5 Star Data Systems, LLC

A Case Study

Plymouth Fabricators, Inc. (PFI)

A Model for Modern Manufacturing Cyber Resilience

August 5, 2025

Version History

Version	Date	Author	Description	Approved by
1.0	Aug. 5, 2025	RLN	First Draft	N/A

Table of Contents

Table of Tables

Executive Summary

This case study examines the journey of Plymouth Fabricators, Inc. (PFI), a $5 million regional custom metals manufacturer operating across Massachusetts and New Hampshire, as it addresses the evolving landscape of cyber risk, compliance, and digital transformation in the manufacturing sector. (PFI is a fictitious company.) PFI's experience—rooted in real-world business priorities, operational complexity, and legacy system constraints—demonstrates how forward-thinking leadership, partnering with 5 Star Data Systems LLC (5SDS), delivered measurable improvements in risk reduction, operational resilience, and market advantage.

Using a combination of vCISO consulting, advanced Zero Trust network deployment, and a comprehensive risk-based approach, PFI transformed its information security and compliance profile. Their investments were not just theoretical but were rooted in tangible business results, including measurable annual loss reduction, insurance savings, successful audits, and increased executive trust in digital initiatives. The case highlights not only technological changes but also practical priorities, challenges, and outcomes that matter to manufacturing executives and supply chain partners.

1. Organizational Profile

Company: Plymouth Fabricators, Inc. (PFI)

Industry: Custom fabricated alloys and tools

Revenue: $5 million (2024)

Sites: Athol, MA (headquarters) and Jaffrey, NH

Employees and Contractors: 43

Ownership: Closely held, family business (founded 1975; 23 shareholders, 500,000 shares)

Debt:

Core Customers: Aerospace, defense, industrial, and precision manufacturing clients

IT/OT mix: Modern office/ERP systems alongside legacy manufacturing and QA equipment

Leadership:

CEO: James Plymouth

COO: Jeri O'Donnell

Strategic direction and operational oversight are dominated by hands-on family leadership, with strong local roots and a reputation for quality and reliability.

2. Business Challenge: The Era of Digital Risk

In late 2024, PFI encountered the same dilemma facing thousands of U.S. manufacturers:

- Legacy systems (including essential QA devices running Windows XP) and industrial OT pose persistent operational and cyber risk, yet remain critical for core processes and difficult to upgrade.
- Rapid expansion in remote work, cloud adoption (Dynamics 365, Microsoft 365), and supply chain integration saw new attack surfaces exposed—well beyond what basic firewalls and antivirus solutions can defend.

- PFI's key government and defense clients mandated compliance with rigorous frameworks (notably CMMC Level 2) as a contract requirement. Yet, existing security and compliance investments were focused almost entirely on confidentiality—leaving integrity, availability, and operational resilience as afterthoughts.
- The company's previous "good enough" security was not only a regulatory risk but left gaps against ransomware, phishing, third-party attacks, and insider threats—exposures rising in frequency, sophistication, and cost.
- Leadership faced competing demands: deliver sustained financial performance, control costs, preserve uptime and product quality, and demonstrate cyber readiness to insurers, customers, and supply chain partners.

Pressure to act was mounting: Insurance premiums rose, self-assessments flagged concerning gaps, operational incidents nearly caused extended downtime, and the broader threat landscape for SMB manufacturers grew more perilous.

3. Choosing a New Path: Engaging 5SDS and Embracing Modern Security

PFI partnered with 5 Star Data Systems LLC (5SDS), an advisory and managed security services firm with deep roots in regional manufacturing, to chart a strategic path from "compliance minimums" to holistic cyber and operational risk management.

