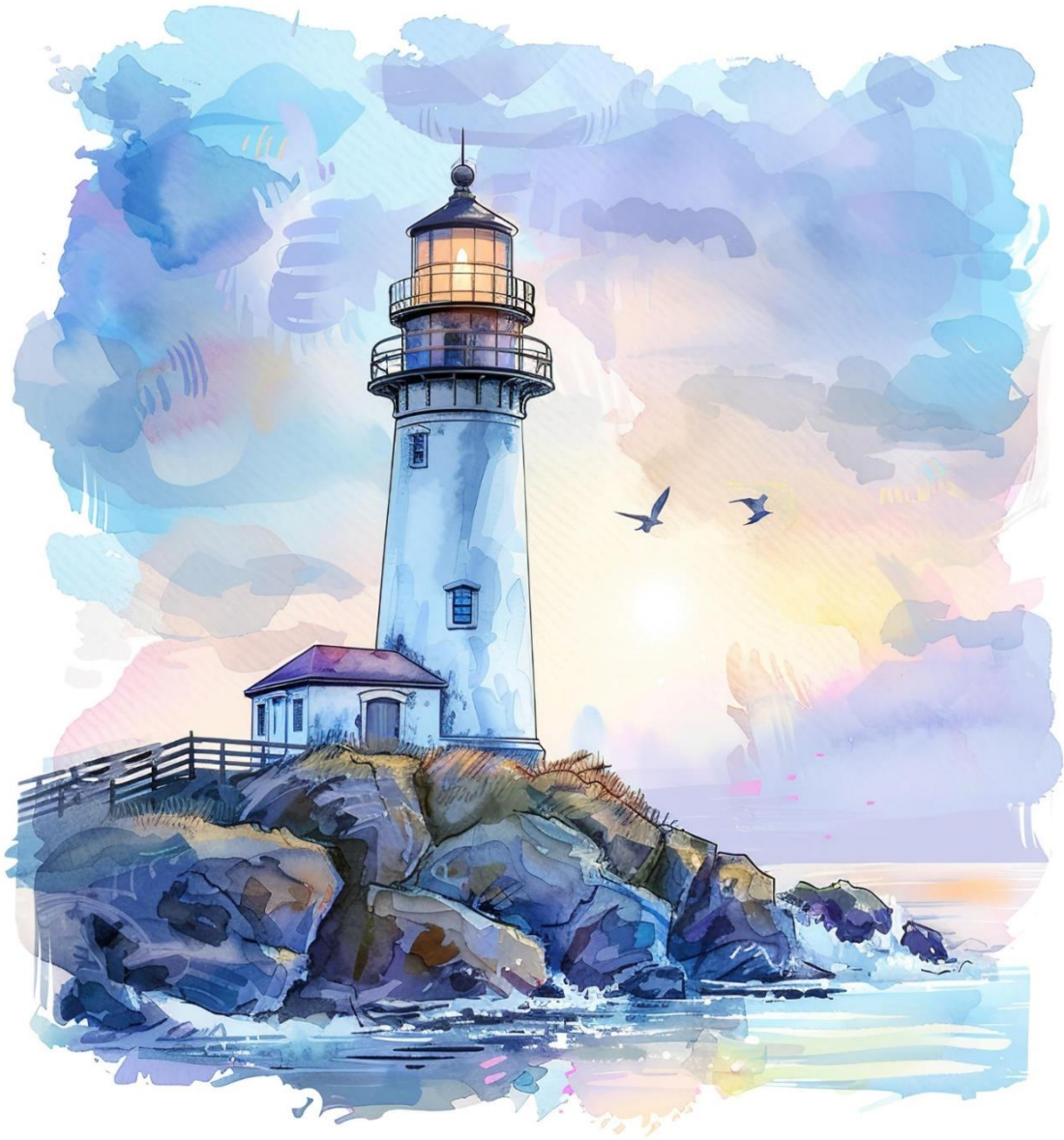
Practical Cyber Resilience

A 2025 Survival Guide for Small Manufacturers



Randolph L. Nethers

THIS PAGE IS BLANK

Copyright Page

Practical Cyber Resilience: A 2025 Survival Guide for Small Manufacturers

First Edition – 2025

Published by 5 Star Data Systems, LLC

Keene, New Hampshire, United States

5sds.com

This publication is intended for educational and informational purposes only. While every effort has been made to ensure accuracy, 5 Star Data Systems, LLC assumes no responsibility for errors, omissions, or damages resulting from the use of this material. Readers should consult professional or legal advisors before making business or compliance decisions based on the information contained herein.

ISBN: (TBD)

Printed and bound in the United States of America.

21 10 2025

Credits and Acknowledgments

This publication reflects the collective experience, insight, and dedication of professionals dedicated to enhancing cybersecurity resilience throughout the American manufacturing sector.

Special thanks go to the clients, partners, and industry peers who shared their real-world challenges and successes, helping to make this guide practical and realistic. Their contributions, whether direct or through collaboration, shaped the lessons and best practices shared in these pages.

Additional thanks to the following resources and foundations that guided this work:

- The National Institute of Standards and Technology (NIST) for its industry-defining cybersecurity frameworks.
- The U.S. Department of Defense and the Cybersecurity Maturity Model Certification (CMMC) Accreditation Body for their leadership in strengthening supply chain security.
- The broader cybersecurity community, whose commitment to education, transparency, and shared defense continues to raise the bar for resilience across industries.

This work was developed, edited, and produced by 5 Star Data Systems, LLC, with strategic and editorial guidance provided by Randolph L. Nethers. Graphic and layout support were guided by the 5SDS digital branding and marketing framework established in 2025.

Every effort has been made to ensure the accuracy and clarity of this work. Any errors or omissions are unintentional, and readers are encouraged to contact 5 Star Data Systems, LLC via 5sds.com for corrections or feedback. The company takes no responsibility for any actions the reader might take because of errors found in this publication—*caveat emptor*.

This book is dedicated to small and mid-sized manufacturers who keep building, innovating, and securing the future of American industry—one resilient decision at a time.

Preface

"Resilience is not built in a day—it's practiced, refined, and earned through preparation."

In today's manufacturing landscape, success is measured not only by productivity or innovation but also by the ability to **adapt and stay secure**. Digital transformation has connected factory floors, suppliers, and customers in new ways—yet that same connection has created hidden risks.

Practical Cyber Resilience: A 2025 Survival Guide for Small Manufacturers was designed to help business leaders, operations managers, and IT teams confidently navigate this new landscape. It provides a roadmap based on practical actions—simple, achievable steps that safeguard not only systems but also reputations and livelihoods.

The following chapters develop much like a resilient organization: starting with awareness and training, then moving through planning, governance, and continuous improvement. Throughout, readers will find strategies based on real-world experience, guidance on regulatory frameworks like NIST and CMMC, and insights into how leadership—particularly through scalable vCISO models—can sustain security over time.

This book was written for manufacturers who believe that cybersecurity should enhance, not hinder, their business. It is a guide for those ready to move beyond fear of compliance toward confidence in control; for those who recognize that safeguarding what you build is just as vital as building it.

May it inspire you to see resilience not as a cost, but as an investment in growth, trust, and your enterprise's long-term future.

Randolph L. Nethers
Founder, 5 Star Data Systems, LLC
5sds.com

Table of Contents

Table of Tables

Chapter 1

The Problem

Introduction

We are a quarter-century into the 21st century. Every day, the digital transformation that began decades ago becomes more widespread. While the rise of computers and digital methods in business and manufacturing has greatly improved efficiency and performance, it has also introduced new risks that didn't exist before. This report solely uses documented market and industry analysis to explain how SMB manufacturers are being targeted, identify the most common attack types, and outline the real-world consequences across downtime, operations, finances, and reputation. It also provides strategies to address the issue and significantly reduce risks to the business and supply chain.

Small and mid-sized manufacturers (SMBs) are at the heart of a rapidly changing cyber threat landscape. As digital transformation speeds up across the industry, manufacturers—regardless of size—are increasingly targeted by cybercriminals looking to exploit operational dependencies, supply chain complexities, and often limited cybersecurity resources. In 2025, manufacturers remain the top target for ransomware attacks globally, with the United States experiencing more than half of all attacks on the sector worldwide. Ransomware and other threats jeopardize their operations, financial stability, and reputation.

Many SMB manufacturers have minimal IT staff, often relying on one knowledgeable person to oversee both production and digital systems, which creates a vulnerability. This weakness has made SMB manufacturers easy targets for attackers seeking maximum disruption and profit with minimal effort. The threat not only affects SMBs but also those downstream in the supply chain. It is especially critical for companies serving defense, medical, and regulated markets, as these sectors make them appealing targets for sophisticated and opportunistic adversaries.

This chapter explores why manufacturers are so vulnerable, the most common threats they face, and the real-world consequences of cyber incidents.

Common Attacks

There are many forms of cyberattacks waged against SMBs. The table below lists seven of the most common types of attacks, their share of the total, and their impact, cost, or effect.

Table 1: Common Cyber Attacks against SMBs

Attack Type	Share of Breaches	Typical Impact	Average Cost/Effect
Ransomware	47%	Production halt, data lockdown (loss)	$200,000 per breach, 24 days avg. downtime, 62% pay ransom
Phishing/Social Engineering	22%	Credential theft, malware infection	$6,000–$150,000 per event, hundreds of incidents per 1,000 users each year
Exploitation of Vulnerabilities	20–30%	Network intrusion, lateral movement	Can mirror the cost of a data breach
Data Exfiltration/IP Theft	~20%	IP and proprietary data loss	$180,000+ per event
Supply Chain/Third-Party Attacks	20%	Multiple site compromise	$120,000+ per event, 431% rise since 2021
Insider Threats	10%	Internal sabotage, data leakage	$40,000+ per incident
Denial of Service (DoS/DDoS)	12%	Service outages, operational loss	$48,000+ per incident

Ransomware remains the biggest threat, causing direct business disruptions and often leading to "double extortion"—where data is both encrypted and stolen, increasing risks for victims who depend on supply chain trust and regulatory compliance. Phishing and social engineering support many other attacks and target the human element, which continues to be the primary source of breaches. Exploitation of unpatched devices, lateral movement between Information Technology (IT) and Operational Technology (OT) networks, and weak remote access security are also common problems.

Supply chain and third-party exploitation have increased as attackers target weaker links like vendors and software providers to breach interconnected SMB networks. Data theft, especially of proprietary product designs or personally identifiable client or customer information, is a growing concern due to regulatory fines and lasting reputational damage.

Ransomware

Ransomware remains the biggest threat to manufacturers. According to the Black Kite 2025 Manufacturing Report, manufacturing accounted for nearly a quarter (22%) of all

publicly reported ransomware attacks from April 2024 to March 2025, surpassing other industries. The U.S. alone represented 52% of all attacks on the global manufacturing supply chain. Ransomware groups are not only targeting large companies but are also increasingly focusing on smaller manufacturers, recognizing their vital role in supply chains and their limited ability to recover quickly.

