ALSTON & BIRD

DRAGOS

Attacks on the Supply Chain and Critical Infrastructure: What you Need to Know and Steps you Need to Take

June 16, 2021

Ben Miller
Vice President, Services and R&D
Dragos

Amy Mushahwar
Partner
Alston & Bird

Kim Peretti
Partner
Alston & Bird

Agenda

- **Critical Infrastructure – Overview**
  - What is critical infrastructure?
  - ICS and OT
  - Legal frameworks
  - Biden Executive Orders to Improve the Supply Chain
- **Current Threat Environment**
  - Risks/Threats
  - Ransomware
- **Prevention & Proactive Steps**

Critical Infrastructure – Overview

"**16 critical infrastructure sectors** . . . considered so **vital to the United States** that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety"

U.S. Patriot Act, 42 U.S.C. 5195c(e)

- Chemical Sector (DHS)
- Commercial Facilities Sector (DHS)
- Communications Sector (DHS)
- Critical Manufacturing Sector (DHS)
- Dams Sector (DHS)
- Defense Industrial Base Sector (DOD)
- Emergency Services Sector (DHS)
- Energy Sector (DOE)
- Financial Services Sector (Treasury)
- Food and Agriculture Sector (USDA/HHS)
- Government Facilities Sector (DHS/GSA)
- Healthcare & Public Health Sector (HHS)
- Information Technology Sector (DHS)
- Nuclear Reactors, Materials & Waste Sector (DHS)
- Transportation Systems Sector (DHS/DOT)
- Water & Wastewater Systems Sector (EPA)

Critical Infrastructure – Overview (Cont'd)

ICS, DCS and OT

ICS/DCS: Industrial Control Systems / Distributed Control Systems

- Information systems that control industrial processes (e.g. manufacturing, production, distribution)
  - Supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets

OT: Operational Technology / Corp Link

- Programmable systems or devices that interact with the physical environment or manage devices that interact with the physical environment to detect or cause a direct kinetic change

Critical Infrastructure – Overview (Cont'd)

Current legal frameworks

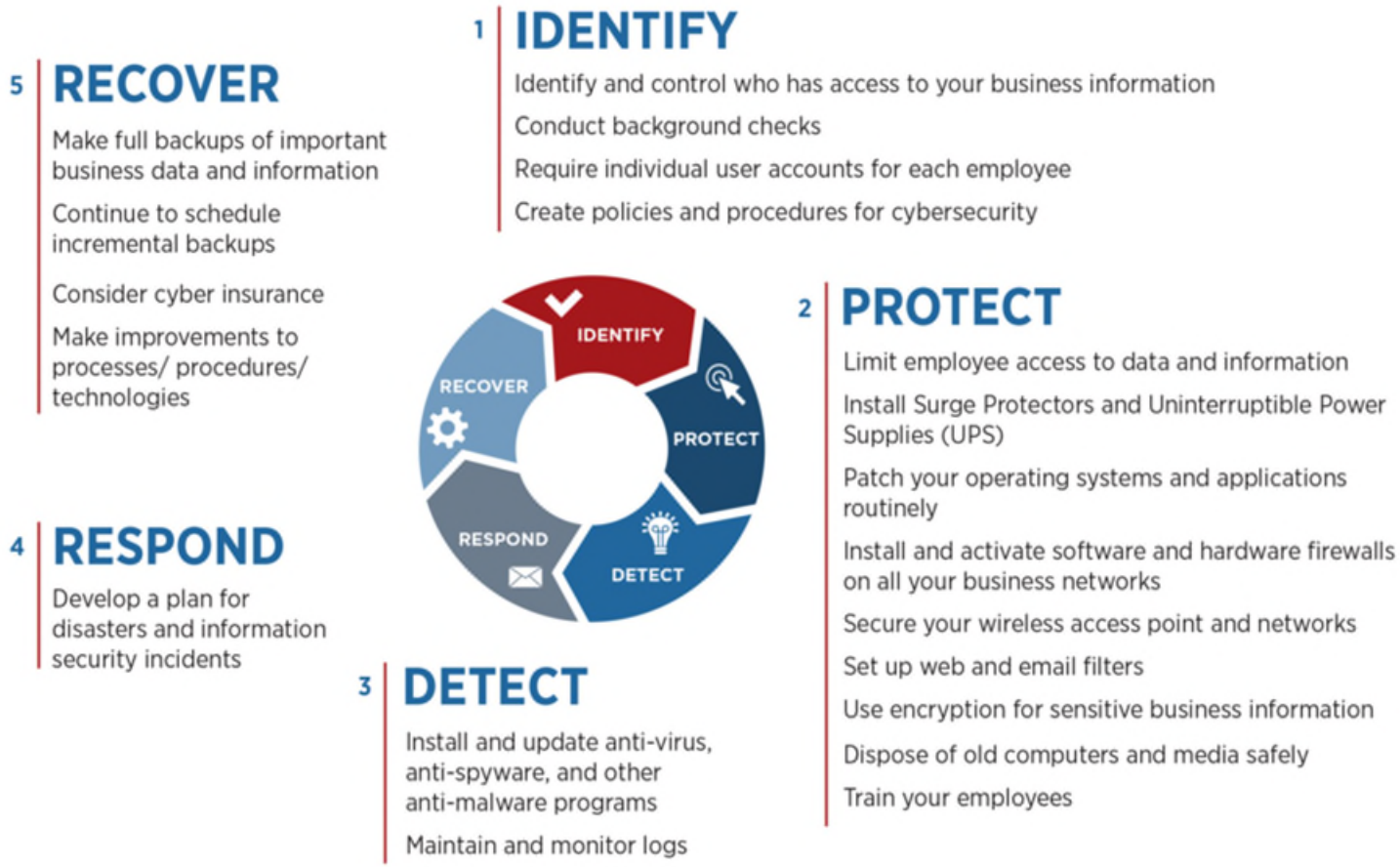
Varies by sector, with DHS-facilitated working groups working to develop and coordinate cyber risk management activities as well as a Cross-Sector Cybersecurity Working Group highlighting cyber dependencies and interdependencies across sectors

