Deloitte.

Enhancing Operational Technology Cybersecurity

Approach for taking strategic steps to better protect our OT environments

Adam Mack

Senior Manager,
US Cyber & Strategic Risk

Deloitte & Touche LLP

Jason Frost

Manager
US Cyber & Strategic Risk

Deloitte & Touche LLP

Discussion Plan for Today

01 **Operational Technology and cybersecurity**

02 **OT cyber attack impacts**

03 **OT cybersecurity approaches to risk reduction**

OPERATIONAL TECHNOLOGY CYBERSECURITY, AND CONSEQUENCES

Interactive Question 1

Do you know what the term **Operational Technology** means?

A. Not at all

B. Heard of it, but unsure

C. Yes, I’m familiar

Introduction to Operational Technology (OT)

OT System Examples

Operational Technology can be known as:

- **IIoT** – Industrial Internet of Things
- **CPS** – Cyber Physical Systems
- **ICS** – Industrial Control Systems

While associated closely with manufacturing, utilities, oil and natural gas sectors, **OT is in use in just about every industry you can think of**. In fact OT is critical to the effective operation of data centers.

Challenges of OT Cybersecurity

Industrial or OT security has been underexposed in the past decades, which left most of the production facilities open to the modern cybersecurity threats.

RISK

Exponential Growth

- **Prioritized productivity** often leads projects to neglect the security imperative, thereby increasing the risk exposure.
- **Evolving threat landscape**, driven by exponential growth in modern technologies, frequently disrupts production.
- **Outdated Operational Technology** lacks vendor support.

URGENCY

Historical Debt

- **Industry 4.0 imperative** requires real time transparency into production, heightening connectivity.
- **Complex transformations** require cost-effective solutions, demanding swift value delivery.
- **Regulations on the rise** demand ongoing investment and broader transformation efforts for compliance and resilience.
- **Cyber debt** has widened due to historical lag in OT security investments.

OPERATIONS

Not In Control

- **Risk management processes** are inconsistently applied across IT and OT domains, leading to a lack of visibility and control over OT operations.
- **Lack of end-to-end thinking** results in fragmented point solutions, impeding comprehensive risk management.
- **Inconsistencies and lack of transparency** prevail across vendors and supply chains due to variations in methods and maturity levels.

OT Cybersecurity Risks and Consequences

When an OT environment is compromised, more than just data is at risk. With systems that can physically manipulate their surroundings, the risks of an incident can affect lives, the environment, assets and more in the worst cases.

What happens when OT environments are compromised?

Physical safety concerns

People and environmental safety risk

Loss of time, product, assets, services, revenue

Shutdown of manufacturing floor and/or damage to machines, and downtime

Impaired operations and judgement

Wrong decision making due to altered or loss of data from sensors

Reputational damage

Potential loss of trust from workforce, customers, vendors, public

Interactive Question 2

Now that you know what **Operational Technology** means, can you identify it in your workplace?

A. Yes

B. No

C. I’m still not sure

HOW WE START
APPLYING FUNDAMENTAL OT SECURITY CONTROLS

Strategic Approaches for Maximizing OT Cybersecurity Risk Reduction

Alignment between business, OT, and IT
(Consistent Governance Program)

Enhanced response and recovery capabilities

Centralized OT cybersecurity monitoring

Improved OT asset visibility and understanding

Enhanced network segmentation

Improved management of access
(employees and vendors)

