Cyber and Physical Security In Manufacturing Environments

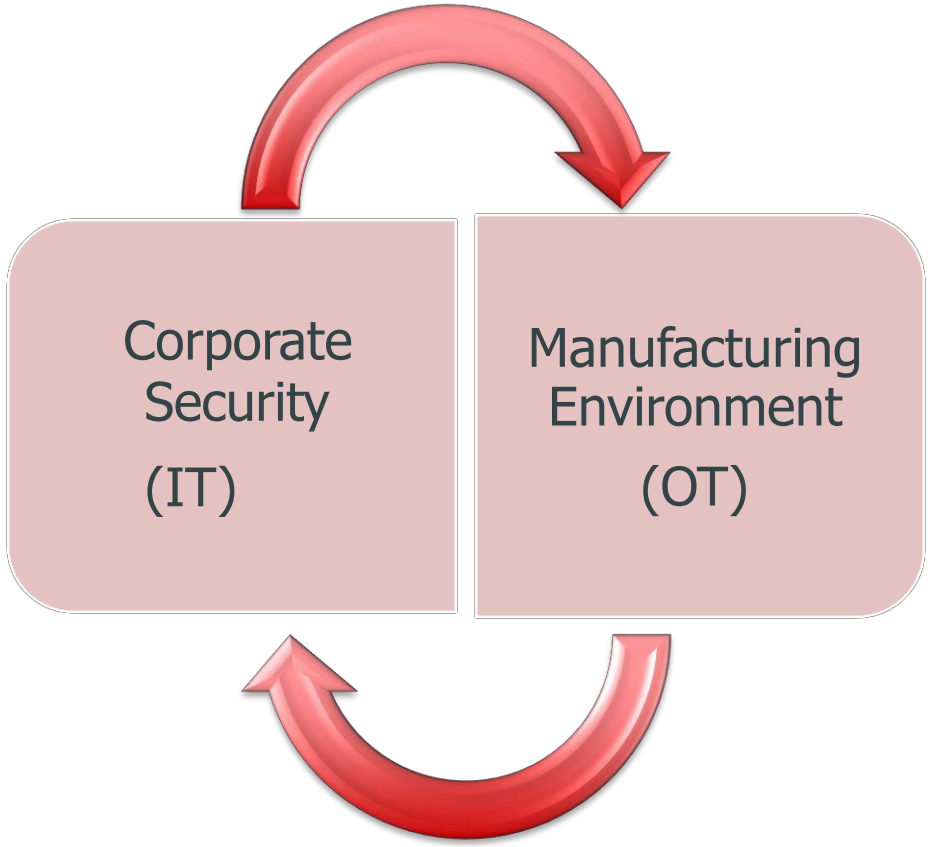
Scott Whelchel
Chief Security Officer – Global Director
swhelchel@dow.com

Sandra Parker
Global Improvement Director – Cyber Security
skparker@dow.com

Dan Rozinski
Technology Fellow - Manufacturing & Engineering
dwrozinski@dow.com

Cybersecurity in Manufacturing

- Cybersecurity continues to be a challenge as threats grow
- Assessments and benchmarks are used to evaluate cyber risks in manufacturing
- With a digital focus, we need to continue to adapt and to evolve to keep pace with both the threat and to enable new business models



Manufacturing Cybersecurity Journey Overview

Pre-2017
Firewall Isolation

- Isolation of Process Control Networks w/Firewalls
- Security compliance and changes managed by M&E IT
- Deployed cyber protection package for ABB systems established
- Local cyber protection varied between different sites, businesses, and platforms

2017 Gen 0
Mfg. Cybersecurity Program Launch

- External Benchmarking against industry peers
- Adoption of NIST Cybersecurity Framework
- Defined Cyber Delivery Specialist role for local support
- Formal program launched with 1st generation scope defined