- **Attack Distribution:** Attacks are widespread across sub-industries, with machinery manufacturing (13%), fabricated metal product manufacturing (12%), and food and beverage manufacturing (11%) being the most frequently targeted (Industrial Cyber. (2025).
- **Financial Impact:** The economic effects are considerable. The average cost of a data breach for small to mid-sized businesses (SMBs) exceeds $2.2 million annually, with expenses expected to rise by 15% over the next five years. For many, even a single incident can threaten their business viability (Alahmaei, Ahmed & Rahman, 2025).
- **Downtime:** Production stoppages can last for days or weeks, leading to missed orders, lost revenue, and damage to reputation. In some cases, 60% of small businesses that experience a cyberattack shut down within six months (Alahmaei, Ahmed & Rahman, 2025).

Ransomware attacks disrupt business operations and are often followed by "double extortion," where data is both encrypted and stolen, increasing the pressure on victims who rely on supply chain trust and regulatory compliance.

Phishing, BEC & Social Engineering

Phishing is a type of social engineering where attackers send deceptive emails, messages, or websites to trick individuals into revealing sensitive information or taking risky actions—such as clicking malicious links or downloading malware. These emails often appear to come from trusted sources, like a supervisor or a known vendor, and may create a sense of urgency or fear to prompt quick responses. Most malicious emails—including spam, phishing, and malware—target companies with fewer than 250 employees. Attackers are increasingly using advanced tactics, such as impersonating trusted suppliers or sending fake invoices or spreadsheets, to deceive employees into revealing credentials or making unauthorized transactions.

Business Email Compromise (BEC) is a more targeted and sophisticated form of phishing. In BEC attacks, cybercriminals impersonate executives, vendors, or other trusted

contacts—often using compromised or spoofed email accounts—to trick employees into transferring funds or sharing sensitive information. Unlike typical phishing, BEC emails might not show obvious red flags like attachments or links, making them harder to detect. Attackers often imitate the tone and style of the person they are impersonating and may spend days or weeks building trust before making their fraudulent request.

Phishing and BEC are both forms of social engineering that involve manipulating people to reveal confidential information or perform actions that compromise security. Other common social engineering techniques include:

- **Pretexting:** Fabricating a scenario to gather information (e.g., pretending to be IT support).
- **Baiting:** Offering something tempting, like free software, to trick users into downloading malware. It might also involve leaving media, such as a USB drive, for someone to pick up and use, or mailing the same type of media.
- **Tailgating:** Following someone into a secure area without authorization.
- **Quid pro quo:** Offering a service or benefit in exchange for information.

All these attacks exploit human trust and behavior, making security awareness training and strong verification processes essential defenses.

Exploitation of Vulnerabilities

Exploiting vulnerabilities is a main tactic in cyberattacks targeting manufacturers and other organizations. A vulnerability is a flaw in software, hardware, or network setups that hackers can exploit to gain unauthorized access, install malware, or cause disruptions. In 2025, the number of newly reported vulnerabilities (Common Vulnerabilities and Exposures, or CVEs) hit record highs, with over 21,500 disclosed just in the first half of the year—an 18% increase from the previous year.

Attackers often quickly exploit these weaknesses, especially those rated as high or critical risk. Many vulnerable flaws do not require authentication and often enable remote code execution (RCE), which allows attackers to run malicious code remotely. Common targets include Microsoft products, edge-security devices like SSL-VPNs, and web applications with issues such as cross-site scripting or SQL injection.

Exploitation can occur before a patch is available (zero-day attacks) or after a fix is issued but not yet implemented (day-one or one-day attacks). The fast pace at which threat actors exploit new vulnerabilities makes timely patching and continuous vulnerability

management essential for defense. For manufacturers, unpatched legacy systems and exposed network devices often serve as entry points, making vulnerability exploitation a persistent and serious threat.

Data Exfiltration & Intellectual Property (IP) Theft

Data exfiltration is the unauthorized transfer of sensitive information from a company's network to an attacker-controlled external location. By 2025, data exfiltration has become a major part of modern cyberattacks, with 96% of all reported ransomware cases involving some form of data theft—the highest level ever recorded. For manufacturers, the stakes are extremely high: attackers target not only customer or employee data but also proprietary designs, formulas, and trade secrets vital to industrial competitiveness. The danger of losing such sensitive data cannot be overstated. Losing DoD-related data jeopardizes national security. Information related to medical devices could enable attackers to exploit weaknesses, steal patient data, or cause harm.

Intellectual property (IP) theft is a specific type of data theft focused on stealing blueprints, source code, manufacturing methods, or other confidential knowledge. Both state-sponsored groups and cybercriminals have carried out large-scale operations to steal trillions of dollars' worth of IP from manufacturers, energy firms, and pharmaceutical companies. For instance, Operation CuckooBees, linked to the Chinese state actor APT 41, extracted hundreds of gigabytes of blueprints, diagrams, and proprietary information from numerous multinational manufacturing firms over several years—often without being detected.

How does data exfiltration happen? Attackers may use malware, stolen credentials, or misconfigured cloud storage to access and steal data. Sometimes, insiders or third-party contractors are responsible. For example, in the 2025 Coinbase breach, overseas support staff leaked sensitive customer information, leading to a $20 million extortion attempt. Other times, attackers exploit vulnerabilities in public-facing applications or remote access tools to gain persistent access and secretly siphon data over weeks or months.

Business Impact: The effects of data exfiltration and IP theft are severe. Besides immediate financial losses and potential extortion demands, companies face long-term harm to their competitiveness, legal issues, and reputation. For manufacturers, stealing unpatented designs or production secrets can lead to counterfeit products, loss of market share, and the erosion of years of research and investment.

In today's threat landscape, data exfiltration and IP theft are not just side effects of cyberattacks; they are often the main objectives. Manufacturers must prioritize data protection, monitor for unusual data transfers, and secure both their digital and physical intellectual property to defend against these increasingly sophisticated threats.

Supply Chain Attacks

Supply chain and third-party cyberattacks have become some of the biggest challenges facing small manufacturers in 2025. As manufacturers digitize their processes and broaden their supplier networks, the risk of supply chain attacks increases. Cybercriminals take advantage of vulnerabilities in third-party systems to access sensitive data or disrupt operations, and they will exploit the relationships between suppliers, service vendors, and partners. The connected nature of manufacturing means that a breach in one part can quickly spread, affecting multiple organizations.

Once seen as an issue only for large companies, supply chain attacks now threaten every part of the production network. Small businesses depend heavily on many vendors—software providers, logistics firms, outsourced IT managers, and parts suppliers—creating thousands of digital and operational links. Each of these links is a possible entry for a cyber attacker. Often, attackers don't target the manufacturer directly. Instead, they compromise a trusted supplier or service provider and use that relationship to break into the manufacturer's network.

Recent studies show that incidents involving the supply chain and third parties have increased by over 430% since 2021, making up about one in five breaches in the sector. The average cost per incident is around $120,000 for small manufacturing companies, though this estimate often doesn't account for the full operational and reputational harm. Attackers take advantage of poorly secured vendor portals, shared credentials, or upstream software dependencies to deploy malware, steal credentials, or alter production data. For smaller companies, the impact can be devastating—disrupting production lines, stopping shipments, and eroding customer trust in the company's reliability.

What makes these attacks uniquely difficult to manage is the limited visibility manufacturers have into their extended digital ecosystem. Vendors often resist audits, small companies rarely impose strict cybersecurity contracts, and existing monitoring solutions typically stop at the company's internal perimeter. This gap allows attackers to embed themselves in suppliers' systems undetected, sometimes for months. When they finally activate

their payload—such as ransomware or digital sabotage—the damage ripples through the entire supply chain, affecting multiple organizations simultaneously.

To build resilience against third-party cyber risks, small manufacturers need to do more than just protect their own systems. They should start evaluating everyone they collaborate with—suppliers, service vendors, and partners. A good first step is to ask questions about how vendors handle cybersecurity and if they follow recognized standards such as the Department of Defense's CMMC/NIST requirements, ISO 27001, or the Center for Internet Security (CIS) controls. Instead of assuming partners are secure, companies can request proof of safeguards. Look for employee training, updated software, and secure data practices. Using tools that continuously monitor for unusual activity—such as unexpected data transfers or login attempts—adds an extra layer of security. Manufacturers should also limit vendor system access, implement deliberate network segmentation, and verify that each network connection is legitimate. By taking these proactive yet simple steps, small companies can significantly reduce the risk of hackers slipping in through a trusted supplier.

Ultimately, cyber resilience in the supply chain is about balancing trust with verification. Manufacturers who maintain real-time oversight of digital relationships and proactively enforce security standards among vendors not only reduce direct exposure but also strengthen the collective resilience of the entire production network. The interconnected nature of modern manufacturing means that a single weak link can trigger a widespread operational crisis—but a well-secured ecosystem can serve as a shield for all participants.

Insider Threats

Insider threats are one of the most underestimated cybersecurity risks in small and midsize manufacturing environments. Though they account for only about 10% of reported breaches, they can be especially damaging because the perpetrators already have legitimate access to systems and data. Insider threats happen when employees, contractors, or business partners misuse their access, whether intentionally or accidentally, to harm operations, leak information, or enable other types of attacks. These incidents usually cost around $40,000 each, but their ability to expose sensitive intellectual property or disrupt production can cause far greater damage.

Unlike external attackers who breach networks from outside, insiders operate from within trusted environments. Some insider threats are malicious, such as disgruntled employees sabotaging production systems or stealing proprietary designs before leaving a

company. Others are non-malicious, caused by human error—such as employees clicking on phishing emails, using weak passwords, or mishandling confidential files. Vendors or contractors can also become insider risks if they retain unnecessary access or fail to follow proper cybersecurity practices. Because insider actions often seem legitimate, detecting these threats can take months, and evidence might only surface after significant damage has occurred.

In the manufacturing industry, insider threats pose a significant challenge because factory networks are increasingly connected with enterprise IT systems. Engineers, maintenance staff, and quality assurance teams often access production data or equipment programming interfaces remotely. This convenience improves efficiency but also raises the risk of accidental misuse or intentional tampering. For example, an employee could accidentally introduce malware via a USB device used for machine diagnostics, or a former contractor might still have credentials that allow remote access to control systems. The range of potential scenarios is broad.

To reduce these risks, manufacturers must cultivate a culture of awareness and implement practical controls that balance security with productivity. Access should be provided only on a "need-to-know" basis, with regular account reviews to ensure that former employees or vendors lose access immediately. Monitoring tools that detect unusual activity—such as large data downloads or access from unexpected locations—can identify problems early without disrupting everyday work. Equally important, leadership should promote open communication and support employees who report security concerns.

Ultimately, insider threat protection depends just as much on people as on technology. Proper training, clear policies, and a culture of accountability can transform employees into allies instead of threats. In a sector where operational continuity is as vital as data security, managing insider threats is essential to achieving true cyber resilience.

Denial of Service

Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks remain persistent and dangerous threats to manufacturing companies in 2025. These attacks flood a company's servers, networks, or online services with large amounts of traffic or repeated requests, causing them to slow down or crash completely. In more serious cases—especially with DDoS attacks—the malicious traffic is spread across thousands of compromised systems worldwide, making it much harder to block or trace.

Within the manufacturing sector, a DoS or DDoS attack can quickly disrupt operational processes. Many production facilities depend on internet-connected systems for inventory management, order fulfillment, logistics coordination, and remote equipment monitoring. When these services go offline, even briefly, it can cause halted production, delayed shipments, and lost business. Denial-of-service incidents make up about 12% of reported attacks, with an average financial impact of around $48,000 per event. For small to midsize manufacturers, this could mean several days of disrupted operations, leading to immediate revenue losses and damage to reputation with customers or partners.