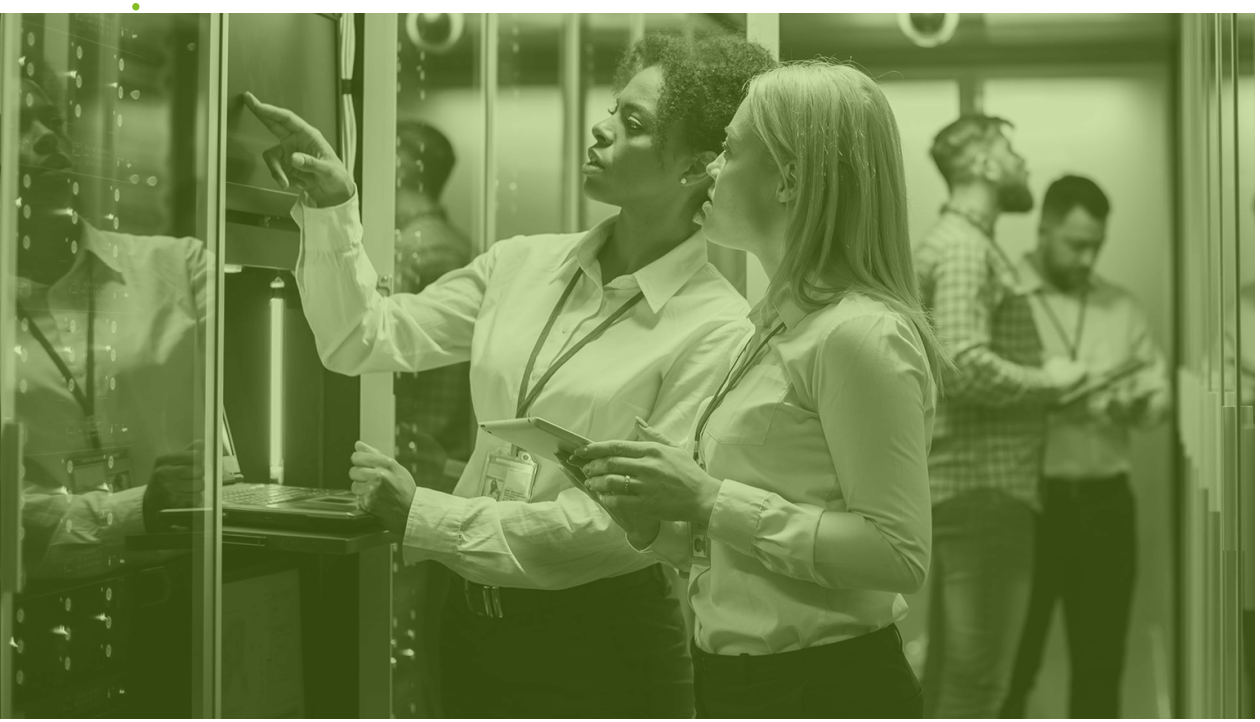
1 Improved OT asset visibility and understanding

Challenge: *Today technology asset details for OT environments are often manually collected. Asset inventories across sites are inconsistent and limited consideration is given to cybersecurity risks.*

- Enables us to more efficiently and effectively maintain our asset inventories
- Through our improved understanding of OT assets, risk assessments can be more focused
- Enhanced understanding of technology communications is gained, which can be leveraged when completing network segmentation efforts and during other projects
- Logs from automated visibility solutions become an enabler for continuous monitoring

2 Enhanced network segmentation

Challenge: *Many company networks are flat and business/OT assets are intertwined. Segmentation that exists is through virtual local area networks (VLANs), which do not provide an appropriate level of cybersecurity protection.*



- Initial efforts should focus on limiting connectivity based on valid business requirements – securely separating IT from OT using physical firewalls
- Additional segmentation efforts should consider systems risks and operational requirements before being undertaken
- Direct internet connectivity to OT networks should not be allowed. If access is required in higher levels, it should be minimized based on business case and tightly controlled
- Windows Active Directory structures should be a focus during segmentation efforts for OT environments

3 Improved management of access

Challenge: *Access across locations is often inconsistently managed and administrator access is pervasively assigned to more easily enable operations. Third parties are also granted access that is more extensive than is required.*

- Administrator access should be granted to a small number of users
- System/generic accounts should be tightly controlled
- A consistent secure remote access solution should be used – when other solutions are required, cybersecurity evaluations should be performed
- Access for both employees and third parties should be part of the access management program – periodic reviews of access granted should be performed
- Roaming engineering laptops and removable media should be tightly controlled

Interactive Question 3

Which of these physical access security issues have you seen before?