Engagement Scope

- **vCISO Service:** 5SDS embedded experienced security leadership at a fraction of the cost of a full-time executive, beginning with 10 hours per week for three months and a lighter ongoing retainer thereafter. The vCISO's mandate: bridge communication between business and technical teams, drive prioritized mitigation, and own compliance deliverables.
- **Technology Investment:** After a focused assessment, PFI invested in a proprietary Zero Trust Network Access (ZTNA) platform—delivering software-based ZTNA to 43 managed endpoints (PCs, Macs, cloud servers) and segmenting OT devices using low-cost hardware gateways (Raspberry Pi with managed switches) for air-gapped legacy machines.
- **Strategic Priorities:** Efforts were triaged to address the four highest priority risks: cloud misconfiguration, ransomware, phishing/social engineering, and insider threats/human error.
- **Control Spend:** A budget of $65,000 was established for control implementation, in addition to professional services and software costs.

Summary of Financial Outlay (Year 1)

- vCISO service: $45,000
- ZTNA platform: $17,720 (including OT hardware; ongoing annual software: $12,720)
- Targeted control investments: $65,000
- **Total cybersecurity investment:** $127,720

4. Methodology: Risk Reduction by "the Numbers"

PFI adopted a risk-based methodology underpinned by widely respected frameworks, including the NIST Cybersecurity Framework v2 and NIST SP 800-53. This approach enabled precise tracking of risk reduction, cost, and business impact:

Top Risks Identified (Before Control Implementation):

- Cloud misconfiguration (ALE: $28,000)
- Ransomware (ALE: $75,000)
- Phishing/social engineering (ALE: $50,000)
- Insider threats/human error (ALE: $27,000)
- **Total annual expected loss (ALE):** $178,000

After Mitigation via 5SDS & ZNTA software: Zero Trust implementation, continuous identity and device assessment, micro-segmentation, user training, and improvements in monitoring, detection, and incident response:

- New aggregate ALE: $66,700/year
- **Annualized risk savings:** $111,300 for just the top four risks

By using metrics such as the Annualized Rate of Occurrence (ARO) and controlled ALE for risk prioritization, PFI was able to target the most "dangerous and likely" events first, maximizing the return on every mitigation dollar.

Return on Investment (3-Year Net Present Value, 10% discount rate):

- Cumulative investment: $202,423
- ALE avoided: $281,760
- **Net ROI over 3 years:** 39%

5. Solution Highlights: What Made the Difference?

A. vCISO as Strategic, Scalable Security Leadership

- Delivered C-suite/board guidance, translating technical risk into operational and financial priorities.

- Owned compliance reporting, audit, and risk dashboards for DoD clients and insurance partners.
- Enabled flexibility: PFI could adjust the scope of services in response to changing threat or business conditions.

B. ZNTA Software: A Universal, Zero Trust Foundation

- Provided ZTNA for all modern endpoints (PC, Mac, Linux) and legacy OT/QA equipment using hardware gateways.
- Achieved network segmentation and lateral movement control—critical for manufacturing plants, where a single compromise can impact production lines and safety systems.
- Supported granular third-party/vendor access, satisfying customer and CMMC policy demands without increasing complexity or operational friction.
- Gave centralized, automated audit trails for compliance and insurance; eliminated vulnerabilities from lost or unmonitored connections.

C. People and Process

- Continuous, scenario-driven user training (phishing, social engineering, insider threat).
- Incident response plans and business continuity playbooks, tested and updated for real-world challenges (ransomware, supply chain breach, system outages).
- Risk register, policy library, and threat monitoring with plain-language reporting for operational leads and executives.

6. Comparative Analysis: Cybersecurity as Core Business Spend

Manufacturers routinely invest five or six figures annually on operational safety (OSHA), quality control (ISO 9001/9002), compliance, and preventive maintenance. Cyber and continuity risk spending with 5SDS was presented—and now viewed—no differently. Refusal to invest in foundational cyber or operational controls would be as risky as skipping safety, quality, or maintenance costs:

- OSHA compliance: $10,000/year

- Equipment safety & maintenance: $20,000/year
- Environmental: $12,000/year
- ISO 9001: $26,000 per 3 years
- CMMC Level 2 certification: $142,000–$150,000 (typical)
- ISO 27001: $60,000–$90,000 (initial, 2–3 year cycle)

PFI's case proved that cybersecurity has become a business continuity and growth discipline—not just a technical cost center.

