



## THE HIDDEN RISKS OF MODERN MANUFACTURING

The modern manufacturing facility looks nothing like the plants of previous generations. Today's production systems are interconnected, with data flowing through every stage of the value chain. And with the rise of AI in the manufacturing process, everything from forecasting and production to inspection and maintenance will depend on constant access to reliable and secure data.

But the push for digital maturity can create as many risks as it does opportunities. As facilities become more connected, the surface area for potential failure increases

across processes, technologies, machines, supply chains, and workers. A disruption that once might have taken a back-office function offline can now bring the entire factory to a screeching halt, making the risk of downtime greater than ever.

While manufacturers continue to modernize their operations, there are five key risks they must proactively manage.



## 1. Cybersecurity Threats

Even though manufacturers focus on physical products, they are as exposed to digital attacks as any e-commerce retailer or SaaS platform provider. In fact, the manufacturing industry experienced nearly **twice as many data breaches in 2025** compared to 2024,<sup>1</sup> making it one of the leading targeted industries for attack.

In addition, one in five attacks was tied to espionage, with attackers looking for sensitive plans and emails that would help give competitors an advantage, while nearly half of attacks involved ransomware.<sup>1</sup> Together, these attacks impact both operational readiness in the moment and future business competitiveness.

## 2. Operational Vulnerabilities

Production lines depend on precise, real-time synchronization between people, machines, data, systems, and workflows. A serious misconfiguration can result in unexpected downtime, **which costs manufacturers an average of \$1.7M per hour.**<sup>2</sup>

Disconnected processes and legacy equipment can create operational vulnerabilities that increase the risk of:

- Unexpected line stoppages.
- Production bottlenecks.
- Mechanical failures.
- Increased scrap rates due to quality control issues.

### 3. The Digital Maturity Gap

Many manufacturers see AI as a path to greater resilience, flexibility, and operational intelligence. But while 73% want to deploy GenAI to build more autonomous, resilient supply chains, **only 7% have actually completed implementation.**<sup>3</sup>

Without the systems and governance needed to support advanced tools, manufacturers will struggle to fully realize the benefits of automation, analytics, and real-time decision-making.

---

### 4. Supply Chain Instability

Because manufacturers depend on a tightly integrated supply network, a disruption anywhere is a disruption everywhere. In many cases, the weakest link is upstream or downstream of the manufacturer, reducing both visibility and control of risk.

As a result, **80% of manufacturers plan to invest at least 20% of their improvement budgets in smart manufacturing initiatives**<sup>4</sup> to help increase visibility, strengthen supplier coordination, and reduce vulnerability to external shocks.

---

### 5. Workforce Challenges

Even as manufacturers adopt more automation and AI, many still struggle with workforce shortages and skills gaps, with **31% of production lines operating without enough staff.**<sup>5</sup> An aging labor pool and difficulty attracting younger workers can create vulnerabilities inside the factory due to limited training and comfort with digital tools.

Devices, machines, processes, and workflows can be misconfigured, while the inability to document and share tribal knowledge can result in inconsistent execution. Meanwhile, a distrust of new technology can lead to low adoption of digital tools, reducing the ROI of digital transformation investments.



## What a Future-Ready Manufacturing Operation Looks Like

As manufacturing becomes more digital and connected, forward-thinking manufacturers are reengineering their environments with technologies, processes, and governance models designed to help reduce complexity, minimize human error, and strengthen control across the entire value chain.

While every organization is unique, the best share several core characteristics.

- **Security embedded throughout operations:** Rather than treating security as a standalone initiative, modern manufacturers integrate security throughout operations, including overlooked endpoints like printers, scanners, and multifunction devices. This helps protect sensitive information, reduce the likelihood of unauthorized access, and prevent operational disruptions before they occur.
- **Integrated systems with end-to-end visibility:** Real-time visibility, connected tools, and automated reporting help reduce the blind spots that let small issues grow undetected. Modern manufacturers leverage shared data environments where production, quality, maintenance, and supply chain workflows operate using a single source of truth.
- **Governed and secure data flows:** As data becomes more central to every stage of production, modern manufacturers are adopting stronger controls around how it is accessed, shared, and managed. Secure document workflows, standardized governance models, and role-based access protocols help protect intellectual property and ensure data integrity across teams.
- **Automation that strengthens consistency:** AI and automation support workers by handling repetitive tasks, capturing data automatically, and triggering quality checks or inspections. These capabilities reduce errors, streamline compliance, and increase output, helping manufacturers overcome labor shortages.
- **Flexible support that scales with the business:** As demand, regulations, and technology continue to evolve, modern manufacturers rely on a blend of internal teams and external partners to maintain the capacity to modernize without disrupting production. Scalable support models help ensure continuity even as operations grow more complex.



As the industry becomes more digital, the risks facing manufacturers will only grow more interconnected and harder to contain. But with the right systems, governance, and support in place, manufacturers can reduce complexity, protect their operations, and turn resilience into a true competitive advantage.

[See how Canon can help modernize your operations.](#)

**SOURCES:**

<sup>1</sup> Verizon, "[2025 Data Breach Investigations Report](#)."

<sup>2</sup> Global Newswire, "[Unplanned Downtime Costs Manufacturers Up to \\$852M Weekly](#)," October 2025.

<sup>3</sup> National Association of Manufacturers, "[Manufacturing Trends 2025](#)."

<sup>4</sup> Deloitte, "[2026 Manufacturing Industry Outlook](#)."

<sup>5</sup> UKG, "[2024 Manufacturing Industry Insights Report](#)."

**Canon**

**1-844-50-CANON**  
**USA.CANON.COM/BUSINESS**

Canon USA does not provide legal counsel or regulatory compliance consultancy, including without limitation, regarding Sarbanes-Oxley, HIPAA, CCPA, GDPR, GLBA, Check 21, or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Some security features may impact functionality/performance; you may want to test these settings in your environment.

Canon is a trademark or registered trademark of Canon Inc. in the United States and elsewhere.

©2025 Canon U.S.A., Inc. All rights reserved.