RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: PDAC-W12

What Lurks within Your IT: Spotlight on the Dark Side of the Supply Chain

Dawn Cappelli

VP Global Security and CISO
Rockwell Automation
@DawnCappelli

Edna Conway

Chief Security Officer, Global Value Chain
Cisco Systems, Inc.
@Edna_Conway

Why Are We Here?
Digital Transformation

IT/OT Convergence

Connected Devices

Function & Data

Multiple Clouds

Convergence of IT & OT

Connected Home

Connected Factory

Critical Infrastructure

Who & What is the 3rd Party Ecosystem

Threats Continue To Rise

Securely Harness the 3rd Party Ecosystem

Threats

Manipulation

Espionage

Disruption

Threat Impacts

Taint

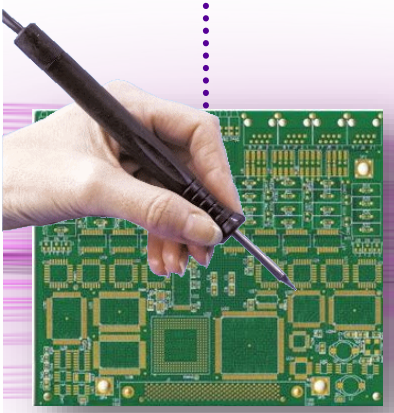
Counterfeit

IP Misuse

Information Security Breach

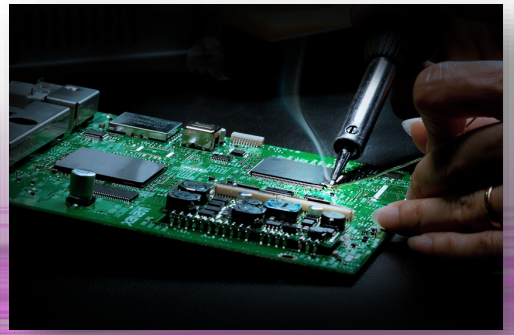
Where & How “Bad Actors” Can Succeed

Altered electrical flow on a printed circuit board



3rd party software containing vulnerabilities

Alteration during import/export or transportation



“Added” integrated circuits on a printed circuit board assembly

Functional impact to critical infrastructure

How Can We Address These Threats?