- Chemical Sector: Risk-Based Performance Standards (RBPS) 8 – Cyber
- Dams Sector: Dams Sector Cybersecurity Framework Implementation Guidance

- Defense Industrial Base Sector (some unique treatment due to involvement of classified information and that DIB primarily works with govn't contractors and NIST standards)
- Healthcare & Public Health Sector: National Health Security Strategy and Implementation Plan

Critical Infrastructure – Security Framework

- Current legal frameworks are generally guided by the NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1
  - 5 Framework Core Functions for all sectors
  - Higher-level rollup and framing tool for more granular NIST standards.



CI /Supply Chain Linkage Background

- Solarium Commission
- CBO
- NIST (IS Standardization)
- CISA (PP Info Sharing)

Executive Orders – Improving the Supply Chain

Executive Order 14017: "America's Supply Chains"

- Gov't wide approach to assessing vulnerabilities in, and strengthening the resilience of, critical supply chains
- ICTS supply chain and other sectors under review in response to pandemic concerns

Executive Order 14028 "Improving the Nation's Cybersecurity"

- To identify, deter, protect against and respond to cyber attacks that threaten the public and private sectors
- Promulgating new cyber proactive and breach reporting standards under the FAR

Executive Orders – Improving the Supply Chain

Executive Order 14028: Improving the Nation's Cybersecurity (cont'd)

- **NIST to publish:**
  - Preliminary guidelines by November 8, 2021
  - Guidance that identifies practices that enhance software supply chain security, with references to standards, procedures, and criteria by February 6, 2022
  - Additional guidelines, including procedures for periodically reviewing and updating guidelines, by May 8, 2022
- **Increased NIST guidance for "Critical Software"**
  - NIST to define "Critical Software" to be published by June 26, 2021
  - Guidance outlining security measures for critical software to be released by July 11, 2021
- **Minimum standards for vendors' testing of their software source code to be released by July 11, 2021 after consultation with NSA**

Current Threat Environment

Threat Environment Challenges

As ICS owners and operators adopt new technologies in their digital transformation efforts to improve operational technology risks emerge:

- Expanded digital attack surface (and perhaps public network exposure),
- Greater integration of OT and ICS within general production IT – we cannot assume that newer deployments are segmented/air gapped, and
- Increasing susceptibility to cyber attack given systems integration (OT and ICS can use commonly-available IT).