7. Overcoming Leadership Objections

During the journey, PFI leadership surfaced key objections—mirroring those seen industry-wide:

- "We can't afford this." → Countered by comparing breach, downtime, or regulatory loss costs (often $100,000+) to risk reduction and insurance savings.
- "We already have AV/firewall." → Explained by modern threats bypassing perimeter-only defenses; Zero Trust and segmentation are now standards.
- "Too technical for us." → Delivered executive dashboards and C-suite briefings, focusing on operational and business outcomes.
- "No sensitive data means no risk." → Countered with ransomware prevalence, IP theft, and supply chain/third-party scenarios.

8. Expanding Beyond Compliance: NIST CSF and Continuous Maturity

While CMMC Level 2 (a $142,000+ investment) and insurance were the initial drivers, adopting NIST CSF v2 provided a complete, risk-based strategy encompassing confidentiality, integrity, and availability—the full CIA triad. This enabled:

- Proactive coverage of uptime, quality, and resilience risk—essential for manufacturing but not detailed in CMMC.
- Mapped business and technical controls to contracts, audit, and customer needs, reducing duplication and confusion.

- Supported future-readiness, adapting PFI's controls for regulatory, customer, or technology evolution.

9. Tangible Achievements and Business Outcomes

Risk Reduction:

- Annual cyber risk (ALE) dropped by 60%+ for the highest-priority exposures.
- Incident detection, response, and recovery capabilities became best-in-class for a firm of its size.

Audit and Compliance:

- Passed CMMC/NIST audits and insurance questionnaires with minimal friction.
- Maintained eligibility for sensitive contracts in defense, aerospace, and industrial sectors.

Financial Advantages:

- Cyber insurance premiums reduced 15–30% ($2,000–$3,000 annual savings).
- Quantifiable ROI for all cyber expenditures: Investment pays for itself in less than 15 months.
- Preserved and enhanced top-line revenue by securing business with high-demand customers.

Executive Confidence and Capacity:

- Leadership can report, with evidence, to the board, customers, and insurers that risk is under control and improving.
- Operational and IT teams are freed from "reactive firefighting," focusing on production, innovation, and core business growth.

10. Lessons Learned and Recommendations

- **Cyber resilience is not optional.** For modern manufacturers, the costs—with or without compliance and insurance—are comparable to those of any other core business protection program.

- **vCISO and Zero Trust are "right-sized" for SMBs.** You do not need Fortune 500 resources; flexible, expert partnerships and cloud-native controls deliver far greater business value at the correct scale.
- **Metrics drive investment.** Using ARO/ALE, NPV, and ROI connects security spending with what leaders care about: cash flow, business continuity, and growth.
- **Regulatory compliance is just a starting point.** True cyber maturity requires resilience, integrity, and operational uptime to be baked into every process.
- **Communication is as critical as technology.** Translating security outcomes into business terms ensures buy-in and continuous support.

Conclusion

PFI's partnership with 5SDS illustrates the new standard for manufacturing cybersecurity and risk management. By moving beyond "checkbox" compliance and embracing business-driven, continuous improvement, PFI achieved world-class resilience, operational confidence, and market advantage—without overextending its budgets or internal headcount. Their data-driven, transparent, and business-centric approach, which blends fractional executive leadership with advanced Zero Trust controls, stands as a blueprint for manufacturers navigating the digital industrial era. Manufacturers, boards, and business leaders seeking clear ROI from their security and compliance investments can draw actionable insights and measurable goals directly from PFI's journey.

Appendix A: Finance Calculations

The following are some deeper analyses of the estimated costs of PFI's proposed information security strategy in collaboration with 5SDS.

Cybersecurity Investment Overview (Year 1)

The table below details the year-one cost of the services and products PFI purchases from 5SDS.

