O3OZONE

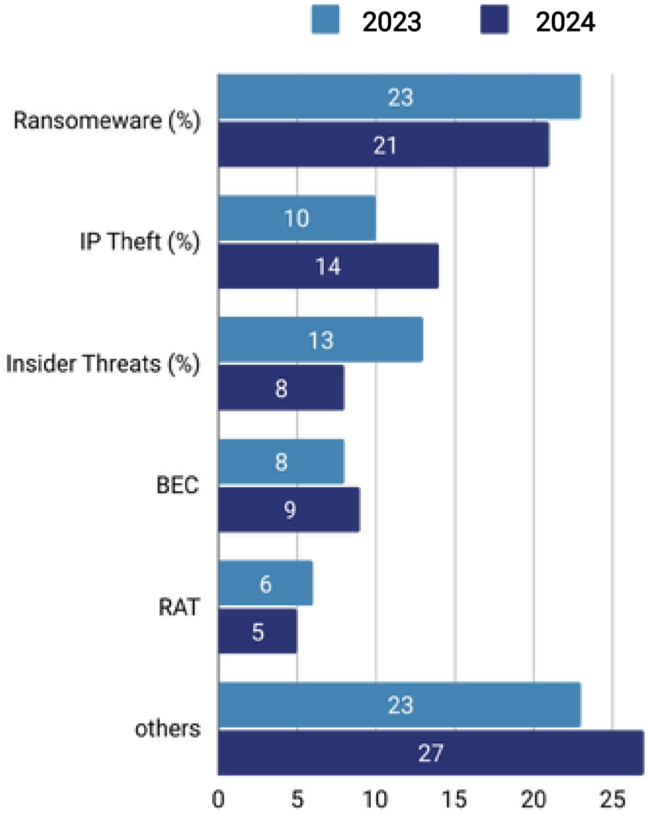
Enhancing Cybersecurity in Manufacturing Digital Solutions

Cyber Risks in Digital Manufacturing

As the manufacturing sector undergoes rapid digitalization, cybersecurity has become critical in safeguarding productivity and operational efficiency.

This white paper addresses the **cybersecurity** landscape specific to manufacturing, identifying vulnerabilities, risks, and the impacts of cyber threats.

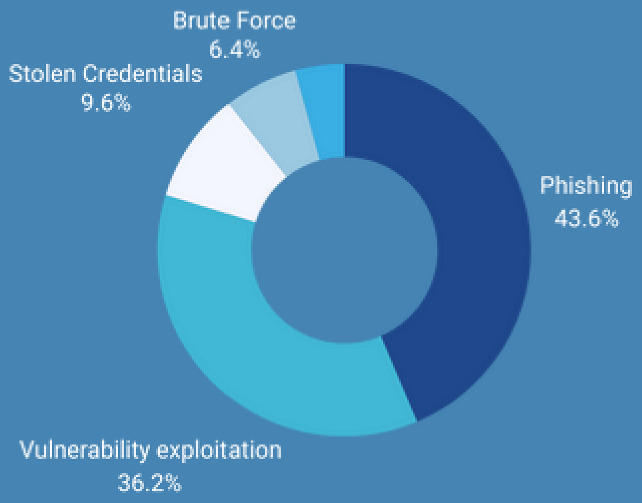
An effective cybersecurity strategy must address the specific risks and challenges that manufacturing faces:



Top attack types, 2023 Vs. 2024
Breakdown of top attack types, 2023-2024
(Source: IBM Security X-Force)

Top infection vector

X-Force Incident Response



(Source: IBM Security X-Force)

Cyber Risks in Manufacturing:

Outdated Systems

Dependence on legacy systems lacking security controls increases vulnerability.

Weak Access Controls

Limited identity and access management systems heighten risks of unauthorized access and insider threats.

IoT Vulnerabilities

IoT devices, with limited security features, introduce numerous exposure points.

Stages of Ransomware & Strategic Cybersecurity Implementation

Stages of Ransomware Attack

Exposure

30% of threats are linked to the outdated software

Infiltration

45% of attacks exploit inadequate access controls

Exploitation

Average detection time: 96 hours

Containment

Zero Trust reduces containment time by 50%

This case study details the steps involved in implementing a cybersecurity strategy in a manufacturing setting, covering assessment, framework selection, phased deployment, and results.

