Integrating Cybersecurity With Industry 4.0
What It Means for Manufacturing

DID YOU KNOW?

Manufacturing is now the **most targeted** industry for cybersecurity attacks.[1]

90% of surveyed manufacturing executives identify **information technology (IT) and operational technology (OT) security** as a top spend area.[2]

$105K Average **cost of a data breach** for small businesses[3]

277 DAYS Average **time to identify and contain** a data breach[1]

In one study, about **1 out of 5 breaches were the result of supply chain compromises.** These breaches took an average of 26 days longer to identify and contain and were 2.5% more expensive.[1]

The different security priorities for OT vs IT:[4,13]

Operational Technology (OT)

AVAILABILITY of operations and data,

INTEGRITY of configuration data,

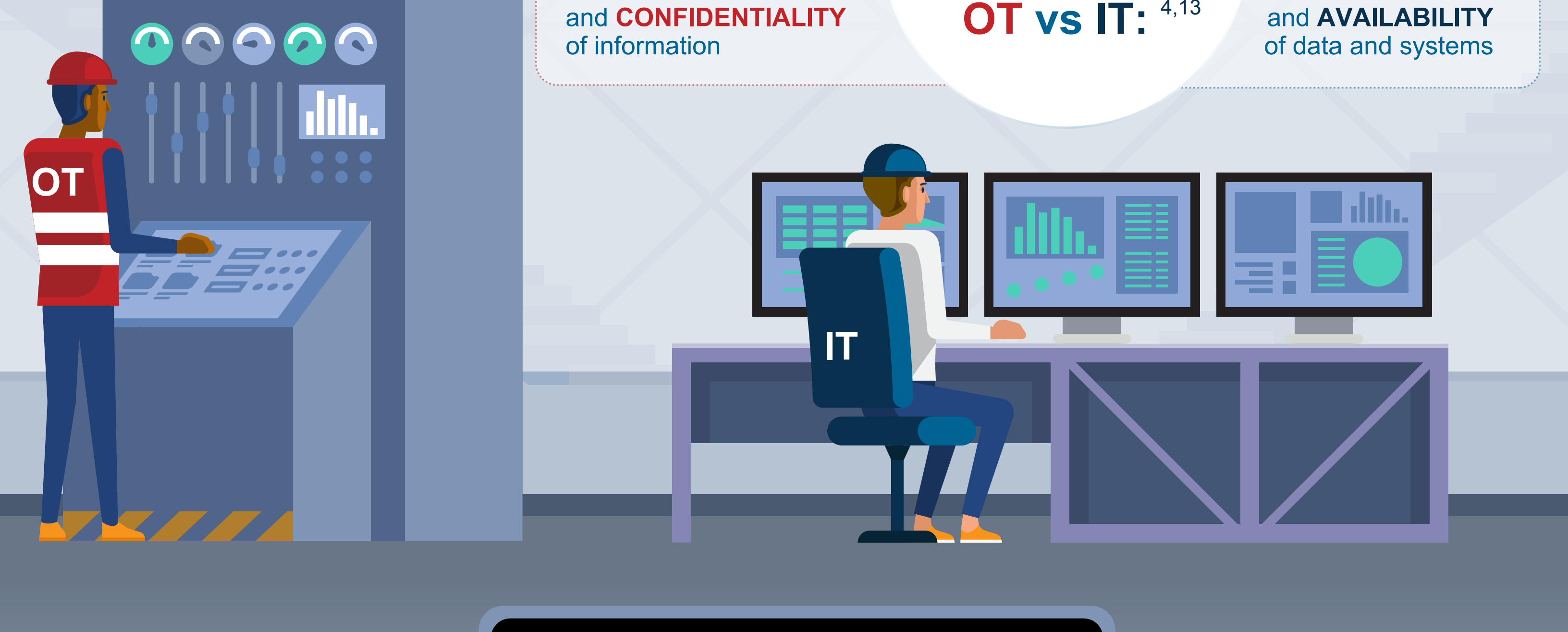
and **CONFIDENTIALITY** of information

Information Technology (IT)

CONFIDENTIALITY of information,

INTEGRITY of data,

and **AVAILABILITY** of data and systems



Balance the needs of each technology, understanding the differences in the OT and IT triads.[2]

Operational Technology	Information Technology
Automation of physical processes	Automation of information
Physical	Logical
Mix of old and new technology (up to 30 years)	Recent technology (max 5 years)
Limited cybersecurity awareness	Average-to-good cybersecurity awareness

The difference in technology lifespans means that an older IT system kept because of customization to OT equipment may become unsupported

A system that cannot be patched becomes an entry point for a breach.