What makes these attacks especially difficult is that they often act as diversions for other intrusions. While IT teams work on restoring network connectivity, attackers can exploit system weaknesses or introduce malware elsewhere in the environment. Some DDoS extortion schemes even threaten to cause more outages unless the company pays a ransom.

To strengthen defenses, manufacturers should collaborate with internet service providers (ISPs) and cybersecurity partners to implement layered protections such as traffic filtering, content delivery networks, and rate limiting. Regular network stress tests and incident response exercises can also help ensure readiness for high-traffic events. Beyond technology, the key is preparation—maintaining continuity through backups, alternative communication channels, and offline capabilities. For resource-constrained manufacturers, outsourcing DDoS mitigation to a managed security service may be the most cost-effective way to protect uptime and uphold customer trust amid these increasingly sophisticated disruptions.

Other Concerns

Seven attack types are listed in Table 1 above, but there are additional issues worth discussing that also contribute to the attacks already covered.

Legacy System Vulnerabilities

Many manufacturers depend on outdated systems that lack modern security controls and are hard to update. These systems are prime targets for hackers, providing attackers with an entry point to explore the network further. Legacy systems—especially those running old operating systems like Windows XP, 7, or early versions of Windows 10—remain a significant cybersecurity and operational challenge for small and midsize manufacturers (SMBs). Many production environments still rely on these older systems to control machine operations, programmable logic controllers (PLCs), quality control software and hardware, or specialized

applications that vendors no longer support. While these systems may still function, their age creates serious vulnerabilities that modern attackers are quick to exploit.

The main problem is that legacy operating systems no longer get regular security updates. For example, Microsoft stopped extended support for Windows 7 in 2020 and for Windows 8.1 in early 2023, leaving millions of machines without official patches for new vulnerabilities. This creates a dangerous environment where common exploits—such as ransomware or remote code execution—can easily bypass outdated defenses. Also, older systems are often incompatible with modern endpoint protection or multifactor authentication solutions, which limits options for securing them without disrupting operations.

For manufacturers, risks go beyond cybersecurity. Legacy systems often use outdated hardware interfaces or cannot connect with newer data platforms and automation technologies, making it challenging to modernize production or implement Industry 4.0 tools. Older software may also rely on unsupported drivers or network protocols, which can cause unpredictable performance issues and compatibility problems when connected to newer devices.

The best approach for SMBs is to start with a phased modernization plan. Critical legacy systems that cannot be replaced right away should be isolated from the main network and protected by firewalls and strict access controls. Even better, they should be "air gapped," meaning they have no direct connection to any other network. Virtualization and network segmentation can also help run old software in secure "sandbox" environments while keeping daily operations running smoothly. When possible, upgrading to current operating systems and using cloud-managed tools not only reduces vulnerabilities but also improves flexibility, compliance, and long-term competitiveness in a digital manufacturing future.

Emerging Threats: Deepfakes and Social Engineering

Cybercriminals increasingly use advanced AI tools combined with proven manipulation tactics to trick targets and gain unauthorized access. One rapidly growing example is deepfakes—AI-generated audio or videos that convincingly imitate voices or faces—to impersonate executives, suppliers, or business partners. Attackers use these fakes to request fund transfers, reveal trade secrets, or approve changes to organizational accounts. What once needed significant technical skill can now be produced with publicly available AI tools, making this threat highly accessible and very hard to detect.

Social engineering, the broader category that includes deepfakes, remains one of the most effective ways to breach an organization's defenses. Instead of exploiting software vulnerabilities, attackers manipulate human trust. The 2023 MGM Resorts breach is a clear example: hackers pretended to be IT support staff to gain administrator access. Similar methods are now targeting manufacturing companies, where attackers impersonate suppliers, send fake invoices, or manipulate procurement communications to divert payments or install malware-laden files.

For small and mid-sized manufacturers with limited cybersecurity training and resources, these attacks are especially dangerous. Employees who infrequently question requests from "executives" or long-time vendors can easily become unwitting participants in a cyber incident.

The best defense is awareness and verification. Regular security training should include real-world examples of deepfakes and social manipulation. Staff should be encouraged to double-check unusual requests—especially those involving financial changes or sensitive data—through an independent channel, not just email or text. Creating a culture where people feel comfortable slowing down and verifying legitimacy is one of the most effective ways to outsmart even the most sophisticated AI-driven scams.

Real-world Examples

Visser Precision (2019)

In April 2019, Denver-based manufacturer Visser Precision became a victim of DoppelPaymer ransomware, marking one of the earliest high-profile cases of double extortion attacks in the manufacturing industry. The attackers infiltrated the company's network, stole confidential files, and encrypted critical systems before demanding a ransom. What made this incident particularly troubling was the sensitive nature of the stolen data—confidential nondisclosure agreements (NDAs), schematics, and production details from clients such as Tesla, SpaceX, and Lockheed Martin. When Visser refused to pay, the attackers leaked parts of the stolen files on dark web forums, including blueprints related to aerospace and defense components.

Although production continued, downstream partners had to initiate emergency containment measures, data protection, and contract reviews to assess their own risks. Visser Precision experienced immediate reputational and operational setbacks, with financial damages likely reaching six figures and ripple effects extending to customers. The incident

showed how a single vendor breach can spread throughout a complex manufacturing supply chain, greatly amplifying the overall impact beyond the initial target. For small and mid-sized manufacturers, the Visser breach highlights the need for third-party risk assessments, continuous system monitoring, and secure data-sharing practices to prevent attackers from exploiting the weakest links in an interconnected production network.

Mondelez (2017)

In June 2017, global food manufacturer Mondelez International—famous for brands like Oreo and Cadbury—was hit by the NotPetya malware. The cyberattack quickly spread across hundreds of multinational networks. Initially disguised as ransomware, NotPetya was later identified as a state-sponsored wiper aimed at permanently erasing data rather than demanding payment. Within hours, the malware encrypted over 1,500 servers and 20,000 laptops, disrupting Mondelez's logistics, manufacturing, and shipping operations worldwide. Many factories went offline, customer orders were delayed, and global supply chains broke down as the company worked to restore basic functions.

Recovery efforts cost over $100 million, not including lost sales and operational delays. NotPetya's impact went beyond direct financial loss—it revealed how even large corporations with advanced IT systems can be severely affected by a single malware incident. The attack also established a precedent for cyber insurance disputes, with insurers claiming that state-sponsored attacks are "acts of war" and therefore not covered. The Mondelez case highlights a crucial lesson: strong cybersecurity requires not only layered technical defenses but also financial resilience plans and incident response strategies capable of handling global-scale digital disruptions.

•••

The Visser Precision and Mondelez incidents illustrate how attack types listed in Table 1—especially ransomware, data theft, and supply chain breaches—can cause damage well beyond an organization's network. Both incidents stemmed from different motives and scales: Visser's ransomware attack involved data theft and extortion, while Mondelez was targeted by a destructive malware campaign disguised as ransomware. In each case, production disruption, financial losses, and reputational harm extended to interconnected stakeholders.

For small and midsized manufacturers (SMBs), these examples highlight two key lessons. First, even small-scale attacks can disrupt relationships within a supply chain, damaging trust with partners and customers who rely on confidentiality and operational

uptime. Second, high-profile cases show that sophisticated tools previously used by multinationals are now accessible to low-cost attackers targeting smaller companies. The same vulnerabilities—unpatched systems, limited monitoring, and weak vendor oversight—exist across nearly all manufacturing sizes.

In today's interconnected industrial landscape, resilience relies on more than just antivirus tools or backups. SMB manufacturers must adopt layered controls, conduct regular risk assessments, and ensure their suppliers meet minimum cybersecurity standards. Proactive defense planning shifts cybersecurity from merely an IT expense to an operational safeguard, reducing the chance that a single breach will spread throughout the entire production system.

The Impacts

Cyberattacks don't just steal data or disable machines—they impact every aspect of a manufacturer's operations. A ransomware attack can lead to missed shipments, halted orders, and restless nights wondering what will happen next. Even after operations resume, the long-term damage to customer trust and vendor relationships can be more difficult to repair than the systems themselves. For many small manufacturers, the shock of a major incident reveals a harsh reality: the digital risks they face are as serious as any mechanical failure on the shop floor. To truly understand what's at stake, we need to examine how everyday tools, connections, and decisions have quietly expanded the modern attack surface.

Why Are Small Manufacturers So Vulnerable?

Complex and Expanding Attack Surface

Modern small manufacturing environments usually combine legacy operational technology (OT), such as programmable logic controllers and industrial equipment, with new information technology (IT) systems for business management, cloud access, and remote monitoring. While this digital transformation enhances efficiency and enables data-driven decision-making, it also significantly increases the number of entry points and pathways for cyber attackers. Older machines with outdated software are rarely updated and often lack strong protections, while Internet-of-Things (IoT, also called "smart") devices or exposed cloud services are sometimes deployed without thorough security reviews. These vulnerabilities allow attackers to move laterally: a breach in the office network can quickly spread to production lines or vice versa, resulting in costly downtime and potential physical damage.

Tight Security Budgets and Lean Staffing

Unlike large companies, small manufacturers often have limited IT staff and cybersecurity budgets. Resource constraints remain a significant challenge for these smaller manufacturers. According to NIST and industry surveys, many SMBs have little or no dedicated cybersecurity personnel and operate with tight IT budgets. As a result, basic controls like regular software patching, network segmentation, backup testing, and incident response planning are often missing or incomplete. Security awareness training is irregular, making employees more vulnerable to phishing or social engineering scams. When an incident occurs, the response is usually slower and less coordinated, increasing both the damage and costs to the company. A recent study shows that 94% of SMBs faced at least one cyberattack in the past year, and over half of small businesses worry that a breach could force them out of business.

Supply Chain Interdependencies and Risks

As we discussed earlier, manufacturers are often part of complex global supply chains involving hundreds of vendors, partners, and customers—each representing a potential risk source, especially as attackers increasingly target supply chain vulnerabilities. A single breach at a third-party supplier or service provider can quickly spread through the network, exposing sensitive data, halting production, and damaging trust across the ecosystem. Recent incidents, including high-profile ransomware attacks, have demonstrated cascading effects; not only does the targeted company suffer, but its partners must also activate emergency protocols and sometimes end business relationships. Gartner and NIST predict that by 2026, attacks on digital supply chains will impact nearly half of organizations worldwide, a trend driven by the use of open-source software and cloud-based platforms.

Rethinking Defense for Small Manufacturers

Recognizing these threats, experts now advise layered, risk-based defense strategies. Affordable measures—such as regular vulnerability assessments, network segmentation, automated patch management, effective backup plans, and outsourced fractional security leadership (“vCISO” services)—can help even the smallest firms significantly lower their risk. Real-time monitoring of supplier health, routine employee training, and the implementation of minimum security standards across partners all boost resilience.

In summary, small manufacturers are prime targets for cyberattacks because of their highly connected systems, limited resources, and crucial role in global supply chains. The stakes are high, but by focusing on practical actions and ongoing improvement, small manufacturers can effectively lower risk and safeguard their businesses.