- **Initial Assessment and Data Collection**

  An effective cybersecurity implementation starts with a thorough assessment of the current security posture:
- **Data Collection**

  Gather baseline security data, including network traffic, access logs, and threat profiles. This data serves as a reference to measure improvements post-implementation.
- **Risk Assessment**

  Identify high-risk assets, common attack vectors, and system vulnerabilities, such as exposed IoT devices or outdated software.
- **Vulnerability Identification**

  Use the collected data to pinpoint areas requiring immediate attention, from unauthorized access risks to unpatched system vulnerabilities.

Strengthening Security Through Frameworks & Advanced Tools

Frameworks and Tools

Selecting and implementing appropriate cybersecurity frameworks and tools is critical for effective threat mitigation.

Zero Trust Architecture

Adopt a Zero Trust model to grant access exclusively to verified users and devices, reducing both internal and external threat exposure.

- **Problem**

  In 2016, Commercial International Bank S.A.E. (CIB), began a five-year strategy to improve identity and access management (IAM) and identity governance by having a zero trust setup.

- **Action**

  Implemented Zero Trust policies, requiring identity verification for every access attempt.

- **Results**

  CIB's strategy reduced manual identity governance efforts by taking over the management of more than 8,000 employee identities.

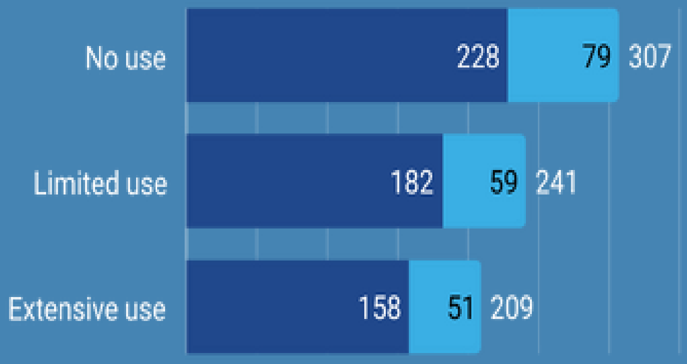
Network Segmentation and Multi-Factor Authentication (MFA)

Organizations are adopting MFA more effectively, reshaping the threat landscape by limiting credential-based attacks and reducing email takeover risks. MFA, coupled with identity management advancements, lowers the risk of ransomware, data theft, BEC, and unauthorized server access while becoming easier to implement.

AI-Driven Threat Detection

Leverage AI and machine learning for real-time threat monitoring and anomaly detection, enabling rapid response to suspicious activity

Time takes to identify and contain a data breach by AI and automation usage level *(days)*

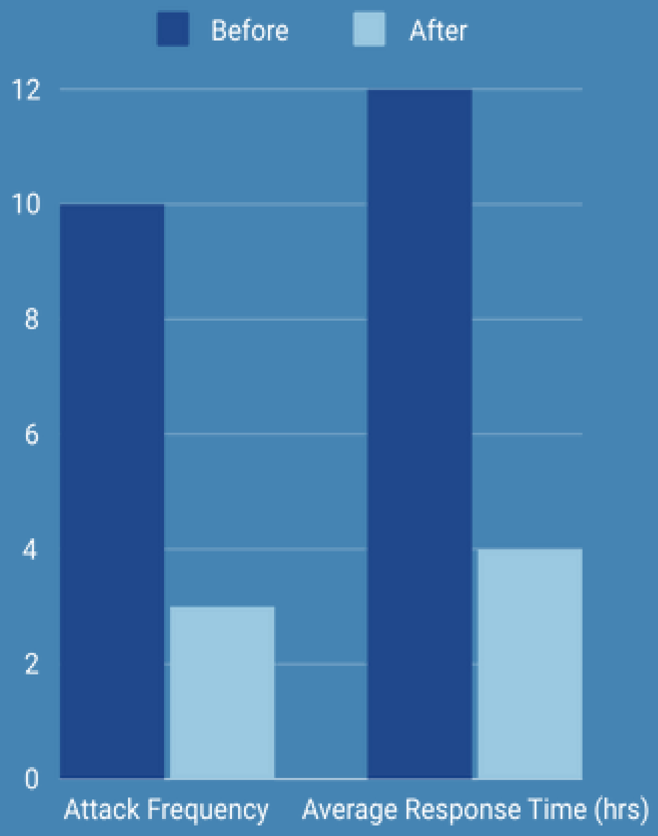


According to 2024 IBM Data Breach Report, Organizations that applied AI and automation to security prevention saw the biggest impact from their AI investments in this year's study compared to 3 other security areas: detection, investigation and response

Implementing Cybersecurity Strategies with Continuous Monitoring

Zero Trust Adoption Impact

(IBM X-Force Report)



Continuous Monitoring and Adaptation

Implement a continuous monitoring strategy with adaptive tools, such as AI-driven threat detection and advanced logging mechanisms, to quickly detect and address new threats. Regular updates to the security framework ensure resilience.

