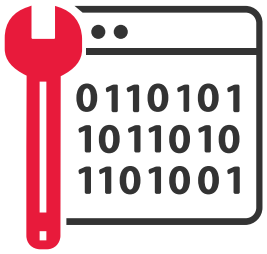
The Top 5 AI Risks in Manufacturing – and How to Manage Them

As market dynamics become less predictable, the manufacturing industry is increasingly leaning on artificial intelligence (AI) to help enhance demand forecasting accuracy, streamline **supply chain processes**, and support operations. According to a **2024 report from the National Association of Manufacturers**, AI is used widely across the industry. The majority of manufacturers (72%) said they're investing in Manufacturing 4.0 technology — such as AI — to reduce costs and improve operational efficiency.

But while AI helps manufacturers drive productivity, it also introduces significant risk. Manufacturing organizations must establish guardrails to mitigate these risks and facilitate safe and responsible AI use.

Read on to learn more about the top five AI risks manufacturers face today.

Risk #1: Poor Data Quality



Manufacturing organizations collect vast amounts of data from Internet of Things (IoT) devices throughout their supply chain and facilities, which they use to inform business decisions. Those that don't **take time upfront** to standardize, structure, and validate their data before implementing AI at scale risk erroneous outputs including flawed inventory predictions, skewed demand forecasting, and even safety incidents from unreliable quality control systems.

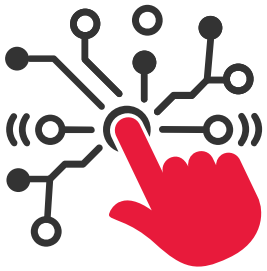
Risk #2: Cybersecurity Threats

The integration of AI tools into interconnected technology systems increases an organization's attack surface, creating multiple new entry points for threat actors.

Many manufacturing plant floors run on operational technology (OT) and house transducers and IoT sensors to capture real-time operational data that now feeds into interconnected AI tools. While this connectivity enables powerful analytics, these vectors must be properly protected to reduce the risk of threat actors accessing wider technology systems and potentially compromising operations or halting production. Consider that OT environments often house legacy control systems that were not built with cybersecurity in the design, meaning that as manufacturers adopt AI — and more frequently connect IT and OT— they create additional attack vectors that must be secured.

Risk #3: Loss of Intellectual Property

When manufacturing organizations upload data into AI systems, that data often contains proprietary information about cycle times, equipment configurations, and manufacturing processes. Additionally, many manufacturers are using open AI platforms connected to the internet, which can allow bad actors to access intellectual property (IP) and potentially replicate operational advantages.



Many manufacturers currently use AI tools without keeping the AI in a closed sandbox. Operating in a closed environment cut off from the internet is crucial to avoid accidental exposure of IP. Additionally, implementing mandatory AI training for all team members — that clearly outlines access protocols and controls — can also strengthen AI governance and help protect IP. IP theft remains a significant concern among manufacturers due to the high risk of revenue loss and even reputational risk.

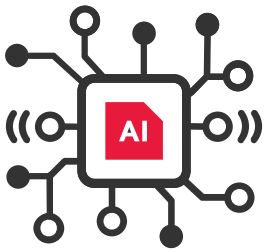
Risk #4: Job Displacement

Manufacturing employees are increasingly expected to learn and leverage digital twins, computer vision, and other AI-enabled tools. Yet as AI **adoption** increases, so does the risk of job displacement.

For example, the development of AI-enabled computer vision means manufacturers no longer need quality inspectors to manually examine products for defects. Instead, quality inspectors and other manufacturing employees will need to be upskilled to enhance their digital literacy and leverage computer visioning and other emerging tools of the trade.

Risk #5: Operational Disruption

Without proper human oversight of AI use, design, and deployment, AI systems can malfunction or hallucinate, significantly disrupting operations. For instance, manufacturers that use AI for demand forecasting but do not have guardrails in place, risk the AI model hallucinating a massive spike in demand. The false prediction may trigger automatic purchasing of excess raw materials or product components, resulting in overstocked inventory and tied-up capital. AI can also trigger product errors if not closely monitored. To prevent disruptions, manufacturers must codify AI testing and monitoring processes as part of cross-functional AI governance. Regular validation and human-in-the-loop oversight is essential, especially for high-impact functions such as demand forecasting.



Manage Risks with Responsible AI

Manufacturers that are embracing AI to gain competitive advantage must establish guardrails throughout the AI lifecycle to protect operations and facilitate responsible AI use.

Identifying specific industry risks — then working internally to address them — is the first step to establishing **responsible AI application** and effective governance.

BDO's experienced AI professionals can help manufacturing organizations at any and every stage of their AI journey. We can provide a step-by-step roadmap to strengthen your data foundation, establish an AI adoption framework, educate and upskill your team, and align use cases to your organization's objectives.

Ready to turn AI risk into resilience?

Download our guide to learn more about strengthening AI governance. ▶

CONTACT

MAURICE LIDDELL
Principal, National Manufacturing Industry Group – Digital Leader
mliddell@bdo.com