing infostealer compromise
5. R&W insurance cyber exclusion review with carrier

Post-Close Priority Items: Credential reset across organization, Fortinet VPN patching, DMARC implementation, RDP remediation, IR assessment for ransomware incident scope.