Moving Forward, with Confidence

The above underscores a serious and clear view of the cyber risks confronting small and midsize manufacturers in 2025. As the industry embraces digital transformation, it has become both more efficient and more vulnerable. Attackers are targeting every new connection, legacy system, or overlooked vendor link. A wide range of threats—from ransomware and phishing to supply chain breaches and data theft—are not limited to large companies. Even the smallest manufacturer can serve as a gateway for financially motivated, opportunistic, or state-sponsored cybercriminals, impacting not only their own operations but also the larger network of partners and clients who depend on them for ongoing functionality.

The challenges are significant. Despite this, practical resilience remains achievable. By analyzing markets and sectors, reviewing real-world incident reports, and applying proven defensive strategies, it's clear that strong cybersecurity isn't about overspending on attackers or achieving absolute perfection. Instead, it involves implementing layered, risk-based defenses, fostering a culture of vigilance, investing in ongoing improvement, and ensuring cybersecurity accountability across all business relationships.

With each example of disruption or loss, the lessons are clear: every manufacturer can take meaningful steps to strengthen systems, train employees, segment networks, and audit supply chains, regardless of their resource limitations. Together, these proactive choices not only benefit individual companies but also improve the security of the entire supply chain.

The digital threat landscape is evolving, but so is the defense toolkit. With a smart, consistent strategy and a willingness to adapt, small manufacturers can not only survive but also thrive—delivering on the promise of digital innovation safely and confidently for years to come.

Chapter 2

Lessons in Resilience – The PFI Transformation

Plymouth Fabricators, Inc. (PFI) is a fictional company based on research of small manufacturers in northern New England. It is meant to represent a typical business that has been operating for more than one generation and maintains a well-established position in New England's manufacturing industry.

Introduction

The PFI story provides a realistic view of what modern cyber resilience means for manufacturers working with limited budgets and outdated infrastructure. Like many small and midsize businesses in industrial supply chains, PFI faced the challenge of staying productive while managing increasing cyber threats. Their journey—from exposure and vulnerability to a measurable decrease in cyber risk—shows that resilience can be achieved through focus, prioritization, and disciplined action.

This chapter examines PFI's experience to highlight practical lessons for other manufacturers looking to strengthen defenses without compromising operational performance. The case study can be found in the appendix.

Background

PFI is a custom fabricator of precision alloys and tooling, located in Athol, Massachusetts, with a secondary facility in Jaffrey, New Hampshire. Like many small manufacturers, they rely on both modern IT systems and decades-old operational technology (OT). Some of their most critical quality assurance devices still run on Windows XP because replacing them would disrupt certified production processes and be very costly. This mix creates what experts often call a "dual digital footprint"—one part modern, one part outdated.

By early 2024, PFI had experienced several close calls: phishing attempts targeting plant managers, occasional downtime from network scans, and sporadic vendor email impersonations. The leadership team recognized that the risks were rising but lacked sufficient internal cybersecurity staff to address them. Their turning point came when routine customer due diligence revealed that PFI's third-party risk rating was in the lowest quartile for suppliers in the defense industry.

The Risk Landscape

For business leaders, risk is quantified by dollars, downtime, and damage to reputation. The first step to improving security was measurement. Using the Annualized Loss Expectancy (ALE) model, PFI hired a small local provider for a fractional vCISO service to assess the annual likelihood and possible financial loss for its ten most critical risks.

The results were sobering. The analysis identified ransomware, phishing, legacy system exposure, and OT security gaps as the four main risks, which together account for over 70% of PFI's modeled annualized losses. Before any control investments, these top risks carried **an expected financial impact of more than $240,000 per year**—enough to threaten profitability after just one incident.

Using the NIST Cybersecurity Framework (CSF) and the Center for Internet Security (CIS) controls, the vCISO team proposed a phased plan for improvement, emphasizing quick wins ("Cyber Hygiene") and long-term strategies to reduce risks significantly.

Compliance to Resilience

PFI's leadership approved an initial one-year investment of approximately $130,000—funds allocated for vCISO guidance, Zero Trust network segmentation, endpoint protection upgrades, and staff training. The goal was not just to meet compliance but to achieve genuine risk reduction.

Key steps included:

- **Fractional vCISO engagement ($45,000):** Provided governance, vendor management, and training.
- **Zero Trust endpoint and OT integration ($17,000):** Consolidated software-defined access for 53 endpoints and network segmentation for 10 OT devices.
- **Phishing and insider-threat mitigation training ($2,600):** Emphasizes awareness and behavior rather than technology.
- **Top four risk corrective actions ($65,000):** Focused ransomware containment, cloud security setup, and credential strengthening.

Risk Reduction by the Numbers

After executing the plan, PFI's recalculated ALE clearly demonstrated a before-and-after comparison.

Table 2: The Numbers

Risk Type	ALE Before Controls	ALE After Controls	ALE After Zero Trust	Total Reduction
Ransomware	$75,000	$22,500	$7,500	90%
Phishing & Social Engineering	$50,000	$25,000	$10,000	80%
Legacy Systems	$42,000	$16,800	$4,200	90%
OT Security Gaps	$48,000	$16,800	$4,800	90%

Across all categories, PFI lowered annualized exposure from $111,300 to less than $40,000, saving over $70,000 annually in modeled risk. More importantly than the numbers, the exercise grounded cybersecurity in concrete, financially driven choices.

Organizational Impact

Beyond metrics, the transformation at PFI led to significant cultural change. Employees who were previously hesitant to question suspicious messages now regularly verify unusual requests. The coexistence of legacy OT and modern IT became a planning challenge rather than a hidden risk. Leadership accepted the idea that cybersecurity was not a one-time project but an ongoing cycle of improvement integrated with operations, safety, and customer trust.

> *PFI's COO, Jeri O'Donnell, summarized the shift clearly: "Cybersecurity stopped being someone else's job—it became part of how we protect uptime."*

This mindset helped PFI retain key contracts with defense-industry partners who required verification of ongoing controls and policy updates. The fractional vCISO model provided the right expertise at a predictable cost, avoiding the expense of a full-time security hire while enhancing the company's strategic posture.

Lessons for Small Manufacturers

The PFI case highlights several universal lessons for small manufacturers.

1. **Start with quantification.** Models like ALE and ARO transform vague risks into clear insights that support decision-making.

2. **Prioritize impact.** Concentrate on the key controls that reduce the most financial and operational risk for each dollar invested.
3. **Balance legacy with innovation.** Old systems can be segmented and safeguarded instead of being immediately replaced.
4. **Build culture, not checklists.** Policies and tools matter less than ongoing awareness and accountability.
5. **Leverage external expertise effectively.** Fractional or virtual CISO partnerships provide valuable leadership without the expense of full-time enterprise-scale staff.

From Reaction to Resilience

PFI's story reflects that of many small and mid-sized manufacturers facing increasing digital challenges. Their success—reducing projected risk exposure by more than half in just a year—shows that improving security is achievable even with limited resources. As the attack surface in manufacturing continues to expand, companies that invest wisely, train regularly, and monitor their progress will become not only compliant but also more resilient.

The next chapter will expand on these principles by exploring how manufacturers can broaden their security efforts from internal systems to their entire supply chain ecosystems, making resilience a collective value rather than an individual goal.

Chapter 3

Building Cyber Hygiene That Endures
Applying NIST CSF and CIS Controls to Strengthen Small Manufacturers

Introduction

Good cyber hygiene is the foundation of every resilient manufacturing business. Before regulations, frameworks, or certifications, there are daily behaviors, protective habits, and simple yet reliable practices that determine whether a business prevents incidents or falls victim to them. For small and mid-sized manufacturers, where every hour of downtime carries a cost, building effective hygiene is not about adding complexity—it's about operational discipline.

This chapter describes how manufacturers can apply proven frameworks like the NIST Cybersecurity Framework (CSF) and the Center for Internet Security (CIS) Controls to establish and sustain discipline. These frameworks offer a practical way to achieve resilience and prepare for compliance with more detailed standards such as CMMC Level 2, NIST SP 800-171, or ISO 27001.

For small and medium-sized businesses without a large IT staff, having a trusted cyber security advisor available to help is invaluable. The advisor can provide services like vCISO guidance, security program management, and hygiene assessments.

Cyber Hygiene First

Cyber hygiene involves keeping digital systems as clean and organized as physical equipment and workspaces, with regular quality checks. It includes routine tasks like applying patches, managing access, making backups, and training employees. Just as machine maintenance is cheaper than repairs, preventing issues through good cyber hygiene is more cost-effective than fixing problems after they occur.

Common signs of poor cybersecurity include shared passwords, unmanaged devices, untrained staff, and gaps in IT oversight between operations and manufacturing cells. A single weak credential or outdated workstation can act as a gateway for ransomware or data theft—disrupting production and harming trust with supply chain partners.

Strong hygiene, by contrast, fosters predictability and confidence by protecting the business in a way that aligns with its goals, supports operations, and secures its role in the supply chain. Strong hygiene lays the foundation for frameworks like CMMC or ISO 27001, allowing compliance efforts to build on a stable operational base.

NIST CSF: Five Functions, One System

The NIST Cybersecurity Framework (CSF) provides the most adaptable roadmap for improving security posture without adding a heavy administrative burden. It divides cybersecurity activities into five key functional areas.

1. **Identify** – Understand assets, systems, and data critical to operations.
2. **Protect** – Develop safeguards to defend those assets.
3. **Detect** – Monitor continuously for unusual activity or attacks.
4. **Respond** – Establish incident response procedures and containment capabilities.
5. **Recover** – Build resilience to resume operations quickly after an incident.

Each function links to categories and sub-controls that can be scaled to fit even the smallest organizations. NIST CSF can serve as the blueprint for helping clients find structure in what often seems like chaos—turning scattered IT practices into a repeatable, auditable program.

CIS Controls: The Fast Start to Hygiene

Where NIST CSF defines the framework, the CIS Critical Security Controls offer the actionable checklist. These 18 prioritized, technology-neutral practices tackle 80% of real-world threats with practical, measurable steps. Examples include:

- **Inventory and Control of Assets (CIS Control 1):** Identify every computer, OT device, and endpoint connected to the environment.
- **Continuous Vulnerability Management (Control 7):** Regularly scan and remediate system weaknesses.
- **Email and Web Browser Protections (Control 9):** Minimize phishing and social engineering exposure.
- **Data Recovery (Control 11):** Implement secure, tested backups of configuration and process data.
- **Security Awareness and Skills Training (Control 14):** Empower employees as the first line of defense.

These controls form the **"Operational Core"** of cyber hygiene—the everyday activities that quietly but powerfully sustain security health.

Where 5SDS Helps: Turning Frameworks into Practice

For many manufacturers, the biggest gap is not motivation—it's **translation**. Frameworks provide structure, but each business needs practical, grounded implementation. A good cybersecurity consulting firm can bridge gaps through managed services designed for small teams, including:

- **Cyber Hygiene Readiness Assessment:** Reviews current practices using NIST CSF and CIS benchmarks to pinpoint control weaknesses.
- **Continuous Hygiene Program:** A monthly service maintaining patching, configuration management, and user training cycles.
- **vCISO Leadership Program:** Fractional Chief Information Security Officer oversight, ensuring decisions remain tied to business goals and compliance requirements.
- **Compliance Readiness and Mapping:** Aligns current hygiene practices directly with CMMC and ISO 27001/27002 controls, reducing audit preparation time and cost.