OT/ICS Subject to Common Attacks

As well as connected corporate infrastructure

- Ransomware
- Malware
- DDoS
- Direct vs. Indirect Infection

Network Segmentation

Level 4

Level 3.5

Level 3

Level 2

Level 1

Safety Zone

Proxy Server

BLAN

Vendor Network

VM Env

DMZ Apps

Plant Info Zone

FTP Servers Dynamo Servers

Backup & Recovery Zone

Operator Workstations

Domain Controllers

DCS

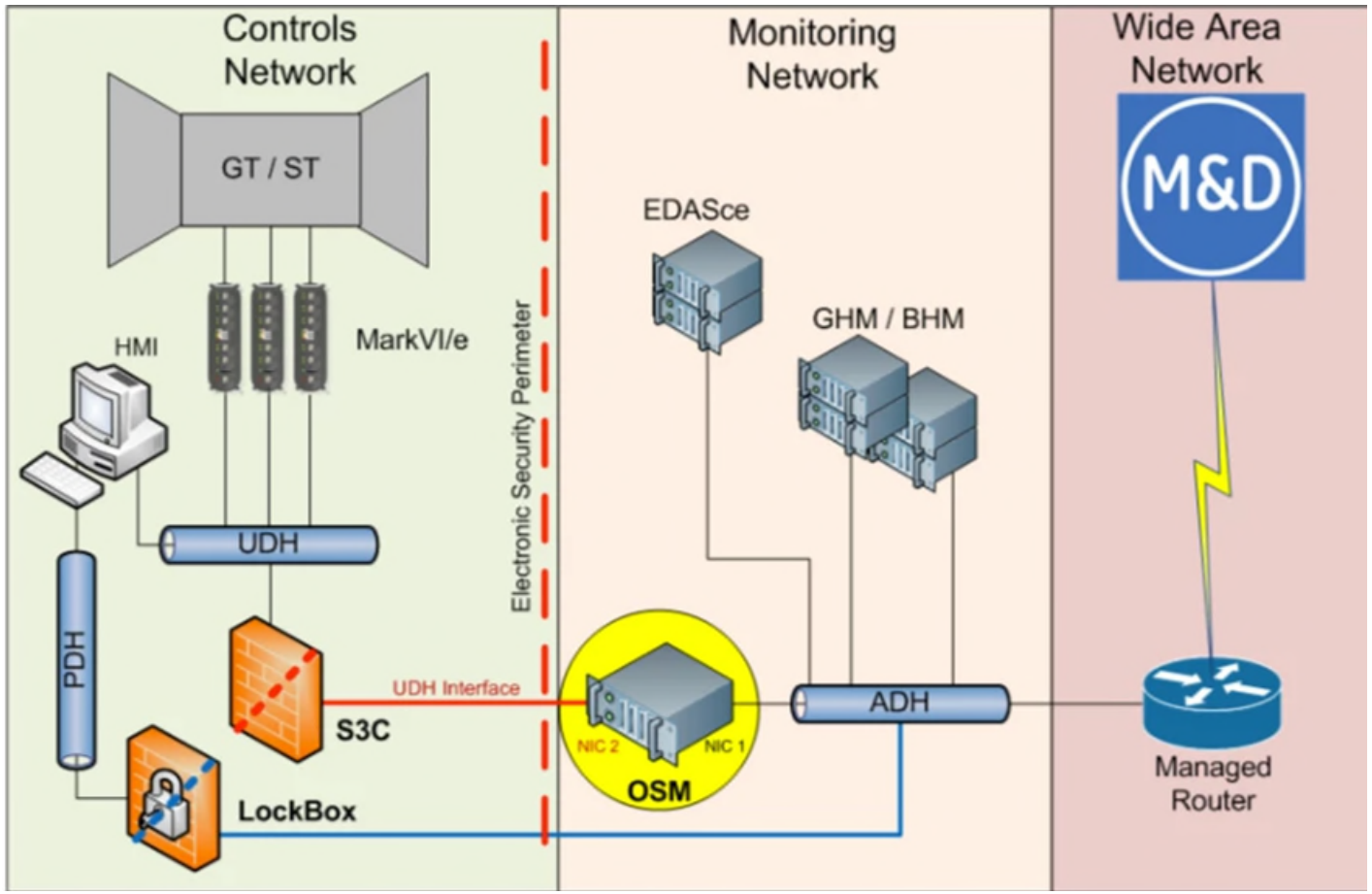
PLCs

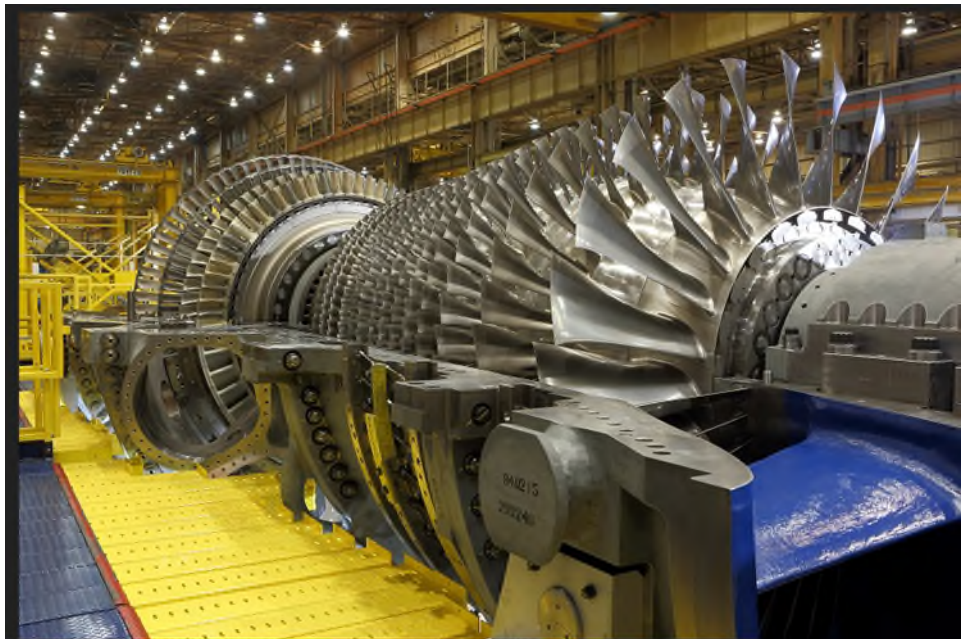
RTUs

Compressors

SIS controllers

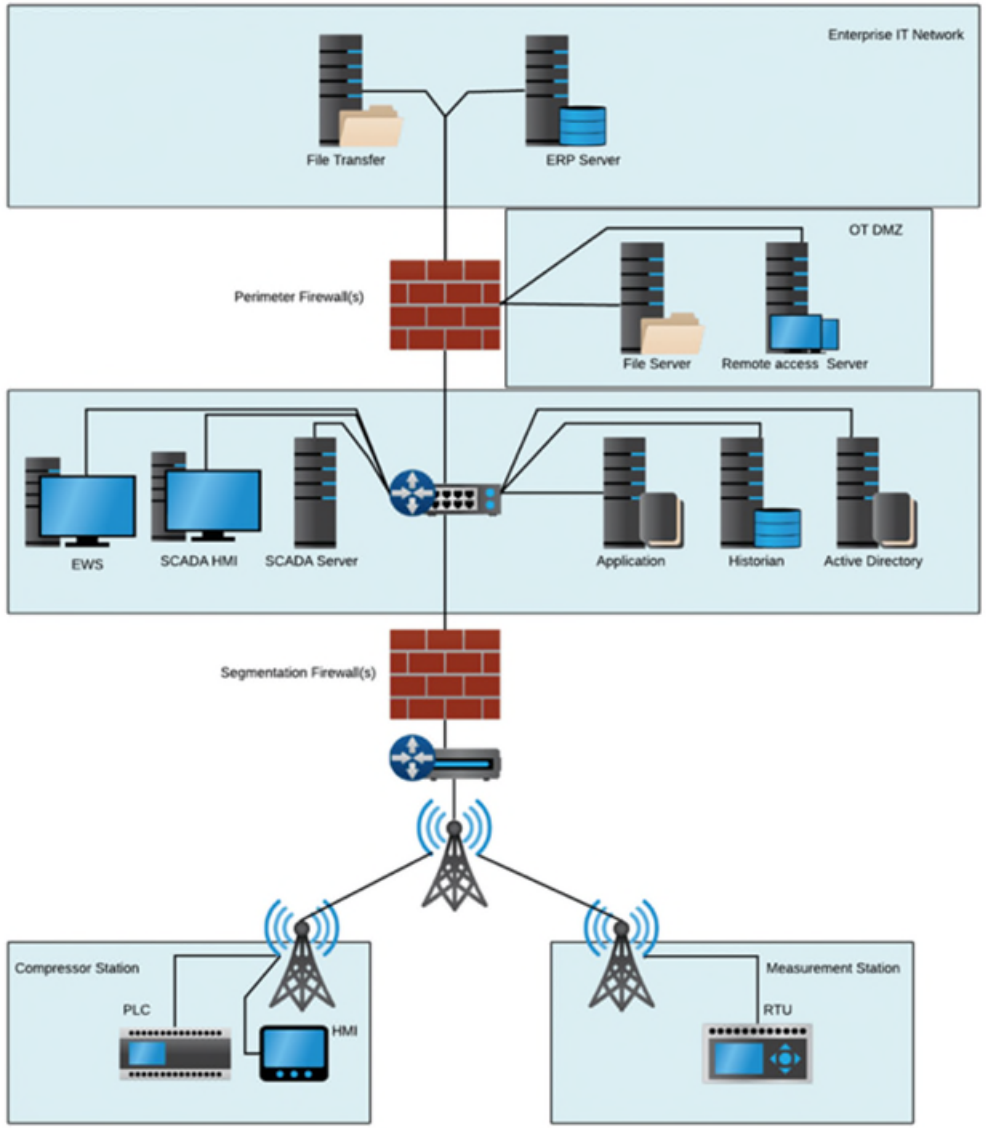
Supply Chains: Direct Connections to OEMs





ICS/OT Architecture

- Provide segmentation (zones) and isolation boundaries between systems of higher or lower trust
- Understand what happens when systems are isolated
- Limit protocols that Ransomware tends use for zone-to-zone movement (e.g., RDP, SMB, NTLM)
- Leverage network monitoring and visibility to detect and respond to malicious behaviors