Table 1: First Year Costs

Item	Cost ($)	Notes
vCISO Service (5SDS, fractional)	$45,000.	Month 1 – 3: 10 hours/week @ $150/hr. Month 4 – 12: 5 hours/week @ $150/hr.
Zero Trust Platform (SW/Endpoints)	$12,720.	53 endpoints (PC, Mac, Linux) at $20/mo. x 12 months
ZTNA for OT Devices HW SW	$5,000. $2,400.	10 devices @ $500 each (hardware, one-time) + $20/mo. per device (software)
Risk Mitigation Controls (Top 4 Risks)	$65,000.	Cloud config, ransomware, phishing, insider threat actions
Other Implementation Costs	$2,600.	Training, minor upgrades, admin.
Total (Year 1, all-in)	**$132,720.**	Includes labor, hard/soft costs, and prioritized controls

Note: Ongoing annual costs drop in Years 2+ as hardware is already deployed and integration costs are non-recurring; ongoing ZTNA software licensing, vCISO, and some controls persist.

Comparing Cyber-Risk ARO and ALE

Here is a detailed review of the changes in Annualized Rate of Occurrence (ARO) and Annualized Loss Expectancy (ALE) for PFI's top ten cyber risks—first before any dedicated cybersecurity investments, then after implementing core security controls (but before ZTNA software), and finally after layering in Zero Trust and segmentation controls.

Table 2: Cyber Risk ARO/ALE Across Three Scenarios

Risk	ARO Before	ALE Before ($)	ARO w/ Controls	ALE After Controls ($)	ARO w/ ZTNA	ALE After ZTNA ($)
Ransomware	0.5	75,000	0.15	22,500	0.07	7,500
Phishing	1.0	50,000	0.5	25,000	0.2	10,000

Risk	ARO Before	ALE Before ($)	ARO w/ Controls	ALE After Controls ($)	ARO w/ ZTNA	ALE After ZTNA ($)
Legacy Systems	0.7	42,000	0.28	16,800	0.1	4,200
OT Security Gaps	0.6	48,000	0.21	16,800	0.08	4,800
Supply Chain Attacks	0.4	16,000	0.16	6,400	0.08	3,200
Cloud Misconfiguration	0.8	28,000	0.24	8,400	0.10	3,500
Insider Threats/Human Error	0.9	27,000	0.36	10,800	0.18	5,400
Compliance Failures	0.3	6,000	0.09	1,800	0.05	1,000
Cyber Talent Shortage	0.7	17,500	0.14	3,500	0.07	1,800
AI/Deepfake Threats	0.3	4,500	0.12	1,800	0.06	900

PFI 2024 Financials

Below is a spreadsheet of PFI's 2024 financials, rounded to the nearest thousand dollars. Also included are the debt and cost of capital calculations.

Table 3: PFI 2024 Financials w/WACC

Line Item	Amount ($1,000)
Revenue	5,000
Cost of Goods Sold	3,100
Gross Profit	1,900
Operating Expenses	1,200
Operating Income	700
Interest Expense	40
Pre-Tax Income	660
Taxes (21%)	139
Net Income	521
Debt	900
After-tax cost (%)	6.3
Cost of capital (%)	11.8
Debt/Capital (%)	18/82
WACC	10.8
Gross Margin (%)	38

Appendix B: PYI's Top Ten Cyber Risks for 2025

For Plymouth Fabricators, Inc. (PFI), the top ten information security risks in 2025 align with those facing leading regional manufacturers. They are shaped by evolving technology, regulatory expectations, and threat actor tactics:

1. **Ransomware and Double Extortion Attacks**

   Modern ransomware not only encrypts data and halts production, but also exfiltrates sensitive information for extortion. Manufacturing remains a prime target due to high downtime costs and unique operational vulnerabilities[1][2][3].

2. **Phishing and AI-Powered Social Engineering**

   Attackers use increasingly sophisticated, AI-generated phishing emails and social engineering ploys—sometimes leveraging deepfake audio or video—to gain credentials or trick users, particularly those with network or financial privileges [2][4][5].

3. **Legacy Systems Vulnerabilities**

   Outdated OT (Operational Technology) and IT systems—often running unsupported operating systems—lack modern security controls and may use insecure protocols, exposing PFI to malware, unauthorized access, and supply chain attacks [6][1].