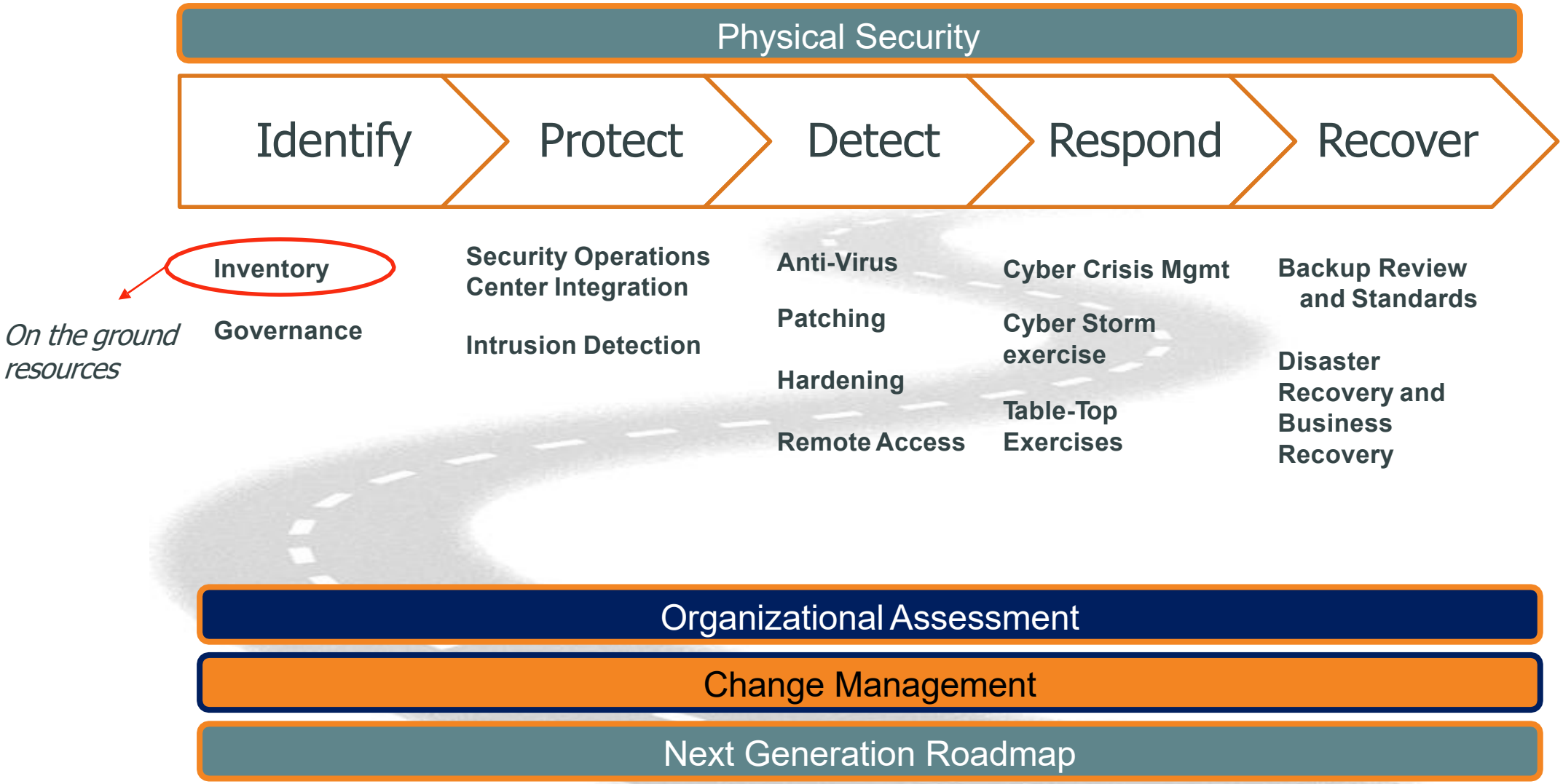
2018 Gen 1
Strategy and Pilot Implementations

