Evolving OT Cybersecurity Posture in Manufacturing

By: **Ed Lee**, Research Director, Security & Trust

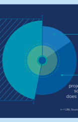
OT and IT Integration Creates Opportunities

While sensitive operational technology (OT) functions remain air-gapped, OT systems are increasingly being connected to information technology (IT) networks.

IT/OT interconnectivity delivers multiple benefits.

n = 1,028, Source: IDC's *WW IT and OT Convergence Survey*, July 2022

47% of companies who have implemented Industrial Internet of Things (IIoT) projects have **realized rapid payback.**



15% have executed IIoT projects and have yet to realize any value.

38% have executed IIoT projects and, although realized some value, the current cost does not justify the expenditure.

n = 1,316, Source: IDC's *Future of Operations Survey*, July 2022

Whether connected or not, both need to be shielded from external and internal bad actors.

IT/OT Integration Increases Security Risk

Many OT systems in use today are decades old, run by outdated hardware, and may use connected IoT devices that cannot be updated or patched, creating security risks.

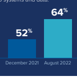
A successful ransomware attack could shut down a manufacturing facility, resulting in thousands to millions of dollars in actual costs and lost productivity.

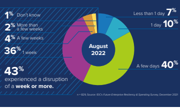
In 2021, **10%** of the 649 complaints the IC3 received were from the critical **manufacturing sector.**

Source: FBI Internet Crime Complaint Center (IC3) Annual Report, 2021

Ransomware is a major attack outcome.

64% of enterprises have experienced a ransomware attack/breach that blocked access to systems and data.





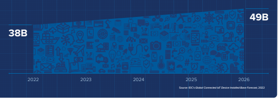
43% experienced a disruption of a **week or more.**

n = 829, Source: IDC's *Future Enterprise Resiliency & Spending Survey*, December 2021

The IoT Attack Surface Is Huge

Digital transformation is driving factory-floor connectivity; and IoT devices are deployed in many critical applications in manufacturing as well as other industries.

By 2026, IDC forecasts there will be over 49 billion connected IoT devices in place, up from 38 billion in 2022.



Source: IDC's *Global Connected IoT Device Installed Base Forecast*, 2022

From a device management/security perspective, manufacturers rank their concerns around IoT deployment:

Manufacturing	
1	Who can access data generated by IoT devices
2	Protecting IoT data in movement and data at rest
3	Lack of security tools designed for OT environments

n = 1,792, Source: IDC's *US IoT Decision Maker Survey*, July 2021

There is need for a *"self-defending manufacturing floor"* – one that is able to identify, prevent, and adapt to threats from both internal and external sources.

Breaches of OT Networks Likely to Start in IT Networks

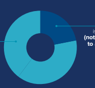
A potential breach of an OT network is more likely to start in the IT network.

Over **25,000** new Common Vulnerabilities and Exposure (CVEs) records were recorded in 2022; only about **6% were assigned** specifically to OT products.

Source: CVE.org & IDC, 2023

More remote workers and more OT systems are being monitored remotely, creating opportunities for sophisticated attackers.

Air-gapped systems still require a comprehensive on-site security program, as all it takes is one unsecured USB port to compromise an organization.



78% of instrumented operational equipment **is connected.**

22% is air-gapped **(not connected to a network).**

Source: IDC's *IT/OT Convergence Survey*, 2022

IT Plays a Major Role in Managing and Protecting OT Systems

Companies' cybersecurity plans should include:

- An inventory of connected devices and their configurations
- A catalog of their vulnerabilities
- A strategy for thwarting attacks and responding when there is a successful breach

IT analysts (for their cybersecurity knowledge) and OT engineers (for their OT knowledge) need to work closely together.

84% describe that **IT supports** the IT infrastructure used by OT systems/organizations, and some or all of the OT systems.

16% describe that **IT does not support** OT systems.

54% IT supports IT infrastructure used by OT systems/organizations, and **some of the OT systems.**

30% IT supports IT infrastructure used by OT systems/organizations, and **all of the OT systems.**

15% IT supports IT infrastructure used by OT systems/organizations, but **not the OT systems.**

1% **IT does not support IT infrastructure** used by OT systems/organizations.

n = 1,028, Source: IDC's *WW IT and OT Convergence Survey*, July 2022

Resource-constrained companies are turning to managed service providers (MSPs), who can step in to assist with both:

1. improving security, and
2. fulfilling regulatory and compliance requirements.

S M L

53% of small to medium-sized businesses expect to use an MSP for operations cybersecurity within 3 years.

Message from the Sponsor

BlackBerry | Cybersecurity

Establishing a Self-Defending Manufacturing Floor

Whether operational technology systems are air-gapped, connected, or somewhere in between, an endpoint solution should eliminate complexity, deliver proven security, and enable uninterrupted evolution. BlackBerry can help establish a self-defending manufacturing floor, delivering a lightweight presence on endpoints - without the need for signatures, heuristics, or even internet connections.

Secure OT-Based Environments

IDC

CA50491123