Often, services are scalable by facility size and system complexity, ensuring manufacturers pay only for what they need while gaining measurable maturity improvements.

Bridging Hygiene and Compliance

While hygiene and compliance may seem like separate paths, they converge closely under NIST and CMMC. The **CMMC Level 2 model**—drawn from NIST SP 800-171—explicitly references the same control families used in both CSF and CIS frameworks.

Table 3: NIST CSF, CIS, and CMMC

NIST CSF Function	Related CIS Control	CMMC Practice Alignment	Example Outcome
Protect	Control 3: Data Protection	AC.2.005, SC.2.178	Role-based data access protections
Detect	Control 8: Audit Log Management	AU.2.041	Secure, monitored log retention

NIST CSF Function	Related CIS Control	CMMC Practice Alignment	Example Outcome
Respond	Control 17: Incident Response and Management	IR.2.092	Documented incident procedures
Recover	Control 11: Data Recovery	CP.2.121	Tested backup and recovery strategy

The integrated structure means that investing in solid hygiene and maturity practices has dual benefits: it reduces risk today and builds compliance readiness tomorrow. The goal is not to chase compliance reports—but to run secure operations that naturally meet regulatory tests.

Practical Steps to Begin

For manufacturers starting fresh, there are three practical momentum builders.

1. **Baseline Your Hygiene:** Use CIS Controls (currently v8) to build an internal checklist or adopt a guided assessment. Having a third-party consulting firm can be very helpful.
2. **Adopt the NIST CSF Core Functions:** Assign each function (Identify through Recover) to individuals or teams responsible for production, IT, and management.
3. **Track Progress Quarterly:** Replace vague "security reviews" with specific, framework-based check-ins—patching rates, training completion, recovery time metrics.

Just these steps elevate predictability, improve vendor trust, and create a living record of improvement—a key requirement in regulatory audits.

From Minimum Compliance to Everyday Resilience

Effective cyber hygiene transforms compliance into a natural byproduct of good operations. When NIST CSF provides direction, CIS offers precision, and an expert partner can manage execution, even small teams can function with the discipline of large enterprises.

Cyber hygiene is not glamorous—it's the unseen backbone of every resilient operation. Manufacturers who adopt its principles build more than defensible networks; they cultivate reliable businesses ready to withstand the disruptions of tomorrow.

Chapter 4

The Human Firewall – Building a Culture of Cyber Awareness

Introduction

Even the most advanced cybersecurity technology can't protect a business if its staff remains untrained, unaware, or unengaged. The strongest defenses collapse when an employee clicks a phishing link, reuses passwords, or ignores basic data-handling procedures. For small and mid-sized manufacturers, where employees wear multiple hats and training budgets are limited, the challenge is greater—but also more solvable.

Cybersecurity culture is built on clarity, consistency, and leadership, not fear or compliance. This chapter discusses how manufacturers can foster practical cyber awareness at every level of their workforce—transforming employees from potential vulnerabilities into strong defenders.

Cybersecurity Begins with Behavior

A strong security culture starts with recognizing the importance of human behavior. According to global research, over 80% of breaches are caused by human error or manipulation. For manufacturers, this often shows up through phishing, weak passwords, or mishandling sensitive production and customer data.

Unlike large corporations, smaller manufacturers can turn behavioral change into a competitive advantage. With flatter hierarchies and tighter teams, communication becomes quicker, and culture spreads rapidly. When employees understand how their actions affect the security of customers, contracts, and jobs, they take ownership.

Key principles of behavior-based security are as follows.

- **Simplicity:** Focus on teaching only what people need to remember. Avoid overwhelming staff with complicated jargon.
- **Relevance:** Connect examples directly to manufacturing operations—malicious USBs on the shop floor, invoice fraud in purchasing, or misuse of remote network login.
- **Repetition:** Incorporate cybersecurity into regular conversations instead of just annual checkbox training.

From Awareness to Empowerment

An effective awareness program shifts from "training compliance" to "operational empowerment." The aim is not just to inform people but to enable and make them responsible participants in defense. The awareness program should include the following.

- **Role-based education:** Training customized for the worker—production staff gets physical device security guidance, while finance teams concentrate on preventing social engineering payment fraud.
- **Scenario-based exercises:** Employees learn most effectively through simulated experiences. Realistic phishing simulations, password hygiene campaigns, and recovery walkthroughs enhance preparedness.
- **Public reinforcement:** Recognize and reward individuals who follow security best practices. Gamification and friendly competition enhance engagement more effectively than annual tests.
- **Visible leadership:** Leaders must lead! Executives who complete the same training as their staff demonstrate accountability from the top, significantly boosting the effectiveness of training efforts.

Cyber-Aware Workforce Model

A good cybersecurity consultancy provides structured awareness and culture-building programs tailored for small manufacturers. These services should integrate seamlessly with existing operations without causing disruptions. Several components to consider include the following.

1. **Cyber Awareness Baseline Audit:** Assesses current training materials, incident response communication, and employee preparedness to identify and report potential threats.
2. **Role-Based Security Curriculum:** Modular 30-minute sessions focused on manufacturing realities—industrial phishing schemes, vendor fraud, and OT access management.
3. **Simulated phishing and behavioral analytics:** Controlled campaigns assess how employees respond to fake phishing attempts and highlight areas that need reinforcement.

4. **Quarterly Reinforcement Packages:** Maintain cybersecurity awareness with newsletters, digital signage, and short reminder videos on password, backup, and access hygiene.
5. **Leadership Coaching:** Equips managers to communicate risk messages effectively and manage live incidents with confidence.

This scalable model suits organizations of all sizes, ensuring that everyone—from machinist to executive—knows their role in resilience.

Integrating Security Culture with Operational Excellence

Embedding cybersecurity into manufacturing excellence programs like Lean or ISO 9001 aligns well with industry culture. Workers already understand continuous improvement and quality control; cybersecurity simply becomes another measurable process. Those strategies include the following.

- **Standard work instructions:** Incorporate basic security requirements, like approved USB use or login procedures, into production documentation.
- **Gemba walks for IT:** Just as quality leaders visit the shop floor, IT or vCISO teams should observe how technology is used every day.
- **Safety and Security briefings:** Include a short cyber safety topic in existing shift start meetings or toolbox talks.
- **Metrics and tracking:** Link security training to plant performance metrics—such as compliance rates, phishing susceptibility, and recovery drill results.

The integration strategies emphasize cybersecurity as a collective responsibility, not just an extra duty.

Extending Culture Across the Supply Chain

An organization's culture extends beyond its firewall. Every trusted vendor, subcontractor, or logistics partner can be a potential link in the chain of resilience—or failure. Small manufacturers can lead by example by setting security expectations in their partnerships.

- Share concise cybersecurity policy summaries and awareness materials with vendors.
- Encourage vendors to adopt NIST CSF and CIS hygiene practices.
- Incorporate simple supplier questionnaires evaluating staff awareness and incident history.

- Require minimal training or attestation for anyone handling controlled unclassified information (CUI) or production data.

By influencing partners, manufacturers increase the impact of their investment. A culture of awareness within one company encourages similar practices throughout its ecosystem—building a shared "resilience posture" that extends protection well beyond the facility boundary.

Where Human Factors Meet Frameworks

Regulatory frameworks like CMMC and NIST SP 800-171 recognize the vital role of people. Many of their practices—such as training, reporting mechanisms, and access control—rely heavily on human execution.

- **CMMC Practice AT.2.056 (Awareness and Training**): Requires organizations to make sure that all system users understand security risks.
- **NIST CSF Protect / PR.AT Category:** Outlines activities that enhance personnel awareness and education.
- **CIS Control 14:** Focuses on continuous security awareness and skills training.

Through this alignment, culture becomes a compliance enhancer—meeting multiple frameworks at once while strengthening behavior-driven defense.

Your cybersecurity consultancy supports clients in aligning training initiatives directly with these control families. By recording attendance, frequency, and measurable improvements (such as reduced phishing click rates), clients can create concrete evidence of their maturity for audits and certifications.

Measuring and Sustaining Engagement

Awareness is not a one-time event. It is an ongoing process that develops over time. Manufacturers should evaluate culture maturity using straightforward, repeatable metrics such as:

- Click rates on phishing simulations over time.
- Training completion percentages by department.
- Incident response time from detection to reporting.
- Post-event debrief participation.

Annual employee surveys can add qualitative insights into whether staff feel confident in identifying and reporting threats. When results improve, awareness becomes ingrained, and cybersecurity shifts from an obligation to a habit.

From Awareness to Collective Resilience

Cyber resilience relies on trust—trust in systems, suppliers, and people. When employees understand the importance of information and the dangers of neglect, they instinctively protect that trust.

Manufacturers who promote awareness programs and align them with frameworks like NIST CSF, CMMC, and CIS Controls do more than just achieve compliance; they build confidence. With expert partners like 5SDS guiding training, policy development, and human risk analytics, even small teams can attain enterprise-level resilience. A resilient workforce leads to a resilient company.

Chapter 5

The Economics of Cyber Resilience — Turning Security into Strategic Value

Introduction

Cybersecurity is often seen as a cost rather than an investment, a view that hinders progress and makes organizations vulnerable, keeping them in constant reaction mode. For small and mid-sized manufacturers, financial strain tempts them to delay security improvements until after an attack—when costs increase dramatically. This chapter shifts the view of cybersecurity to an economic perspective, showing it not as a sunk cost but as an initiative that protects revenue, maintains reputation, and supports operational sustainability. Building resilience is not just about preventing loss — it's about empowering confidence, ensuring continuity, and boosting competitiveness in a growing digital supply chain.

The Real Cost of Inaction

Every organization has a cyber risk balance sheet, even if it's invisible. Not investing in security results in measurable impacts—lost productivity, ransom payments, recovery costs, regulatory fines, and damage to reputation. Industry data indicates that the **average cost of a ransomware attack on small manufacturers exceeds $200,000**. **Upwards of 60% of affected SMBs go out of business within six to twelve months** after a major cyber incident.

Financial impacts can be grouped into three dimensions:

1. **Direct costs:** Incident response, downtime, data restoration, and legal expenses.
2. **Indirect costs:** Reputational damage, contract loss, and regulatory penalties.
3. **Opportunity costs:** Delayed innovation, missed bids, or exclusion from compliant supply chains (CMMC, DFARS, ISO 27001).

Mitigating these losses requires understanding the specific areas where cybersecurity provides real financial benefits.

Quantifying Resilience — Cyber ROI

Traditional ROI models have difficulty capturing avoided losses. To evaluate cybersecurity's economic value, manufacturers can utilize a **Risk Reduction ROI** model, comparing expected annual losses (ALE) before and after implementing controls.

$$\text{Cyber ROI} = \frac{(\text{ALE}_{\text{before}} - \text{ALE}_{\text{after}}) - \text{Cost of Controls}}{\text{Cost of Controls}} \times 100$$

If improving endpoint security and backup infrastructure decreases modeled losses by $50,000 annually while costing $15,000 to implement, the ROI is over 200%. This financial perspective shifts cybersecurity talks from "How much will this cost?" to "How much risk will this eliminate?"