For example, a Windows 10 operating system that is running machinery has little cybersecurity protection.[5]

If a system can be patched, the lag time between the patch release and its implementation becomes an entry point for a breach.[6]

INDUSTRY 4.0:
Managing Cybersecurity Where OT and IT Meet[1,2,6,7,8,9]

Identify who is responsible for ALL security aspects, including intellectual property as well as employee safety and health, to improve and integrate governance.

Collaboration among all responsible for security is key.

Adopt a zero trust security approach.

Assume user identities and the network itself may already be compromised and instead rely on artificial intelligence and analytics to continually validate connections among users, data, and resources.

Protect sensitive data in cloud environments using policy and encryption.

Traditionally, manufacturing equipment was not connected to the network. This "air gap" created segmentation, which provided some level of security. Now that OT/IT are converging, manufacturers **must enable segmentation and strong cybersecurity safeguards to guard against unauthorized users.**

Control Zones

- **Operations** e.g., Manufacturing Execution Systems
- **Supervisory** e.g., Supervisory Control and Data Acquisition
- **Basic** e.g., Programmable Logic Controller
- **Safety** e.g., Safety Instrumented Systems
- **Process** e.g., Corporate Governance Index report

Use tools that help protect and monitor endpoints and remote employees, including employees using their own devices, company computers and mobile devices.

Form an incidence response team, develop an incidence response plan and procedures, then test extensively.

READINESS: → **RESPONSE** → **RECOVERY**

Roles, responsibilities, actions

Communication is key

Plan and practice; run drills to rehearse the response to an incident

Balancing the need for:

SECURITY

Securing networks to thwart threats

SHARING

Transferring data to employees for production

Sharing information to necessary partners, suppliers, and clients[5]

HOW THE MEP NATIONAL NETWORK™ HELPS

MEP of Louisiana (MEPOL) helped ***Haydel's Game Calls***, a 12-employee, nationally recognized leader in the manufacture of quality game calls with a "blow wet" feature that sets them apart, by conducting a cybersecurity assessment and training to make sure that its sensitive and highly competitive data and processes would be secure.[9]

New Hampshire MEP (NH MEP) helped ***JMK, Inc.***, which designs, manufactures, and distributes commercial EMI/RFI powerline filters and suppression devices for commercial, military, and medical applications, engage Mainstay Technologies and performed a gap analysis for compliance to NIST 800-171. This included an action plan and milestones to achievement. The company, which had already experienced a data breach, was able to move forward with training, hardware installation, and procedures to enhance security.[10]

Manufacturing Works in Wyoming, helped ***L&H Industrial***, a leader in technology innovations, custom manufacturing, and services for heavy industrial machinery used in mining, oil and gas, railways, and other industries stay on track to continue to do business with the DOD. This included linking them with 4th State Communications to document and solidify their internal cyber standards in order to complete a NIST 800-171 assessment and submit a new system security plan.[11]

South Dakota Manufacturing and Technology Solutions helped ***Rensberger Technologies***, a manufacturer with about 15 employees who create custom precision components for aerospace, defense, and medical equipment, achieve its AS9100 certification, complete a cybersecurity compliance assessment, and develop a system security plan, along with an action plan and milestones, enabling the company to retain its customers.[12]

Need Some Guidance?

The MEP National Network™ has the resources to help you safeguard your information, your systems, your employees, and your product. Contact your local MEP Center for assistance.

Visit: **https://www.nist.gov/mep/mep-national-network** | Call: **1-800-MEP-4MFG**

MEP National Network™

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

(1) https://www.ibm.com/reports/threat-intelligence/ note: IBM Cost of a Data Breach Full Report 2022 (p. 11) [study of 550 organizations, 3600 individuals interviewed, impacted by data breaches from 3/21 to 3/22] (2) https://www.cgi.com/sites/default/files/2020-08/industry-4.0-cybersecurity-methodology-en.pdf (https://www.cgi.com/en/white-paper/manufacturing/industry-4-and-cybersecurity-how-to-protect-your-business-against-cyber-risks) (3) https://prowritersins.com/cyber-insurance-blog/average-cost-of-a-data-breach-for-small-businesses. (4) https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-critical-component-industry-40-implementation (5) https://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf (6) https://concinnity-risks.com/assets/Briefing_Cyber_Security.pdf (7) https://www.inductiveautomation.com/blog/the-benefits-of-integrating-your-mes-system-with-scada] (8) https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf (9) https://www.nist.gov/mep/successstories/2022/great-progression-hub-cybersecurity (10) https://www.nist.gov/mep/successstories/2022/compliance-nist-800-171-cybersecurity-ensures-growth-jmk-inc (11) https://www.nist.gov/mep/successstories/2021/lh-industrial-path-government-contracting (12) https://www.nist.gov/mep/successstories/2022/precision-manufacturer-finds-fast-growth-service-aerospace-defense (13) https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence