Data Quality and Security in Manufacturing Essential to Unlocking Industry 4.0 Benefits

Industry 4.0 has transformed manufacturing, reshaping the competitive landscape and powering innovation. By leveraging disruptive technologies such as AI and 3D printing, factories increase productivity while quickly adapting to customer demands. At the same time, the changing landscape underscores the importance of data quality and security in manufacturing.

For example, a smart factory might use 3D printing to create complex customized products on demand. Additionally, smart sensors constantly monitor for minute changes in machine health, optimizing maintenance and minimizing downtime. These improved tools and processes both require and generate huge amounts of data that must be carefully managed and protected.

Data Challenges

Modern manufacturing runs on data. And while that data opens the door to unprecedented opportunities, it also introduces significant risk. Predictive maintenance systems and supply chain optimization depend on accurate, complete, and timely data. Poor quality data, on the other hand, leads to errors, increased downtime, waste, and decreased customer satisfaction.

In addition, the huge quantities of data generated by smart factories represent a treasure trove for cyber criminals. And cloud computing, while it eases collaboration and maintenance, introduces doors for bad actors to steal intellectual property, disrupt operations, or extort ransom. IoT devices further broaden the attack surface.

Underscoring the danger, IBM's Security X-Force Threat Intelligence Index 2023 found that manufacturing topped the list of industries targeted by cyber criminals. Ransomware attacks cost manufacturers millions of dollars in lost revenue, regulatory liabilities, ransoms, downtime, and equipment damage.

Comprehensive Data Security a Must

To keep critical data safe from breach, manufacturing organizations should regularly review and update their security programs. Strategies should include tools and practices such as:

- Network segmentation – Isolate IoT devices from mainstream equipment using network segmentation. This will limit how far an attack can spread, containing any damage.
- Access management – Guard against unauthorized access by implementing MFA and least privilege access. Remember to address IoT devices. Typically designed and purchased for cost rather than security, IoT devices often fly under the radar, opening a convenient back door for attackers.
- Keep software and systems up to date – Implement patch management to ensure that security patches get applied in a timely manner. This includes keeping antivirus and anti-malware current.
- Monitor networks for anomalies – Automated 24x7 system monitoring will provide early alerts to any potential problems, especially when enhanced by AI.
- Use encryption – Implement quality encryption methods to protect data in transit and at rest.
- Ensure regular backups – Implement backup plans for critical data and systems, regular testing backups and recovery.

Information Governance Best Practices Build Data Quality

In an environment that relies heavily on data, information governance plays a critical role. Manufacturers must identify data sources and users and understand the purpose of the data. They must also be able to monitor and cleanse the data and introduce appropriate controls around data access and data lifecycle.

Data cataloging tools prove critical for locating and indexing data across the enterprise, generating a dynamic, searchable data inventory. These tools support the management of metadata that describe each data item. Metadata in turn proves critical to creating an audit trail and facilitating the process of managing the data lifecycle.

Managing data and metadata at scale requires automation, powered by AI and machine learning. Automated tools refine the process of data classification, facilitating policy enforcement and regulatory compliance while reducing errors.

However, while sophisticated tools and automation power the process, effective information governance requires a variety of human players, from asset owners and executive sponsors to individual data users.

Stakeholders must assess the current state of data and then determine data quality requirements and outline improvement actions, including evaluation metrics. End users represent the front line. As such, they must understand data security fundamentals, as well as how to implement information governance policies.

Enhance Data Quality and Security in Manufacturing with Expert Help

New technologies such as cloud computing, AI, and robotics enable manufacturers to achieve an unprecedented level of performance and innovation. That opportunity comes with risk, however, requiring a multi-faceted approach to managing and protecting critical data.

The data experts at Messaging Architects bring the tools and expertise to assist manufacturers as they design and implement cyber security and information governance best practices.