4. **Operational Technology (OT) Security Gaps**

   Weak segmentation and visibility across the IT/OT boundary mean that attacks targeting plant floor equipment or process controls (often exploiting protocol or integration weaknesses) can disrupt physical operations or cause safety incidents [6][3].

5. **Supply Chain Cyber Attacks**

   Third-party vendors and software suppliers present significant risk: attackers infiltrate less-secure partners to reach their ultimate target, with manufacturing's complex supply chains offering many points of entry [1][3][5].

6. **Cloud Misconfigurations and Shadow IT**

As PFI adopts more cloud solutions (e.g., ERP, remote work, file sharing) and remote access grows, misconfigured or unmonitored systems and “shadow IT” (unsanctioned technology) increase exposure, sometimes putting sensitive data at risk [6][2].

7. **Insider Threats and Human Error**

   Whether malicious or accidental, employee mistakes (e.g., mis-sending emails, falling for phishing scams, or violating security policies) remain a leading cause of security incidents—especially in rapidly changing environments with new technology tools [2][4].

8. **Regulatory Compliance Failures**

   Failure to comply with CMMC, NIST SP 800-171, state data regulations (such as 201 CMR 17), or sectoral requirements (PCI-DSS) can mean lost contracts, fines, and reputational risk—particularly for manufacturing businesses with complex regulatory environments [6].

9. **Lack of Skilled Cybersecurity Talent**

   A shortfall in skilled IT/OT security pros makes it harder to secure networks properly, manage vulnerabilities, and respond to incidents—especially where modern digital and legacy plant-floor tech intersect [6][2].

10. **Emerging Threats from AI and Deepfake Technology**

    AI-powered malware, automated attack tools, and deepfake social engineering (which involves impersonating executives or vendors) enhance the speed, scale, and believability of attacks, necessitating new detection, training, and verification strategies [4][5].

These risks require a layered defense: robust cyber hygiene, continuous user education, segmentation of IT/OT environments, active supply chain risk management, regulatory vigilance, and a proactive approach to monitoring new and emerging threats [6][1][2][3][4][5].

PFI's Top Ten Prioritized

To prioritize mitigation investments for PFI's top 10 information security risks, use a benefit-cost lens, focusing first on actions that deliver the most significant reduction in expected annual losses (ALE) for each dollar invested. Following is a methodical, data-driven approach based on your latest figures:

Step-by-Step Prioritization Approach

1. Calculate Benefit-Cost Ratio for Each Risk

- Divide the annual loss expectancy (ALE) reduction by the mitigation investment for each risk—higher ratios mean better risk-reduction value per dollar.

2. Sort and Invest by Benefit-Cost Ratio

- Address risks from highest to lowest benefit-cost ratio. This maximizes the "risk return" on each dollar spent—delivering rapid reductions in business exposure.

3. Refine with Strategic Context

- If risks have similar ratios, also consider raw ALE reduction (i.e., address absolute worst-case exposures, like ransomware, early), as well as any regulatory or operational imperatives.

Table 4: Ranked Mitigation Priorities

Priority	Risk	Investment ($K)	ALE Reduction ($)	Benefit-Cost Ratio
1	Cloud Misconfig.	10	19,600	1,960
2	Ransomware	30	52,500	1,750
3	Phishing	15	25,000	1,667
4	Insider Threats	10	16,200	1,620
5	Legacy Systems	20	25,200	1,260
6	OT Security Gaps	25	31,200	1,248
7	Cyber Talent Shortage	20	14,000	700
8	Supply Chain Attacks	15	9,600	640
9	Compliance Failures	15	4,200	280
10	AI/Deepfake Threats	10	2,700	270

Key Insights

- Risks like **cloud misconfiguration**, **ransomware**, **phishing**, and **insider threats** give PFI the best "risk bang for the buck"—they sharply lower annual expected losses for comparatively modest spend, and are also the most likely to be exploited or to cause production-stopping incidents.
- **Legacy and OT risk controls** are "next tier"—still robust returns, and critical when old equipment or unsegmented networks exist.
- Lower on the list, but not to be neglected, are longer-tail risks like compliance, emerging AI/deepfake threats, and the ongoing shortage of cybersecurity talent.
- This approach ensures PFI tackles its most damaging and likely risks first, justifies investments with clear financial analysis, and positions the company for scalable, cost-effective security improvement.