Aligning Resilience with Business Strategy

Cyber investments should mirror an organization's risk appetite, customer commitments, and operational priorities. Manufacturers ought to align cybersecurity budgets with three guiding principles:

1. **Protect what matters most.** Focus on systems linked to revenue-generating activities—such as production machinery, ERP systems, and vendor data exchange platforms.
2. **Invest in scalability.** Opt for controls—such as managed detection, cloud-based backups, and MFA—that lower both IT effort and long-term maintenance expenses.
3. **Integrate with frameworks.** Map technology and training investments to NIST CSF and CMMC controls, ensuring compliance readiness while demonstrating maturity improvements to stakeholders.

Executives recognize value when investment directly enhances contractual eligibility, uptime, and insurance accreditation. The company's investment in an information security strategy aligned with the business's goals will deliver all these benefits.

Cyber Insurance and Financial Safeguards

For resilient manufacturers, cyber insurance plays a crucial—but often misunderstood—role. Insurers are increasingly requiring evidence of controls before granting coverage or processing claims. Typical underwriting requirements include:

- Multi-factor authentication (MFA) across administrative accounts
- Regular patch management and endpoint detection
- Offline or immutable backups
- Documented incident response plans

Insurance should support, not replace, defensive maturity. Companies that achieve higher hygiene standards (NIST CSF Tier 3 or above) qualify for lower premiums and greater payout certainty, turning compliance into a clear financial benefit.

The Role of Financial Modeling

Regular financial reviews elevate cybersecurity to a top-tier board concern. Shared dashboards and simple models help decision-makers track the metrics in Table 4 below.

Table 4: Financial Metrics

Metric	Description	Reason for Tracking
Annualized Loss Expectancy (ALE)	Predicted yearly cyber loss exposure	Quantifies financial risk
Risk Reduction ROI	Net benefit of implemented controls	Justifies investment
Cost per Incident	Average financial impact per recorded event	Identifies high-cost vulnerabilities
Insurance Leverage Ratio	Cost of premium vs. claim payout efficiency	Tests the insurance's effectiveness

Using these financial health indicators, cybersecurity becomes a manageable, predictable investment instead of an unpredictable emergency expense.

The Compliance Dividend

Meeting standards like CMMC, NIST SP 800-171, HIPAA/HITECH, or ISO 27001 can indirectly boost financial performance. Certification opens doors to markets such as defense contracts, medical device manufacturing, and aerospace supply chains. Each compliance milestone can unlock opportunities.

- **Eligibility for new contracts** with federal agencies or primes.
- **Preferred vendor status** among security-conscious buyers.
- **Higher valuation** during mergers, acquisitions, or loan underwriting.

Resilience therefore enhances as a business differentiator—companies that safeguard themselves also build greater trust and unlock more opportunities.

Communicating Value to Stakeholders

One of the most dependable indicators of long-term success is an organization's ability to communicate the value of cybersecurity effectively. Quarterly executive summaries and dashboards should emphasize:

- Reduction in quantified risk (financial terms, not technical jargon)
- Control maturity progress (aligned with frameworks)
- Incident response readiness metrics (mean time to detect and recover)

When security leaders share results emphasizing operational uptime and customer trust, cybersecurity becomes a critical component of brand value—not merely about compliance.

Sustainable Investment for Small Manufacturers

Practical resilience doesn't need large capital spending. The most effective use of resources often involves a balanced combination of:

- **People:** Regular awareness training, phishing simulations, and policy alignment.
- **Process:** Updated response plans, vendor assessment schedules, and governance.
- **Technology:** Automated backups, SOC-as-a-Service, and access control systems.

Manufacturers should set aside modest, regular budgets (3–5% of operational costs) for cybersecurity, similar to machinery maintenance—steady, predictable, and strategic.

From Cost to Competitive Advantage

When managed strategically, cyber resilience isn't just a shield—it acts as a lever for growth. Companies that show consistent control maturity and transparency secure more bids, negotiate better insurance, and maintain customer trust even during disruptions.

Credible risk management demonstrates professionalism, building partnership trust in an increasingly interdependent supply chain. The message for small manufacturers is clear: **security pays** — not just by preventing losses but also by unlocking new business opportunities.

Chapter 6

The vCISO Advantage — Scalable Leadership for Cyber Resilience

Introduction

Effective cybersecurity isn't just about software, policies, or compliance — it's about leadership. Many small and mid-sized manufacturers reach a point where their technology has improved, their employees are trained, and their compliance processes are underway, but cybersecurity decision-making still lacks clarity. Who owns cyber risk? Who connects operational priorities to security goals?

This chapter introduces the **virtual Chief Information Security Officer (vCISO)** model, a practical solution to that leadership gap. It explains how small businesses can gain from enterprise-level security strategies and governance—without hiring a full-time executive.

The Leadership Gap in Cyber Resilience

A traditional Chief Information Security Officer oversees all aspects of an organization's cybersecurity program—risk, compliance, incident response, vendor security, and executive communication. However, in small and mid-sized companies, this role is often unfilled or managed informally by IT staff who lack authority or capacity.

This leadership gap creates three common weaknesses:

- **Strategic drift** — Cyber efforts occur piecemeal, not as part of a unified plan.
- **Reactive spending** — Budgets are driven by incidents instead of foresight.
- **Compliance fatigue** — Frameworks like CMMC, NIST, ITAR, and DFARS become checkboxes instead of competitive advantages.

A vCISO fills this gap by delivering executive-level cybersecurity strategy on a fractional or subscription basis—offering affordability, flexibility, and strategic continuity.

What a vCISO Really Does

A vCISO offers the same core services as an in-house Chief Information Security Officer, customized to your company's size. Their focus is on aligning people, processes, and technology with clear, measurable objectives, while helping business leaders understand the cyber landscape and make better decisions that meet the company's needs.

Core responsibilities typically include:

- Developing and maintaining a risk management plan using a framework such as NIST CSF, CMMS, or ISO 27001.
- Developing and revising company security policies to ensure they are practical and enforceable.
- Leading efforts in incident response planning and recovery exercises.
- Managing third-party vendor evaluations and contractual security obligations.
- Delivering executive briefings that translate risk into business language—safeguarding uptime, fulfilling audit requirements, and building customer trust.

Where small businesses often view cybersecurity as a technical burden, a vCISO reframes it as a form of business governance—a catalyst for growth, customer confidence, and operational stability.

Fractional Expertise, Full-Time Value

Hiring a full-time CISO is too expensive for most small manufacturers. Annual pay for such roles often goes over $200,000, excluding benefits or staff support. In contrast, a vCISO service offers the same senior-level strategy through part-time work—usually at 10–20% of the cost.

Typical service structures include:

- **Monthly retainer** — A fixed package covering governance, reporting, and advisory.
- **Project-based engagement** — Targeted tasks such as gap analysis, CMMC audit readiness, or policy redevelopment.
- **Continuous improvement model** — Ongoing risk tracking and training oversight integrated into operations.

With predictable pricing and measurable results, SMBs receive enterprise-level leadership without the high costs, making it a good fit for manufacturing margins.

Governance Made Measurable

One of the main benefits of a vCISO is turning cybersecurity from a vague IT issue into a measurable part of the business. Virtual CISOs create dashboards and governance tools that monitor:

- **Mean Time to Detect (MTTD)** and **Mean Time to Recover (MTTR)**
- **Audit readiness scores** based on CMMC or NIST controls

- **Training completion rates** and social engineering test results
- **Supply chain risk ratings** for key vendors

These measurements offer ownership visibility and ensure accountability. Boards and executives can now approach cybersecurity like finance—measured, tracked, and enhanced.

Integrating the vCISO into Business Strategy

A vCISO goes beyond just managing compliance. They focus on aligning cybersecurity efforts with business goals. Common strategic deliverables include:

- **Roadmaps for compliance,** such as aligning CMMC Level 2 efforts with DoD contract timelines.
- **Technology modernization planning** that incorporates resilience objectives.
- **Cross-departmental coordination**, ensuring operations, HR, and IT follow unified security principles.

In small manufacturers, this coordination can promote innovation—supporting digital transformation (like adopting smart factories) while upholding trust and compliance.

Relationship to CMMC and NIST Frameworks

Most SMB manufacturers must meet cybersecurity maturity expectations to compete in supply chains. The vCISO ensures program design follows applicable frameworks:

- **CMMC 2.0:** Guides compliance audit readiness and continuous improvement for defense suppliers.
- **NIST SP 800-171/CSF:** Adds structure to risk assessments, documentation, and control implementation.
- **ISO 27001 (optional):** Aligns international governance for firms with global suppliers.

The vCISO's expertise ensures compliance efforts lead to greater resilience, not just paperwork.

The vCISO in Practice — A Use Case Example

Consider a small aerospace machining company in New England. Facing defense audits, it hired a cybersecurity consultancy vCISO to create a cybersecurity roadmap. Within six months:

- All security policies were rewritten around CMMC Level 2 requirements.
- Employee phishing resilience improved from 55% to 92%.

- Backup testing frequency increased, reducing recovery time from two days to under four hours.
- The company passed its supplier risk audit—and won a new contract because of its documented cybersecurity maturity.

This highlights the core value of the vCISO: transforming scattered IT and compliance efforts into a cohesive resilience program that enhances business credibility.

When to Consider a vCISO

Cybersecurity programs have reached a maturity tipping point, where ad hoc management is no longer enough. It's time to consider a vCISO when:

- Your business handles **controlled unclassified information (CUI)** or regulated or sensitive vendor data.
- **Insurance underwriters** begin requiring formal cybersecurity documentation.
- Security tasks exceed your IT team's capacity or expertise.
- **CMMC or NIST audits** are on the horizon.
- Leadership recognizes cybersecurity as a business investment, not just a cost.
  A vCISO guarantees your investments meet specific, measurable, and auditable goals.

Building Partnership Resilience

The most effective vCISO relationships are ongoing partnerships, not single solutions. They build on trust, transparency, and alignment.

- Regular executive check-ins on metrics and priorities.
- Ongoing adaptation of controls as threats and regulations evolve.
- Vendor collaboration to ensure that external dependencies don't undermine internal compliance.

For many cybersecurity consultancies, the vCISO model is the peak of their service offerings. This strategic partnership helps each client maintain resilience as a lasting competitive edge, not just a compliance obligation.

Chapter 7

Future-Proofing the Factory
Automation, AI, and Continuous Monitoring

Introduction

The future of manufacturing will be shaped not only by speed and accuracy but also by the ability to adapt securely. The rise of automation, artificial intelligence (AI), and connected industrial systems has revolutionized production, but it has also expanded the digital attack surface. Every new sensor, robot, or cloud integration offers both opportunities and risks.

This chapter examines how small and mid-sized manufacturers can integrate cyber resilience into their digital transformation—leveraging automation and AI for operational excellence while keeping security a fundamental priority, not an afterthought.

The Convergence of IT, OT, and Cybersecurity

In traditional factories, Information Technology (IT) and Operational Technology (OT) operated separately. IT handled data, email, and ERP systems, while OT managed machines and production processes. Today, connected equipment and industrial IoT blur those distinctions. Data streams flow continuously from plant floors to corporate networks and cloud services.

This integration provides exceptional efficiency—real-time analytics, predictive maintenance, and remote monitoring—but it also brings new vulnerabilities:

- Legacy control systems that lack encryption or password protection.
- Remote access tools used for maintenance that attackers can exploit.
- Insider or supplier-related risks through shared credentials or unmanaged endpoints.

To future-proof operations, manufacturers must adopt a unified cyber-physical security strategy, treating machines as digital assets that require the same protection as servers or data.

Building a Secure Digital Foundation

Before deploying automation or AI tools, a business must make sure its basic cybersecurity hygiene is strong.

- Separate networks for administrative and production environments.
- Implement endpoint detection and response (EDR) across both IT and OT systems.

- Implement robust authentication and logging for all remote access.
- Keep dependable offline backups of essential control settings.

Industrial resilience starts with visibility. You can't safeguard what you can't see. Ongoing asset discovery and monitoring systems are vital for detecting shadow devices and identifying firmware vulnerabilities before they lead to incidents.

Artificial Intelligence in Cyber Defense

AI is transforming both the battlefield and defense in cybersecurity. For manufacturers, AI-driven technologies now assist in predicting and preventing threats before they cause disruption.

- **Anomaly detection tools** identify unusual patterns in network traffic or equipment telemetry**.**
- **Predictive analytics** identify maintenance or performance issues caused by malware or misconfiguration.
- **Automated response orchestration** isolates compromised devices or initiates backup cutovers with minimal downtime.

However, AI also enhances the abilities of attackers. Deepfake phishing, automated credential attacks, and adversarial machine learning all target human or system weaknesses. The key to staying ahead is combining human oversight with machine speed—AI manages scale and pattern recognition, while humans verify context and judgment.

Continuous Monitoring — The Heart of Modern Resilience

In an always-connected environment, security must be dynamic. Continuous monitoring turns cybersecurity from a reactive defense into proactive assurance. For small manufacturers, this involves adopting cost-effective managed security services (MSSP or SOC-as-a-Service) that provide:

- 24/7 threat detection and response.
- Alert triage that filters out false positives, directing focus to genuine threats.
- Compliance logging aligned with CMMC and NIST standards.
- Regular reporting to keep executives informed and validate insurance.

The ultimate goal is operational confidence—ensuring that systems are always verified, not just checked occasionally.

Automating Cyber Resilience Processes

Automation isn't just for production—it's for protection. Organizations can automate essential security tasks to save time and minimize human error.

- **Patch Management:** Automatically deploy updates across both IT and OT without interrupting production cycles.
- **Access Control:** Enforce least-privilege roles with automated approval workflows.
- **Incident Response:** Combine detection with automatic quarantine of endpoints or starting backups when triggered.
- **Compliance Mapping:** Use software automation to align policies and evidence across multiple frameworks at the same time.

Through automation, smaller teams can achieve enterprise-grade security maturity without increasing scaling overhead.

Smarter Data, Stronger Security

Smart factories produce large amounts of data—such as production telemetry, supply chain transactions, and system logs. Data security is now essential for competitiveness. To handle this responsibly, manufacturers should:

- **Encrypt data at rest and in transit** using modern protocols (TLS 1.3, AES-256).
- **Classify data by sensitivity**—distinguishing production metrics from proprietary design data.
- **Apply retention policies** to minimize unnecessary exposure and cost.
- **Use AI-based analytics** to identify data usage anomalies that could signal IP theft or insider abuse.

Secure data stewardship not only prevents breaches but also builds trust with customers and prepares the business for upcoming privacy standards.

Innovation and Compliance Move Together

Many manufacturers see compliance as a restriction, but in the digital age, achieving compliance maturity speeds up innovation. Standards such as NIST CSF, CMMC, and ISO 27001 promote structured progress.

- Policies and procedures become blueprints for stable operations.
- Documented recovery testing supports safe system innovation.

- Regular audits reinforce accountability across departments.

Compliance maturity thus acts as a foundation for connected manufacturing, supporting automation and AI adoption within a robust governance framework.

Preparing for Next-Generation Risks

Future threats won't come just from hackers—they'll arise from complex ecosystems.

- AI-driven attacks mimicking trusted users.
- Supply chain compromises that infect firmware before delivery.
- Energy grid or IoT disruptions affecting entire regions.

The solution lies in adaptive resilience—creating systems that learn, change, and recover more quickly than threats can exploit. Small and mid-sized manufacturers that keep improving their cyber defenses will be seen as trusted, flexible partners in global supply chains.

A Vision for the Future

Cyber resilience is a journey, not a fixed goal; it involves ongoing learning, improvement, and collaboration. As automation, AI, and industrial connectivity transform manufacturing, leaders must ensure technology enhances trust.

Manufacturers who commit to secure modernization today will shape the future of American industry—more productive, more competitive, and more resilient against disruption.

The story of cyber resilience doesn't end here. It never does. Each new development presents fresh challenges and opportunities. By integrating security into every decision, from the factory floor to the boardroom, small manufacturers safeguard not only their data but also their legacy.

Afterword

The Future Belongs to the Resilient

The manufacturing world is entering a period where traditional boundaries—between people and machines, data and operations, security and strategy—are breaking down. Success will no longer rely just on machinery, workforce skills, or pricing power. It will depend on trust—the trust of customers, partners, and communities who rely on manufacturers to produce safely, securely, and consistently.

Cyber resilience goes beyond merely defending. It is a business culture that values foresight, discipline, and adaptation. It involves recognizing that technology can fail, but preparation and leadership must not. It requires every organization—regardless of size—to build resilience not only against today's threats but also against unseen challenges that may arise in the future.

Cybersecurity maturity is best built through steady, practical improvements. Resilience isn't about being perfect; it's about being persistent. Every small step, policy update, and employee training adds another layer of defense and another day of operational confidence.

Manufacturers are the backbone of American innovation and economic strength. Yet without digital resilience, even the most advanced production lines face disruption. Our shared goal is to help the next generation of small and mid-sized manufacturers succeed—not just in productivity, but in security, integrity, and readiness.

The path ahead will change fast—artificial intelligence, automation, and global connectivity will reshape how we work, learn, and compete. But one truth will stay the same: **resilient organizations endure**.

•••

If this guide has helped you see what's possible, let it be the beginning — not the end — of your cybersecurity journey. When security becomes part of your company's identity, you'll realize that resilience is not a final goal. It's a way of doing business.

Mission: *Building resilience. Protecting innovation. Enabling growth.*

About the Author

Randolph L. Nethers is an information security consultant, educator, and strategic advisor with over 30 years of experience helping organizations manage risks and improve resilience. His career includes IT systems engineering, compliance management, and executive leadership, with a focus on cybersecurity for manufacturing, defense, and industrial sectors. He holds an MBA and an MS in Cybersecurity from Norwich University, as well as a BA in Information Systems from Southern New Hampshire University. He also has certifications, including Certified Information Security Systems Professional (CISSP) and Certified Information Security Manager (CISM), among others.

As the founder of 5 Star Data Systems, LLC, Randolph acts as a fractional Chief Information Security Officer (vCISO) for clients throughout New England, guiding small and mid-sized businesses toward practical, compliant, and sustainable cybersecurity maturity. His approach combines deep technical knowledge with a focus on business value—helping leaders view cybersecurity as both a strategic asset and a competitive advantage.

Randolph is dedicated to making cybersecurity clear and achievable for all organizations. He believes that every manufacturer, no matter its size, deserves the confidence that comes from being secure, compliant, and prepared for the future.

About 5 Star Data Systems, LLC

5 Star Data Systems, LLC (5SDS) is a cybersecurity and compliance consulting company based in Keene, New Hampshire, that helps small and mid-sized manufacturers and businesses reduce risk, prepare for CMMC and NIST compliance, and develop lasting cyber resilience.

Founded on the belief that resilience should be affordable, measurable, and attainable, 5SDS provides services that connect technology with leadership. Its offerings include fractional vCISO governance, risk and compliance assessments, training and awareness programs, incident response planning, and vendor security audits.

5SDS partners with clients to turn cybersecurity from a regulatory burden into a competitive advantage—empowering manufacturers to operate confidently in today's digital supply chain.

For more information, visit 5sds.com to explore how practical cyber resilience can help your business thrive.

5 Star Data Systems, LLC

A Case Study: Plymouth Fabricators, Inc. (PFI)

A Model for Modern Manufacturing Cyber Resilience

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 are complex to upgrade.
- Rapid expansion in remote work, cloud adoption (Dynamics 365; Microsoft 365 Business (Premium/Basic)), 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 discipline for business continuity and growth—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 5: 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 6: 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
Legacy Systems	0.7	42,000	0.28	16,800	0.1	4,200

Risk	ARO Before	ALE Before ($)	ARO w/ Controls	ALE After Controls ($)	ARO w/ ZTNA	ALE After ZTNA ($)
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 7: 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: PFI'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 8: 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

Glossary

Access Control (AC): Policies or mechanisms ensuring only authorized users can view or use specific resources.

Access Control List (ACL): A list specifying which users or systems can access specific resources within a network or application.

Account Harvesting: The process of collecting legitimate account names on a system, often as a precursor to attacks.

Advanced Encryption Standard (AES): A widely used encryption algorithm to protect sensitive data adopted by the U.S. Government as its standard, specifically AES128 and AES265.

Advanced Persistent Threat (APT): A long-term, targeted cyberattack using stealth and sophistication to gain access to sensitive systems.

Antivirus: Software designed to detect and remove malware from computers and networks.

Asymmetric Cryptography: Encryption using a pair of keys (public and private) for secure data exchange.

Asset: Any item of value to an organization, such as data, devices, or infrastructure.

Asset Management: Cataloging and maintaining organizational assets to ensure protection and compliance.

Audit Trail: A record showing who accessed a system, when, and what actions were performed.

Authentication: The process of verifying a user, device, or system's identity before granting access.

Authorization: Granting approved users specific permissions to access data or systems.

Availability: Ensuring systems and data are accessible and usable when needed.

Backup: A copy of data kept to restore operations after data loss or a cyber incident.

Baseline: A baseline is a documented set of minimum security controls, configurations, and standards established to protect systems and data. It serves as a benchmark for measuring security posture, ensuring compliance, and detecting deviations that may indicate risks or vulnerabilities.

Bastion Host: A specifically hardened server used as a primary defense in a network.

Biometrics: A security process that uses unique biological characteristics (fingerprints, facial recognition) to verify identity.

Bot/Botnet: A bot is automated software; a botnet is a network of infected devices used for malicious activities (DDoS, spam).

Brute Force Attack: Repeated attempts to guess passwords or encryption keys.

Business Continuity Plan (BCP): A plan to ensure business operations continue after major disruptions.

Business Impact Analysis (BIA): Identifying the effects of business process disruptions.

Certificate-Based Authentication: Authentication that relies on digital certificates, used in Public Key Infrastructure (PKI).

Change Management: Controlling changes to systems or processes to minimize risk and disruption.

Chief Information Security Officer (CISO): Senior executive responsible for an organization's cybersecurity.

Cloud Computing: Delivery of computing services via the internet instead of local servers.

Compliance: Adhering to legal, regulatory, or organizational standards.

Confidentiality: Ensuring data is only accessible to authorized parties.

Confidential Unclassified Information (CUI): Information the U.S. government creates or possesses—or that an organization handles on its behalf—that requires safeguarding or dissemination controls under federal law, regulation, or government policy. CUI is not classified but must be protected to prevent unauthorized access or disclosure. Examples include export-controlled data, technical drawings, or defense-related specifications managed under DFARS or CMMC rules.