Baseline Security Assessment

This phase involves evaluating the security baseline to understand current strengths and areas requiring improvement for enhanced resilience.

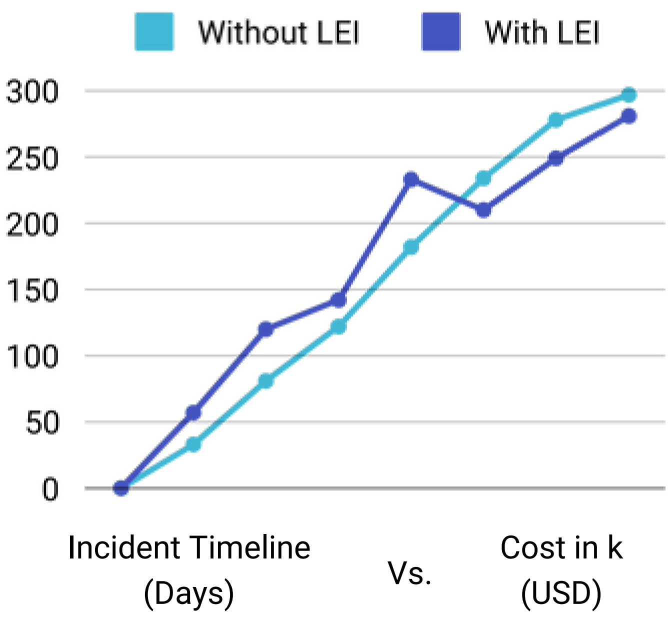
Risk Mitigation and Framework Deployment

Address identified vulnerabilities by isolating legacy systems, strengthening IoT device security, and implementing network segmentation.

This stage involves close coordination between IT and operational technology teams to align goals.

Cost Savings Chart

(Law Enforcement Involvement)



Results & Impact Analysis

Upon completing the phases, the manufacturing site observed significant security improvements:

- **Reduction in Successful Attacks**

  Incidents declined due to improved controls and faster detection of potential breaches.
- **Improved Response Times**

  Reduced mean time to detect and respond to threats led to less downtime and higher production uptime.
- **Cost Savings**

  With fewer incidents, the facility saw cost savings in response efforts, recovery time, and operational losses.

Operational Efficiency

This implementation resulted in notable improvements including fewer incidents, faster response times, and cost savings due to reduced breach impacts.

- Reduced attack frequency, quicker detection, and substantial cost reductions.
- Enhanced uptime, fewer incidents, and increased employee awareness and engagement in cybersecurity practices.

Companies using AI-driven threat detection and Zero Trust frameworks report up to a 40% drop in cyber incidents.

40% Reduction

100% *Incidents / year*

60% *Incidents / year*

Organizations applying Zero Trust frameworks can respond twice as fast to cyberattacks

(Source: IBM X-Force)

50% Reduction

96 *hrs*

48 *hrs*

Companies implementing AI in cybersecurity save an average of $1.288 million annually on breach recovery costs

(Source: IBM Data Breach Report)

45% Reduction

5.72 *million*

3.84 *million*

Monitor Batches Throughout Your Factory with O3OZONE

O3OZONE integrates with your ERP system for real-time data capture and analysis.

Using GS1 standards as a benchmark, O3OZONE allows you to scan batches at any operational stage and get up-to-date info such as machine numbers, date and time of production, and supplier details.

The O3OZONE platform includes advanced analytics and reporting tools to extract meaningful insights from traceability data. You can carry out in-depth analyses, identify trends, and forecast potential issues before they escalate.

Meet Regulatory Compliance

Many industries have strict traceability requirements and regulation, especially food and beverages, pharmaceuticals, and automotive. O3OZONE makes audits easier by collecting, processing, and analyzing traceability data and producing reports.

Improve Quality Control

Identify and address quality issues early for improved consistency. Integrating O3OZONE with your ERP for full traceability helps reduce waste and meet customer quality expectations.

Optimize Supply Chains

Reduce costs by optimizing your supply chain. Track products and components back to their origin to identify bottlenecks and inefficiencies. This leads to better inventory management, reduced lead times, and improved resource allocation.

Contact Us Today