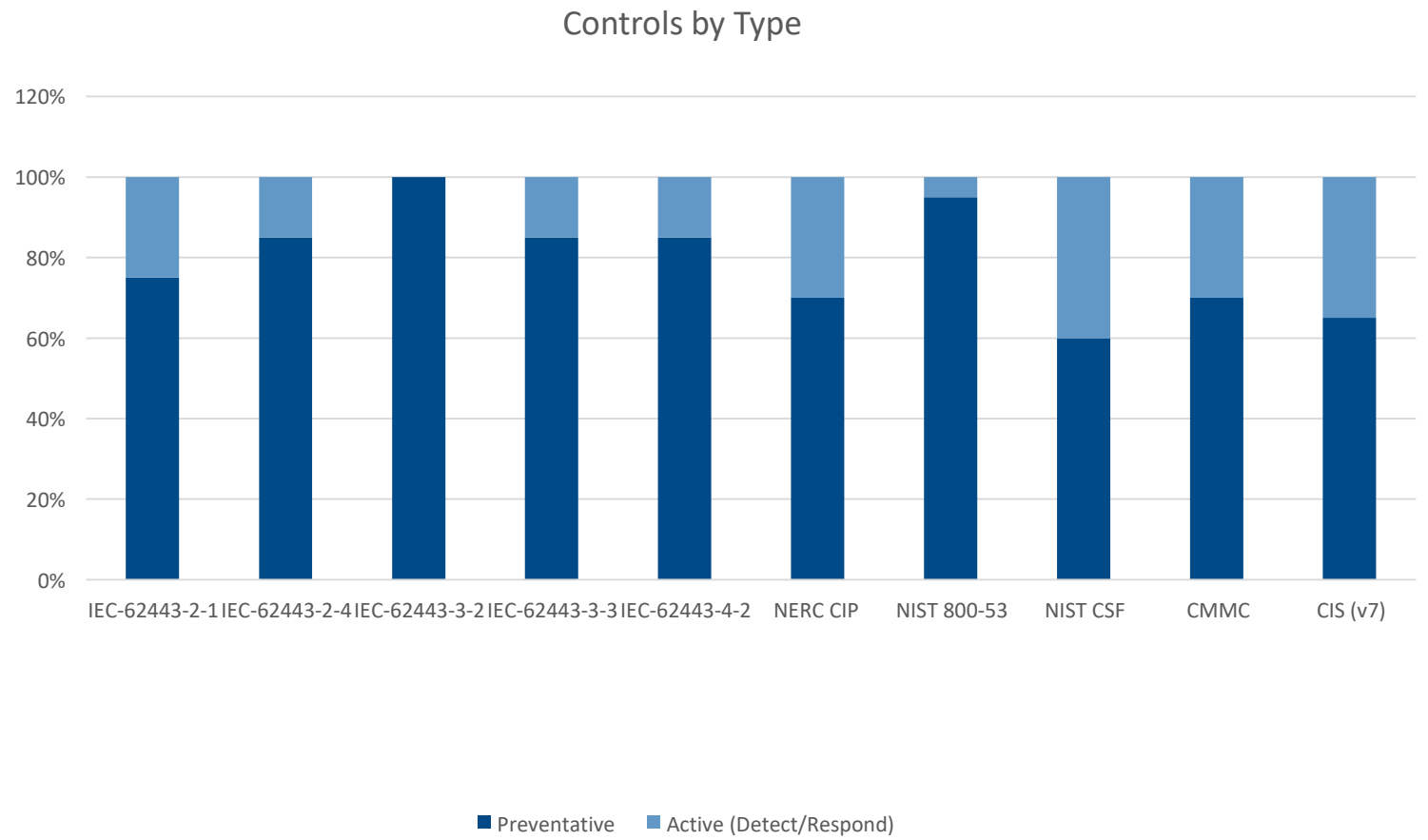


16

Prevention & Proactive Steps

Why Are We Here?

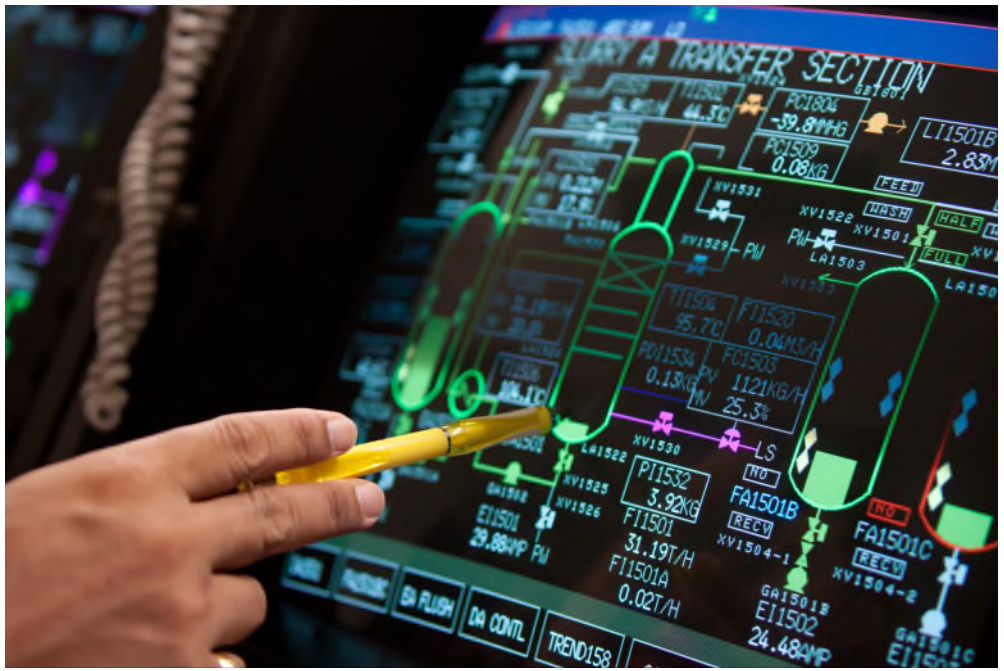
- OT is heavily influenced on standards
- Standards focus on prevention



ALSTON & BIRD | DRAGOS

Starting the Technical Ownership Conversation: Key Questions to Ask

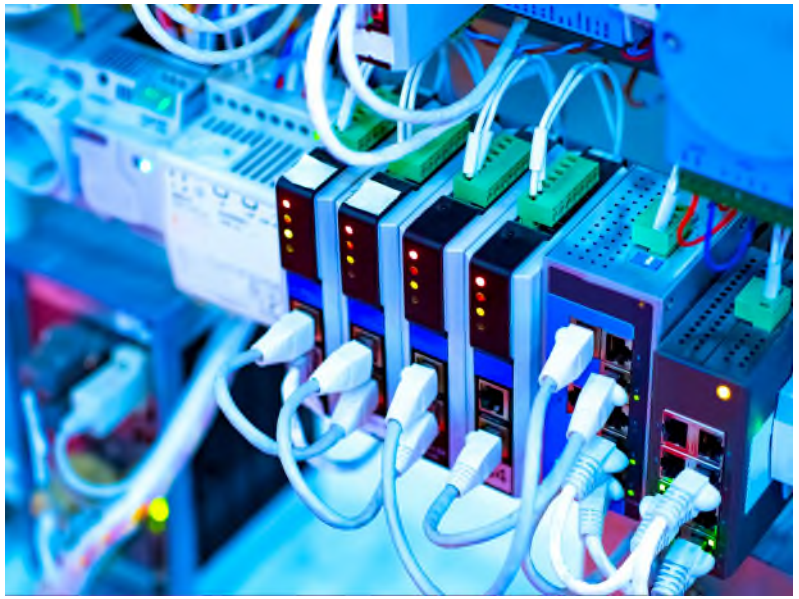
- Do you have an owner for OT/ICS risk? Can your organization adequately frame the risks?
- Do you understand specific threat profiles for OT/ICS?
- Do you understand the OT/ICS impact analysis to the business?
- What taxonomies or standards do you map to for OT/ICS risks? How do you stack up?



Technical Action Item: Start the Roles and Responsibilities RACI for ICS, OT & Connected Tech

Who is responsible, accountable, consulted, and informed of specific ICS, OT, and connected corporate infrastructure:

- Access Controls
- Vulnerability Management (patching and configurations)
- Business Continuity / Disaster Recovery
- Network Security Architecture and Monitoring
- Device/Node Security Architecture
- Change Management
- Incident Response (IRP may need to be tailored for ICS)



Action Item: Questions for Lawyers

Technical / Operational:

- Do we know the universe of our Internet enabled ICS and OT architecture?
- Do we know what corporate systems are connected to these systems?
- Who is responsible for the security of ICS, OT and connected infrastructure?
- What security training is available for employees in areas impacting ICS, OT and connected infrastructure?

Audit:

- Does our architecture follow any broader security audit standard?
- Are risks addressed on a prioritized basis?
- Is there a recent risk assessment (internal or third party) over the architecture?

Management:

- Who has security budget authority over the architecture?
- If any ICS, OT or connected systems are vendor managed systems, who is managing the vendor and ensuring security compliance?
- What is our company governance infrastructure for the architecture?

Action Item: Back Legal Questions with Evidence – What are our Artifacts of Compliance?

- **Systems and Business Universe:** Data map / inventory
- **Security Documentation:** Policies / Procedures / Standards
- **Accountability:** RACI / Roles & Responsibilities / HR Job Descriptions
- **Objective Evidence:** Audits / Scans / Security Appliance Dashboarding (firewall, vulnerability scans, EDR/NDR)
- **Risk Evidence:** Risk Assessments / Risk Register (POAMs) / Corresponding Ticketing (for risks, SDLC and project management) / Vendor Management Tracking/Scorecards
- **Financial Responsibility:** Information security budget requests
- **Management Accountability:** Presentations, board minutes and IT/Security Roadmaps
- **Incident Response:** Tabletop exercises and after-action incident reviews

ALSTON & BIRD

DRAGOS

Questions?