- Deployed an asset inventory for M&E computing systems
- Deployed cyber protection packages for Siemens, Foxboro and generic systems
- Integrated M&E cyber alerting to the Security Operations Center
- Deployed new cyber detection layers (IDS/ logging) on plant firewalls
- Developed multi-factor authentication for secured remote access
- Reviewed and updated cyber assessment and response processes for M&E
- Piloted staffing for Cyber Delivery Specialists at high priority plants

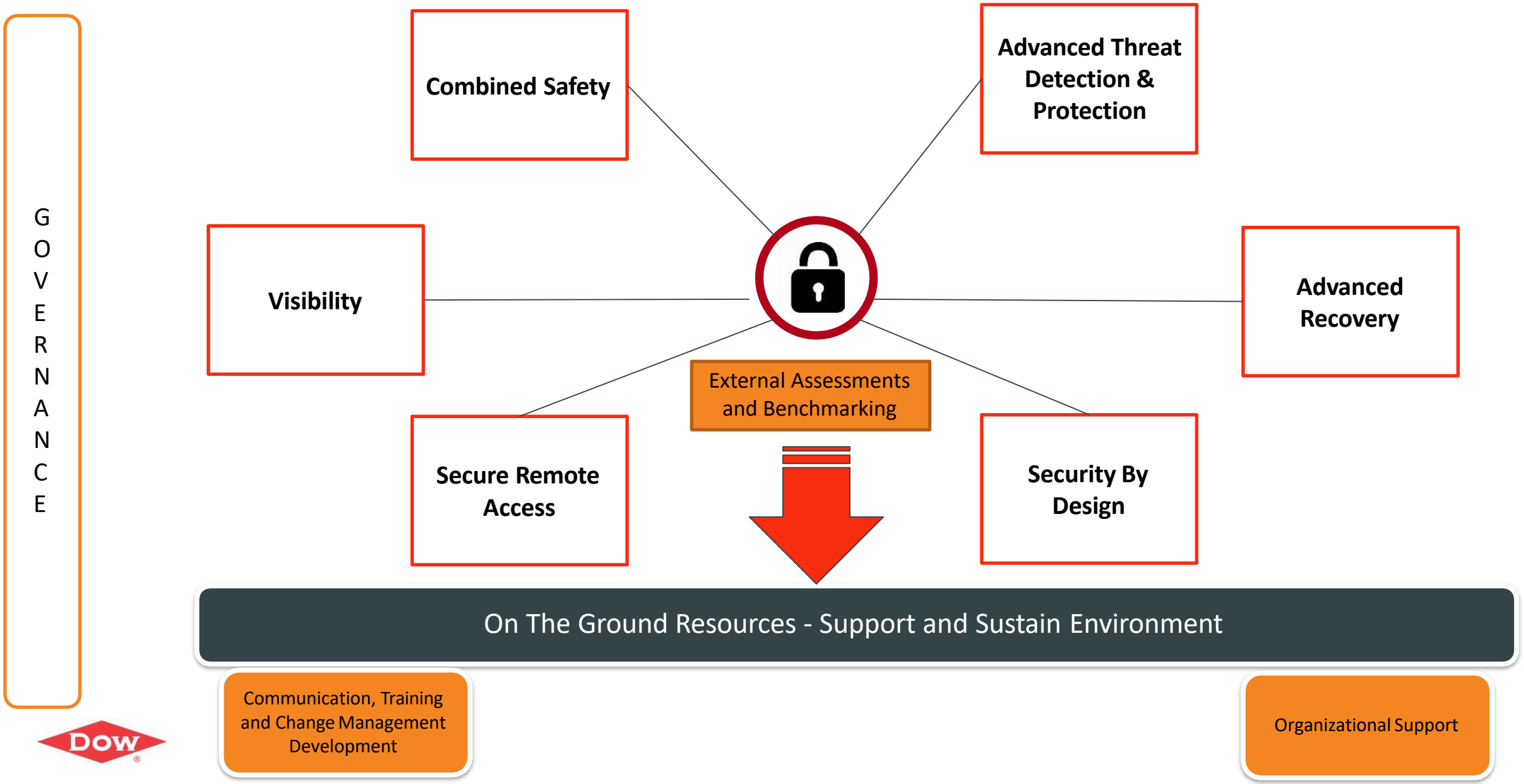
2019 Gen 2
Protecting High Risk Sites

- Develop cyber protection packages for Emerson and Honeywell systems
- Cyber assessments conducted and local cyber protection applied at high priority plants *
- Deploy multi-factor authenticated remote access to high priority plants
- Launch 2-N initiative to start delivery of security controls to all production facilities
- Complete staffing for Cyber Delivery Specialists for high priority plants
- Launch 2nd generation of initiatives to shift from a reactive to proactive approach in detecting threats

Manufacturing Cyber Security Roadmap



Five Year Outlook (2020++)



Support and Sustaining Environment

Our goal is to improve cybersecurity while minimizing the impact on the operation of any plant we engage.

A plant engagement model was developed to provide an organized and coordinated approach …

- Assess the current state of cybersecurity
- Identify and Inventory all networked computing devices
- Create a plan of improvements for the specific plant
- Deploy asset management, anti-virus and Windows patching tools where appropriate
- Document completed improvements and outstanding risk

On the ground resources at our Priority plants was necessary to help deploy tools and processes

Approach & Role Description

Staff based on priority level of plant/site

Implementation approach for small remote sites that don't justify a dedicated Cyber Delivery Specialist.

- Shared Cyber Delivery Specialists near another sites
- Small remotes sites with standardized process control technology could be implemented with a different approach and then maintained by the local Process Control technology staff.
- Other small remote sites would need to be handled as one offs to see if a current person can manage the Cyber Delivery Specialist role or if they can justify the position.

The **Cyber Delivery Specialist** is responsible for ensuring the adequate implementation of Cybersecurity solutions at supported locations with close engagement to Cyber Security and Corporate Information Security Services teams.

Responsibilities

- The implementation and support of the manufacturing cyber security management systems within their assigned facilities in order that the businesses, sites, and plants are protected against a cyber security events and can appropriately respond if one would occur.
- Ensure client supported devices (CSDs), and Internet of Things (IoT) devices implemented at the plant comply with Cyber Security controls.
- Ensures Cybersecurity work processes, tools, standards and procedures are effectively applied within assigned plants.
- Tracks and communicates Cybersecurity performance
- Participates in cybersecurity audits, investigations and response
- Identifies, escalates and resolves potential cyber risks at the site level
- Participates in site security assessments

Accelerating Collaboration

Exercise design and objectives

- 2019 – performed Corporate Crisis Management Team tabletop exercise following HSEEP methodology
- CEO and top 25 Crisis Leaders for 3 hours
- All functions, geographies and businesses in Dow
- Plans vs. Planning
- Scenario based on “NotPetya” impacts to Maersk
- Strengthened business continuity and cross-functional planning

- Objectives:
  - Test & evaluate the Dow Crisis Management System
  - Assess internal and external information sharing protocols
  - Provide a collaborative environment for Crisis “Team of Teams” to form

Security Risk Assessment

- Risk = Consequence x Likelihood x Vulnerabilities
  - Cybersecurity – Physical security – Process Safety = risks simply from different vectors
- Combined virtual and physical risk focus into one assessment
- More comprehensive risk spectrum to include non-manufacturing risk and other threats
- Bringing risk ownership beyond security personnel
  - Business leaders own the risk

“Converged” layers of security

- Enterprise Security Risk Management
- Security Intelligence and Situational Awareness
- Risk Management (Insider Threat, Red Teaming)
- Event & Incident Management
- Identity Management & Governance
- Compliance visibility