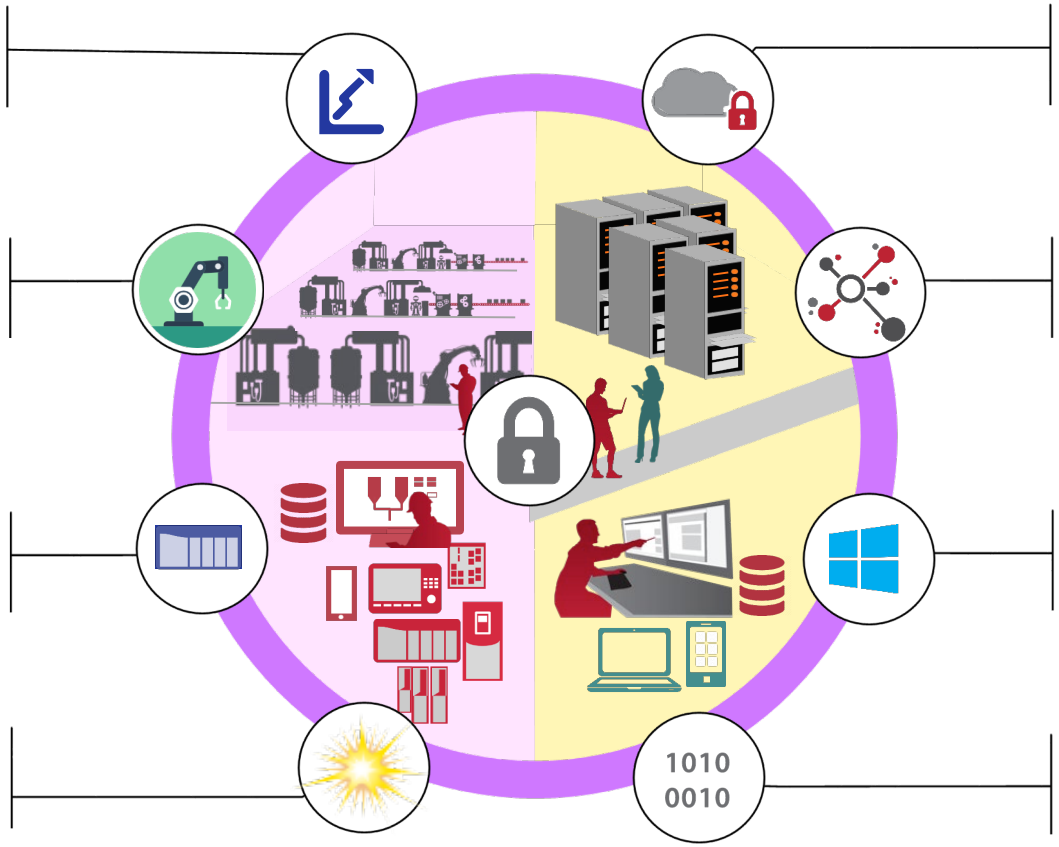
OT

Priority:
reliability and system integrity

Architectures:
proprietary, isolated, task specific systems

End-points:
task specific, long lifespan

Outcomes are physical



IT

Priority:
availability and data integrity

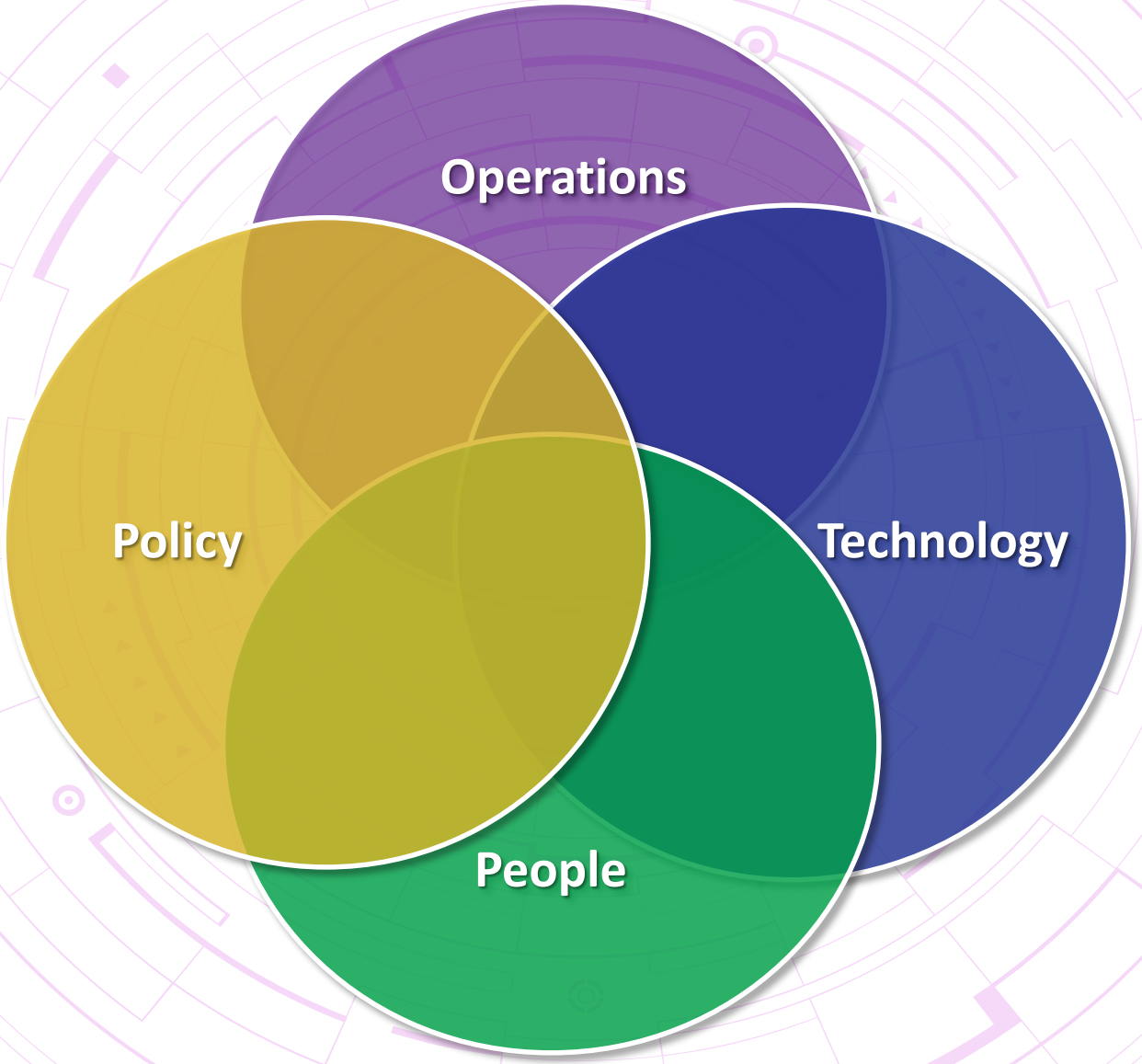
Architectures:
open, connected, integrated systems

End-points:
multi-function, shorter lifespan

Outcomes are digital

Leverage NIST Cybersecurity Framework Across IT & OT

Ensure Suppliers Comprehensively Address Security



Operations

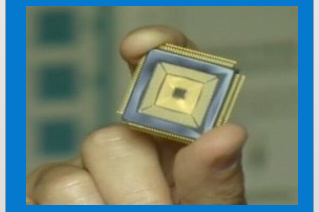
IT Meets OT

- **Authentication certificates** for identity management
- **AI & ML** leveraged for analysis of IoT data streams
- Secure, audit-level **tracking of IoT data** transactions
- **Blockchain** of custody for immutable device ID
- **Encryption** for data deployed in transit and at rest
- Joint IT and OT **resiliency** built in
- **Enterprise security** as part of your **Industrial IoT deployment**

Technology

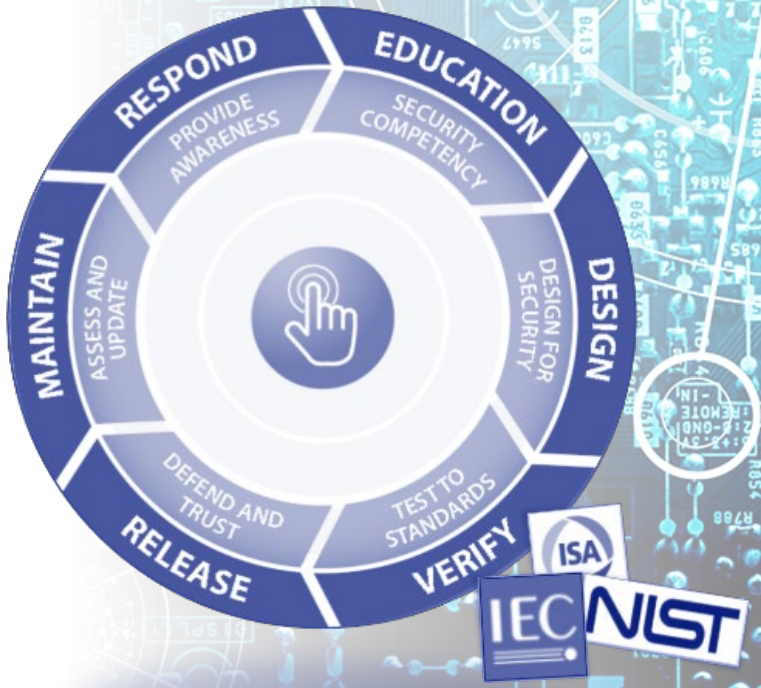
Trust Anchor

Secure Identity Verification	Product Security
• Authenticity and License Check • Verify Secure Identity	• Immutable Identity • Secure Storage (Keys and Objects) • Certifiable Entropy Source • Secure Crypto Assist • Secure Application Certificates



ICT Passport

Build Security In



cisco Rockwell Automation

Policy

Architecture Domain Structure

Personnel Security
Asset Management
Third-Tier Partner Security
Security Incident Management
Security Engineering and Architecture
Security in Manufacturing and Operations
Physical and Environmental Security
Security in Service Management
Security in Logistics and Storage
Information Protection
Security Governance

Security Policy

People

Human Risk → Security Champions

- ✓ Formal program to **protect Intellectual Property**
- ✓ **Controls for cyber sabotage** of products and customer sites
- ✓ Controls and **training** for data handling (e.g. USB usage)
- ✓ **Background checks**
- ✓ **Third parties** as insiders
- ✓ **Security awareness** campaigns
- ✓ Role-based security **competency programs**

Ensure Suppliers Deploy a Layered Approach to Security

Public-Private Partnership

Homeland Security

enisa
European Network and Information Security Agency

Defense Security Service

NIST
National Institute of Standards and Technology

Charter of Trust

Navigating the Dark Side of Supply Chain
A Roadmap You Can Apply

1

Stage 1:

Build Your Foundation

- Map the who, what and where of your 3rd party ecosystem
- Implement a secure development lifecycle
- Identify areas for potential unauthorized modification
- Research modification detection techniques/technology

Navigating the Dark Side of Supply Chain
A Roadmap You Can Apply

2

Stage 2:

Develop Your Roadmap

- Develop a comprehensive architecture employing a layered approach
- Address 3rd party security based on risk
- Leverage government, academic and industry partnership

Navigating the Dark Side of Supply Chain
A Roadmap You Can Apply

3

Stage 3:

Execute Flexibly

- Limit access and connection with a least privilege, role-based approach
- Balance benefit of connectivity vs. risks of information access and control
- Deploy IT security practices in operations (*e.g.* segmentation)

We are ***ALL*** in this ***TOGETHER***.

Questions?