Configuration Management: Maintaining system integrity by managing configuration changes securely.

Control (Security Control): Policies or mechanisms to reduce risk and achieve compliance.

Corrective Action Plan (CAP): Actions taken to fix identified compliance gaps.

Cyber-Attack: Attempt to gain unauthorized access, disrupt, steal, or damage digital assets.

Cybersecurity Maturity Model Certification (CMMC): DoD standard for assessing and improving cyber hygiene for defense contractors.

Data Breach: An incident where sensitive, protected, or confidential data is accessed or disclosed without authorization.

Data Classification: Assigning levels to data indicating required levels of security.

Data Custodian: The individual responsible for the stewardship, management, and safekeeping of an organization’s data.

Data Encryption: The process of converting data to an unreadable form unless decrypted with a key.

Data Loss Prevention (DLP): Tools and processes to prevent unauthorized sharing or leakage of sensitive data.

Data Owner: The person who has responsibility and authority for data assets.

Denial of Service (DoS/DDoS): Attacks that overload or cripple systems or networks, making them unavailable.

Disaster Recovery: Strategies for restoring IT functions and data after a disruptive event.

Endpoint: Any device connected to an organization's network (laptop, smartphone, server).

Endpoint Security: Measures to protect endpoints from being compromised by attacks, including a local firewall and anti-malware software.

Encryption: Using cryptography to make information unreadable without special knowledge (decryption).

Federal Contract Information (FCI): Information provided by or generated for the U.S. government under a contract that is not intended for public release. FCI is less sensitive than CUI but still must be protected by contractors and subcontractors following basic safeguarding requirements in FAR 52.204-21, such as access control, system monitoring, and data protection.

Firewall: A technology or device that controls network traffic according to security rules.

FIPS: Federal Information Processing Standards are publicly announced standards developed by NIST for use in government computer systems. FIPS specifies security requirements, cryptographic protocols, and data handling procedures to ensure consistent protection and interoperability across federal agencies, thereby supporting compliance with laws such as FISMA.

FISMA: The Federal Information Security Modernization Act is a U.S. federal law that establishes mandatory security standards and frameworks for protecting federal information systems. It requires agencies and contractors to implement, review, and report on security controls to ensure the confidentiality, integrity, and availability of government data and operations.

Framework: A set of best practices and guidelines for managing risk (e.g., NIST CSF, ISO 27001).

Governance: Establishing policies and procedures for guiding and managing cybersecurity efforts.

HIPAA: The Health Insurance Portability and Accountability Act, a U.S. law for protecting health information privacy and security.

HITRUST: A certifiable framework for managing data protection and compliance, especially in healthcare.

Identity and Access Management (IAM): Tools or processes to review and control user identities and permissions.

Incident Response: The process to detect, contain, eradicate, recover, and review cyber incidents.

Information Security (InfoSec): Protecting data and systems from unauthorized access, disclosure, modification, destruction, or disruption.

Infrastructure: Underlying tech (servers, networks, devices) needed for company operations.

Insider Threat: Security risks originating from within an organization (employees, contractors).

Internet of Things (IoT): IoT refers to a network of interconnected physical devices embedded with sensors, software, and connectivity, allowing them to collect, share, and act on data autonomously or with minimal human intervention, frequently including OT and smart devices.

Intrusion Detection System (IDS): Tech that monitors networks or systems for malicious activity.

Intrusion Prevention System (IPS): Technology that not only detects but also prevents attacks.

ISO 27001: International standard for information security management systems (ISMS).

Least Privilege: The strategy of giving users the minimum levels of access required to perform their tasks.

Log Management: Collecting, analyzing, and storing logs to detect anomalies or prove compliance.

Malware: Malicious software designed to harm, exploit, or otherwise compromise systems.

Managed Security Services Provider (MSSP): A third-party company delivering outsourced security monitoring and management.

Mandatory Access Control (MAC): Access policies defined by a system, not users or owners.

Multi-Factor Authentication (MFA): An access control method requiring two or more proofs of identity.

National Institute of Standards and Technology (NIST): A U.S. agency that develops cybersecurity frameworks and standards. NIST publications are publicly available. Many are required by Federal law for Federal agencies, but are very useful for private organizations. Other publications were explicitly designed for private organizations.

NIST CSF: The NIST Cybersecurity Framework is a widely adopted guideline for handling cybersecurity risk.

NIST RMF: The NIST Risk Management Framework is a structured, risk-based process used by federal agencies and organizations to identify, implement, assess, and monitor cybersecurity controls. It ensures effective management of security and privacy risks throughout an information system's lifecycle while meeting the requirements of FISMA.

NIST SP 800-171: NIST Special Publication outlining controls to protect Controlled Unclassified Information (CUI).

NIST SP 800-53: NIST Special Publication with detailed controls for federal information systems.

One-day Attack: (Or Day One Attack) An attack that exploits a vulnerability for which a fix has been released on that day or very shortly thereafter. Such an attack exploits the fact that a vulnerability has been publicly announced, but very few users have applied the patch.

Operational Technology (OT): Refers to hardware and software that monitors or controls physical devices, processes, and infrastructure in industrial environments—such as manufacturing, utilities, or transportation—distinct from IT, which manages business data and applications.

Patch Management: Applying software updates to close security vulnerabilities.

Payment Card Industry Data Security Standard (PCI DSS): Standard for securing credit card data.

Penetration Test (Pen Test): Simulated attack to uncover weaknesses in systems or applications.

Personally Identifiable Information (PII): Information that can be used to identify an individual.

Phishing: A social engineering attack where attackers trick users into revealing confidential information.

Physical Security: Securing physical premises to prevent unauthorized access to assets.

Plan of Action and Milestones (POA&M): A document identifying tasks needing completion to address security weaknesses.

Policy: A documented set of rules or principles guiding decisions and actions.

Privacy Impact Assessment (PIA): Analyzing how systems/processes impact individual privacy.

Privacy: The right and expectation of individuals to control their personal information.

Privileged Account: Accounts with higher-level access to systems or data/settings.

Privilege Escalation: Gaining unauthorized, elevated access to resources.

Protected Health Information (PHI): Information about health status, provision of care, or payment related to healthcare.

Public Key Infrastructure (PKI): Framework for managing digital certificates and encryption keys.

Recovery Point Objective (RPO): The maximum amount of data loss a business can tolerate.

Recovery Time Objective (RTO): The maximum time a business can tolerate data/service downtime.

Remote Access: Ability to connect to a system or data from a location outside the organization.

Residual Risk: Remaining risk after mitigation measures are implemented.

Risk Assessment: Identification and evaluation of risks to organizational operations.

Risk Management: Ongoing identification, assessment, and prioritization of security risks.

Role-Based Access Control (RBAC): Access decisions are made based on a user's assigned roles.

SCF (Secure Control Framework): Comprehensive cybersecurity and privacy control framework mapping to major standards.

Security Awareness Training: Programs to teach staff about recognizing and preventing cyber threats.

Security Control Assessment (SCA): Evaluation of safeguards and countermeasures to determine their effectiveness.

Security Incident: Any event that threatens the confidentiality, integrity, or availability of data/systems.

Security Information and Event Management (SIEM): Tools to collect and analyze security event data in real time.

Separation of Duties: Dividing tasks and privileges among multiple people to prevent fraud or error.

Service Organization Control (SOC): A SOC audit report is an independent, third-party evaluation of a service organization's controls over financial reporting, security, or privacy, providing assurance and transparency to customers and stakeholders regarding risk management and compliance practices.

Single Sign-On (SSO): An authentication method that allows users to access multiple systems with one set of credentials.

Small Business Cybersecurity: Adjusted security best practices and standards appropriate for SMBs.

Smart Device: A smart device is an electronic device, often network-connected, capable of autonomous and interactive operation through sensors, processing, and communication, enabling it to collect, process, and exchange data, and often to automate tasks—for example, a smart switch, smart thermostat, or smart television.

Social Engineering: Manipulating people into disclosing confidential information.

Standard: Documented, required minimum of technical specifications of security controls.

Supply Chain Security: Ensuring external partners and suppliers do not pose cybersecurity risks.

System Security Plan (SSP): Description of system boundaries, environments, and security controls.

Threat: Any circumstance or event with the potential to cause harm to information or systems.

Threat Actor: An individual, group, or organization conducting malicious activity.

Tokenization: Replacing sensitive data with unique identification symbols (tokens) to protect the original data.

Two-Factor Authentication (2FA): See Multi-Factor Authentication.

User Provisioning: Process of creating, managing, and deactivating user accounts.

Virtual Chief Information Security Officer (vCISO): A consultant or consultancy firm hired to serve as a CISO, often on a part-time basis and also referred to as a fractional CISO.

Vulnerability: Weakness in a system or process that can be exploited.

Vulnerability Assessment: Systematic examination to identify and fix vulnerabilities.

White Hat: An ethical hacker performing authorized penetration testing.

Zero-Day: An undisclosed vulnerability with no available fix.

Zero-day Attack: An attack that exploits an undisclosed vulnerability for which no fix is available.

Further Reading

Below are some of the sources from which this eBook was taken and could serve as a starting point for further reading.

Alahmaei, A., Ahmed, M. K., & Rahman, M. (2025). A review of cybersecurity challenges in small business. Open Journal of Business and Management, 13(10), 4214–4240. https://www.scirp.org/journal/paperinformation?paperid=130449

Shiffman, A. (2025, April 18). Chinese hackers took trillions in intellectual property from about 30 multinational companies. CBS News. https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/

IBM Institute for Business Value. (2025, April 16). IBM X-Force 2025 threat intelligence index. IBM. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index

Industrial Cyber. (2025, October 16). Black Kite 2025 manufacturing report detects relentless ransomware pressure, exploitation of supply chain gaps. Industrial Cyber. https://industrialcyber.co/manufacturing/black-kite-2025-manufacturing-report-detects-relentless-ransomware-pressure-exploitation-of-supply-chain-gaps/

National Institute of Standards and Technology. (2023, May 16). Cybersecurity risk mitigation for small manufacturers. Manufacturing Innovation Blog. https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-risk-mitigation-small-manufacturers

Recorded Future Insikt Group. (2025, July). H1 2025 malware and vulnerability trends. Recorded Future. https://www.recordedfuture.com/research/h1-2025-malware-and-vulnerability-trends

Risk & Insurance. (2024, December 9). Manufacturing most vulnerable to cybersecurity risks across industries: Report. https://riskandinsurance.com/manufacturing-most-vulnerable-rising-cybersecurity-risks-across-industries-report/

VIPRE Security Group. (2025, April 10). Business email compromise in 2025: What, who, and why. VIPRE. https://vipre.com/blog/business-email-compromise-2025-what-who-and-why/

Vakulov, A. (2025, March 29). 14 top social engineering attack types and their subcategories. Forbes. https://www.forbes.com/sites/alexvakulov/2025/03/29/14-top-social-engineering-attack-types-and-their-subcategories/

Winsor Consulting. (2025). What is phishing & BEC? Business email compromise explained. IMEC. https://www.imec.org/what-is-phishing-bec-business-email-compromise-explained/

World Economic Forum. (2024). Building a culture of cyber resilience in manufacturing. World Economic Forum. https://www3.weforum.org/docs/WEF_Building_a_Culture_of_Cyber_Resilience_in_Manufacturing_2024.pdf