In summary

Prioritize actions with the highest ALE reduction per dollar—rapidly focusing resources where they'll make the biggest tangible impact on business risk and resilience. This not only protects operations and compliance standing, but also makes it easy to justify and track ROI to leadership with numbers, not just narratives.

Appendix B Citations

1. hxxps://socradar.io/major-cyber-attacks-manufacturing-industry-in-2025/
2. hxxps://blog.symquest.com/small-business-cybersecurity-threats
3. hxxps://www.forescout.com/blog/cybersecurity-in-manufacturing-threats-trends-and-preparation/
4. hxxps://onlinedegrees.sandiego.edu/top-cyber-security-threats/
5. hxxps://cloudsecurityalliance.org/blog/2025/01/14/the-emerging-cybersecurity-threats-in-2025-what-you-can-do-to-stay-ahead
6. hxxps://manufacturing-today.com/news/how-cyber-risk-is-reshaping-manufacturing-in-2025/

Appendix C: Sources for ARO and ALE

Here is a reference-supported explanation of how ARO (Annualized Rate of Occurrence) and ALE (Annualized Loss Expectancy) are defined, calculated, and typically modeled for top cyber risks in small manufacturing organizations, based on published sources and industry data.

1 – Understanding ARO and ALE

Annualized Rate of Occurrence (ARO):

- **Definition:** The expected frequency (probability) with which a specific risk, such as a cyberattack, is anticipated to occur each year. [1][2][3][4]
- **Calculation:** ARO = Number of incidents / Number of years. For example, if an event is expected once every two years, the ARO = 0.5. [5][1]

Annualized Loss Expectancy (ALE):

- **Definition:** ALE expresses the likely annual financial loss from a specific risk by factoring in both the probability (ARO) and the magnitude of a single loss event (SLE: Single Loss Expectancy). [6][7][8][5]
- **Calculation:** ALE = ARO × SLE.

  For instance, if a ransomware attack (SLE) incurs a $100,000 loss each time and is expected to occur once every 4 years (ARO = 0.25), then ALE = $100,000 × 0.25 = $25,000/year. [8][5]

2 – Industry Examples for Small Manufacturers

1. Ransomware

- **ARO:** Industry data for SMBs often estimates ransomware AROs between 0.1 and 0.5 (i.e., one attack every 2–10 years), but some sectors see higher rates. [9][10] Manufacturers can see AROs as high as 0.5 to 0.67!
- **SLE:** Ransomware can cause costs (including downtime, recovery, and ransoms) ranging from $25,000 to over $300,000 per incident for SMBs. [11][12]

- **ALE example:** If the SLE is $100,000 and the ARO is 0.3, ALE = $30,000 annually. For reference, one study found an SMB experiencing a ransomware-related ALE of $150,000 when the SLE was $300,000 and the ARO was 0.5. [13]

2. Phishing

- **ARO:** Phishing is reported as a widespread risk, with estimates for SMBs ranging from several times per year (ARO = 1.0) to even higher depending on exposure and lack of training. [10]
- **SLE:** Phishing SLEs can vary widely ($10,000 to $50,000 typical), accounting for direct fraud, business email compromise, and incident recovery. [9] [10]
- **ALE example:** If SLE is $25,000 and ARO is 0.5, then ALE = $12,500/year. Organizations that improve training and filtering often reduce ARO by half, which is reflected in the corresponding decrease in ALE. [9]

3. Legacy Systems/OT Risks

- **ARO:** OT/legacy risks can be less frequent (ARO = 0.1–0.3/year) but have severe potential SLEs if exploited, given operational and safety impacts, with SLEs in the tens of thousands of dollars or more. [1] [4]
- **ALE example:** SLE of $42,000 × ARO of 0.2 = $8,400/year.

