Apperture SOLUTIONS

OT Cybersecurity 101

Fundamentals of Protecting Industrial Control Systems

Steve Allison

Senior IT/OT Engineer

Agenda

- Understanding OT Cybersecurity and Its Importance
- IT & OT Differences
- Common OT Threats and Weaknesses
- Real World Examples
- Frameworks and Governance
- Administrative and Technical Controls
- Summary
- Q&A

What is Operational Technology (OT)?

Operational Technology (OT)

Operational Technology includes hardware and software that monitor and control physical industrial devices and processes.

Examples of OT Systems

Common OT systems include HMIs, PLCs, DCS, and ICS used in manufacturing, energy, and utilities sectors.

OT vs IT Systems

OT systems manage physical processes, unlike IT systems which focus on data and information management.

Why OT Cybersecurity Matters

- Convergence of IT and OT has expanded the attack surface
- Attacks within OT space and growing faster than any other sector with Ransomware attacks increasing by 87% in the last year
- Regulatory and customer pressure is rising
- Cyber insurance requirements are tightening
- Downtime in the OT space is costly

IT vs OT – Key Differences

ASPECT	IT FOCUS	OT FOCUS
Priority	Confidentiality	Safety & Availability
Lifecycle	3-5 Years	15-30 Years
Patch Management	Frequent updates	Limited due to availability
Impact	Data loss	Physical process disruption

Cybersecurity Triad IT vs OT

IT Cybersecurity Triad

- **Confidentiality:** Focuses on protecting data from unauthorized access and breaches.
- **Integrity:** Ensuring that data is accurate and unaltered is the second priority.
- **Availability:** It ensures that systems and data are accessible when needed, but not at the expense of confidentiality and integrity

OT Cybersecurity Triad

- **Availability:** In OT, Systems must always be operational and accessible.
- **Integrity:** Maintaining the accuracy and reliability of data used to control physical processes.
- **Confidentiality:** Although still important , the focus is more on ensuring that systems are running smoothly and safely.

Common OT Threats & Weaknesses

Malware Targeting OT Environments

- Ransomware spreading from IT into OT and encrypting HMIs, historians, or workstations
- Wipers that render controllers or systems unusable

Legacy and Unpatched Systems

- End-of-life equipment or inability to patch without downtime
- Known vulnerabilities left exposed for years

Flat Networks & Poor Segregation/Segmentation

- No Effective Containment During an Incident
- Expanded Attack Surface
- No DMZ between IT and OT

Unauthorized Remote Access

- VPNs without MFA
- Externally Exposed RDP or VNC
- Vendor remote access
- Temporary access that was never revoked

Real World Examples

Consequence

- Factories & some supplier factories shut down for over a month
- $890M estimated losses
- $2.5B estimated losses to UK economy

Detail (August 2025)

- Presumed ransomware but not confirmed
- Employee data also stolen
- $2B load from UK government for recovery

Consequence

- Halted all production for 5 days
- Ran in “Emergency Mode” until full restoration about 1 week later

Detail (June 2025)

- Qilin ransomware group – RaaS
- No details on what all systems IT vs OT were affected/disabled by Ransomware

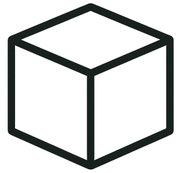
SILOKING

Consequence

- Halted operations at dozens of tire manufacturing & retreading plants in North and South America including Aiken, SC.

Detail (September2025)

- Few other details exposed
- No evidence of customer or employee data being exposed
- Promises a full report



Frameworks – Standardization Enables Secure Operations

- Establishes Consistent, Repeatable Security Practices
- Aligns Cybersecurity to Operational Risk
- Enables Measurable Maturity and Improvement
- Demonstrates Due Diligence and Regulatory Compliance
- Examples: Such as ISA/IEC 62443 and NIST CSF

Governance – Structure Anchors your OT Cyber Journey

- Defines Roles/Responsibilities, Accountability and Ownership
- Clearly Defined OT Cybersecurity Policies and Procedures
- Risk-based decision making

Administrative Controls

- **Governance –** Roles and Responsibilities, Accountability and Ownership
- **Policies and Procedures –** Used to structure the program
- **Training –** Awareness training and role-based training
- **Compliance, Oversight and CI –** Assessments, Audits and Performance Metrics

Technical Controls

- **Network Security –** Network Segregation & Segmentation, Firewalls, Jump Server, NAC
- **System & Device Security –** Endpoint protection, Allow-Listing, B & R, SIEM
- **Identity and Access Management –** Role Based Access Control (RBAC), MFA, PAM
- **Data & Application Security –** Encryption, Secure Protocols (SSH)
- **Physical & Environmental Security –** Access Control Systems, Camera Systems, Control Cabinets Locks, Environment sensors

Summary and Key Take Aways

- **OT cybersecurity is fundamentally about safety, availability, and reliability:**
  - Protecting industrial operations means preventing cyber events that can disrupt physical processes, production, and safety—not just data.
- **IT and OT have different risk priorities and constraints:**
  - OT systems have long lifecycles, limited patching windows, and real-world consequences, requiring security approaches designed specifically for industrial environments.
- **The OT threat landscape is growing and increasingly targeted:**
  - Ransomware, malware, insecure remote access, and flat networks continue to be the most common causes of OT incidents and downtime.
- **Frameworks and governance provide the foundation for success:**
  - Clear ownership, defined roles, and alignment to standards like ISA/IEC 62443 and NIST CSF enable consistent, risk-based decision making.
- **Effective OT cybersecurity requires both administrative and technical controls:**
  - Policies, training, and oversight must work together with segmentation, access control, endpoint protection, and monitoring.
- **Cyber resilience in OT is a journey, not a one-time project:**
  - Continuous improvement, regular assessments, and operational alignment are key to reducing risk and maintaining secure, reliable operations.

Questions?