A. Allowing “piggybacking” badging entry

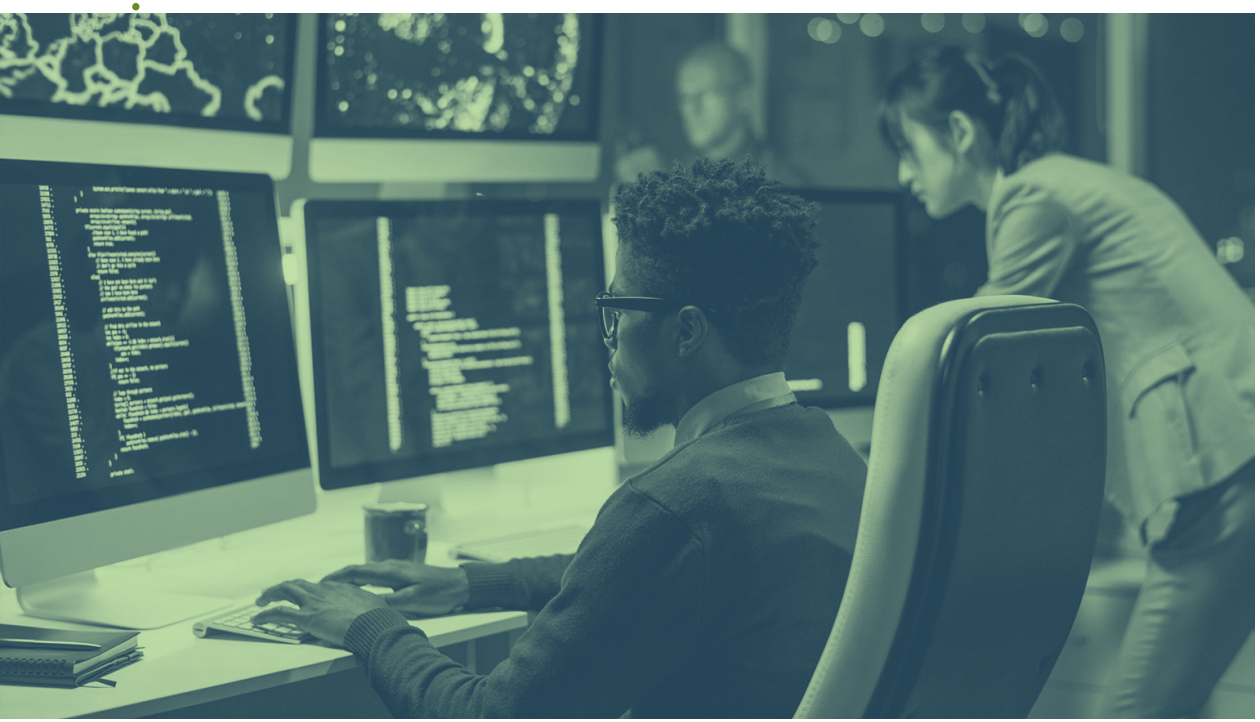
B. Shared passwords on common computers

C. Guests and/or vendors using enterprise Wi-Fi

D. All of these

4 Centralized OT cybersecurity monitoring

Challenge: *Many companies cannot identify if a cybersecurity event is occurring unless it physically effects a process within OT. When an event does occur, there is confusion around who should complete the research required and begin to work the response.*



- Centralized monitoring (Security Operations Center (SOC)) should be established that focuses on identifying indicators of compromise and vulnerabilities
- Key contacts across the company should be identified so it is understood who to contact when feet on the ground are needed
- SOC Analysts can operate as the quarterbacks when indicators of compromise are being researched and responded to
- Business value can be created through alerting at the asset level – identifying when configuration or other changes are made
- Ability to hunt threats and model impact for cybersecurity risk scenarios should be enabled

5 Enhanced response and recovery capabilities

Challenge: *Within business operations, companies seldom consider the risk of physical events (earthquake, fire, tornado, hurricane, etc.), but have not considered cybersecurity events. Even if response plans are documented for cybersecurity, they are seldom tested.*

- The ability to detect if an event is occurring within an environment timelier is needed
- Playbooks should be created that provide direction when the team is having to respond – responders are different in OT because site level personnel need to have a role
- Consistent processes are needed for taking backups at the site level
- Once incident response plans have been created, testing of those response plans should occur
- Lessons learned from testing exercises should be integrated into plans and controls

6 Alignment between business, OT, and IT (Governance)

Challenge: *Roles and responsibilities for OT cybersecurity are rarely understood across stakeholders. Cybersecurity is often an afterthought and there is not a defined strategy for driving consistency.*

- Ownership should be defined across IT and OT team members
- Cybersecurity services are documented, and roles/responsibilities assigned down to the site level
- A consistent control framework should exist
- Documented policies and standards are needed
- A consistent OT cybersecurity risk assessment framework should be defined that that considers safety, quality, and business operations
- A training and awareness program specific to OT cybersecurity should be established
- Metrics (KRIs and KPIs) should be defined to measure the effectiveness of the OT cybersecurity program

Interactive Question 4

Which of these is not an approach to reduce OT cybersecurity risks?

A. Governance Alignment

B. Network Segmentation

C. Plugging found USBs into computers

D. Centralized Security Monitoring


Questions?

Deloitte.