4. Risk Reduction with Controls

Implementing controls (training, MFA, EDR, segmentation) is documented to lower ARO significantly, often by 50% or more, depending on control strength and coverage. For example: [14] [9]

- **Before controls:** Ransomware may have an ARO of 0.5 (every two years).
- **After controls:** ARO can drop to 0.1–0.2. ALE accordingly drops: e.g., from $75,000/year to $12,000–$15,000/year. [13] [8] [9]

Zero Trust and advanced network segmentation (such as that offered by products like ZTNA software) further decrease ARO by restricting attacker movement and automating rapid response, often reducing both the likelihood and expected losses of lateral-moving threats. [15]

3 – Quantitative Risk Modeling Frameworks

- **NIST SP 800-30** and the **FAIR Model** provide widely accepted quantitative frameworks for risk assessment: NIST focuses on identifying likelihood and impact, while FAIR breaks down loss frequency and magnitude—both recommend estimating risks using empirical data when available, and expert analysis when not. [16] [17] [18] [15]
- FAIR and NIST methodologies are routinely used to model ARO and ALE in dollar terms, assisting organizations in justifying security investments based on expected financial benefit. [18] [16] [15]

4 – Industry Benchmarks

- Small manufacturers spend between $25,000 and $3 million per major cyber incident, with the typical range for most SMBs closer to $50,000–$150,000 per event. [12] [11] [10]
- For the top risks (ransomware, phishing, OT compromise, supply chain, etc.), the frequency and impact assumptions cited in your tables are squarely within these industry-reported ranges. [11] [10] [13] [9]

5 – In summary

- The ARO and ALE figures presented for common manufacturing cyber risks are grounded in accepted industry methodologies (NIST, FAIR), with typical values and calculations supported by published benchmarks, risk modeling guides, and empirical incident data.
- This quantification approach enables justifiable risk reduction ROI and is recommended by cybersecurity frameworks and the insurance industry for SMB cyber investment decisions. [6] [15] [8] [18] [9]

Appendix C Citations

1. hxxps://www.sangfor.com/glossary/cybersecurity/what-is-annualized-rate-occurrence
2. hxxps://www.riskythinking.com/glossary/annualized_rate_of_occurrence
3. hxxps://thorteaches.com/glossary/annualized-rate-of-occurrence-aro/

4. hxxps://www.becker.com/accounting-terms/annualized-rate-occurrence-aro
5. hxxps://www.itsecurityguru.org/2015/06/10/risk-analysis-how-to/
6. hxxps://tiomarkets.com/en/article/annualized-loss-expectancy-guide
7. hxxps://www.sciencedirect.com/topics/computer-science/single-loss-expectancy
8. hxxps://en.wikipedia.org/wiki/Annualized_loss_expectancy
9. hxxps://tolumichael.com/what-is-ale-in-cyber-security/
10. hxxps://www.bdemerson.com/article/small-business-cybersecurity-statistics
11. hxxps://blog.techheads.com/the-cost-of-a-cyberattack-to-small-and-medium-businesses-smbs
12. hxxps://travasecurity.com/learn-with-trava/blog/what-is-the-average-cost-per-cyber-attack/
13. hxxps://tolumichael.com/annual-loss-expectancy-cybersecurity/
14. hxxps://www.cyberdefensemagazine.com/small-manufacturers-big-target-the-growing-cyber-threat-and-how-to-defend-against-it/
15. hxxps://www.balbix.com/insights/fair-model-for-risk-quantification-pros-and-cons/
16. hxxps://www.cybersaint.io/blog/selecting-the-right-cyber-risk-quantification-model
17. hxxps://www.scrut.io/post/how-to-select-the-right-cyber-risk-quantification-method
18. hxxps://www.logicgate.com/blog/the-fair-model-an-objective-approach-to-risk-measurement/
19. hxxps://5sds.com/compliance-consulting-1
20. hxxps://hazards.fema.gov/nri/annualized-frequency
21. hxxps://secureframe.com/blog/risk-analysis-calculation