Consistent Implementation of Cyber Security Measures
Challenges & Learning Experience

Durchgängige Umsetzung von Cyber Security-Massnahmen
Herausforderungen und Lernerfahrungen

Technical Expertise & Support

TES 20 20 10 10 10 BY 2020

Leverage Globally, Act Regionally, Execute Locally

Faster & Smarter

Rainer Oehlert, Dow

BIO Rainer Oehlert

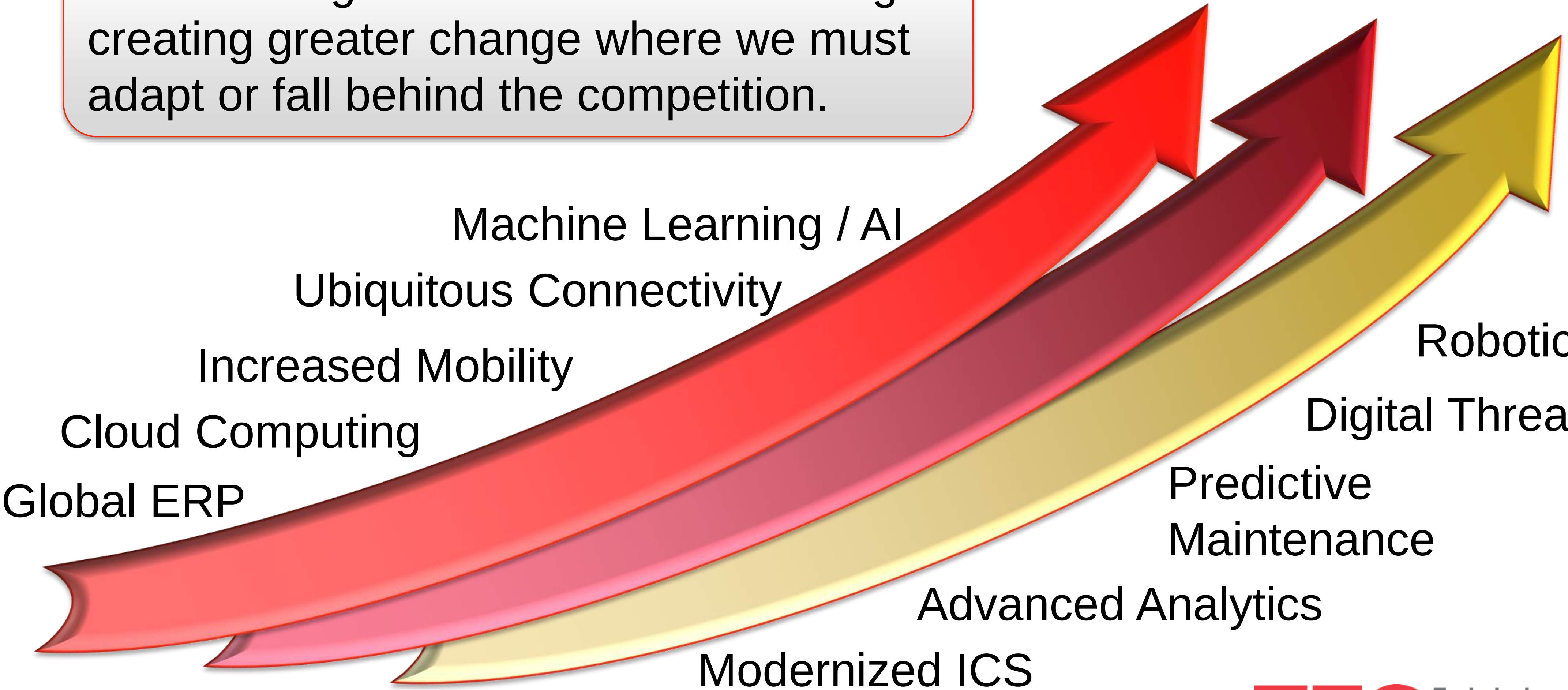
- **Master Degree in Chemical Engineering** from Dortmund Technical University,
- Joined Dow in 1985 with roles in **Production-, Technology & Engineering**
  - ➢ **Lead Process Automation Engineer** for Capital-, Improvement-, DCS- Migration Projects globally,
  - ➢ **Regional Leader EMEA** for Process Automation(PA) & Process Engineering (PE),
  - ➢ **Regional Engineering Director EMEA** for all Engineering Disciplines,
  - ➢ **Global Technology Center Directo**r for all Engineering Disciplines
    Till 7/2019 Global Technology Center Director for Process Automation Process Control Application Technology, Process Control (DCS) Hardware & OT Security, Manufacturing Execution Systems (MES), Advanced Process Control (APC), Safety Instrumented Systems (SIS), DCS Migrations, Functional Safety,

Agenda

- Industry Trends
- Dow Manufacturing Cyber Security Program
  - Program Overview
  - Roles in Manufacturing
  - Plant Engagement Model
  - Dissemination of Information
  - Program Challenges
  - Local Challenges
  - Potential Measures (Manufacturing)
  - Protection Measures at Plant Level

IT and Manufacturing Trends

Trends in digitalization are accelerating creating greater change where we must adapt or fall behind the competition.



Machine Learning / AI

Ubiquitous Connectivity

Increased Mobility

Cloud Computing

Global ERP

Robotics

Digital Thread

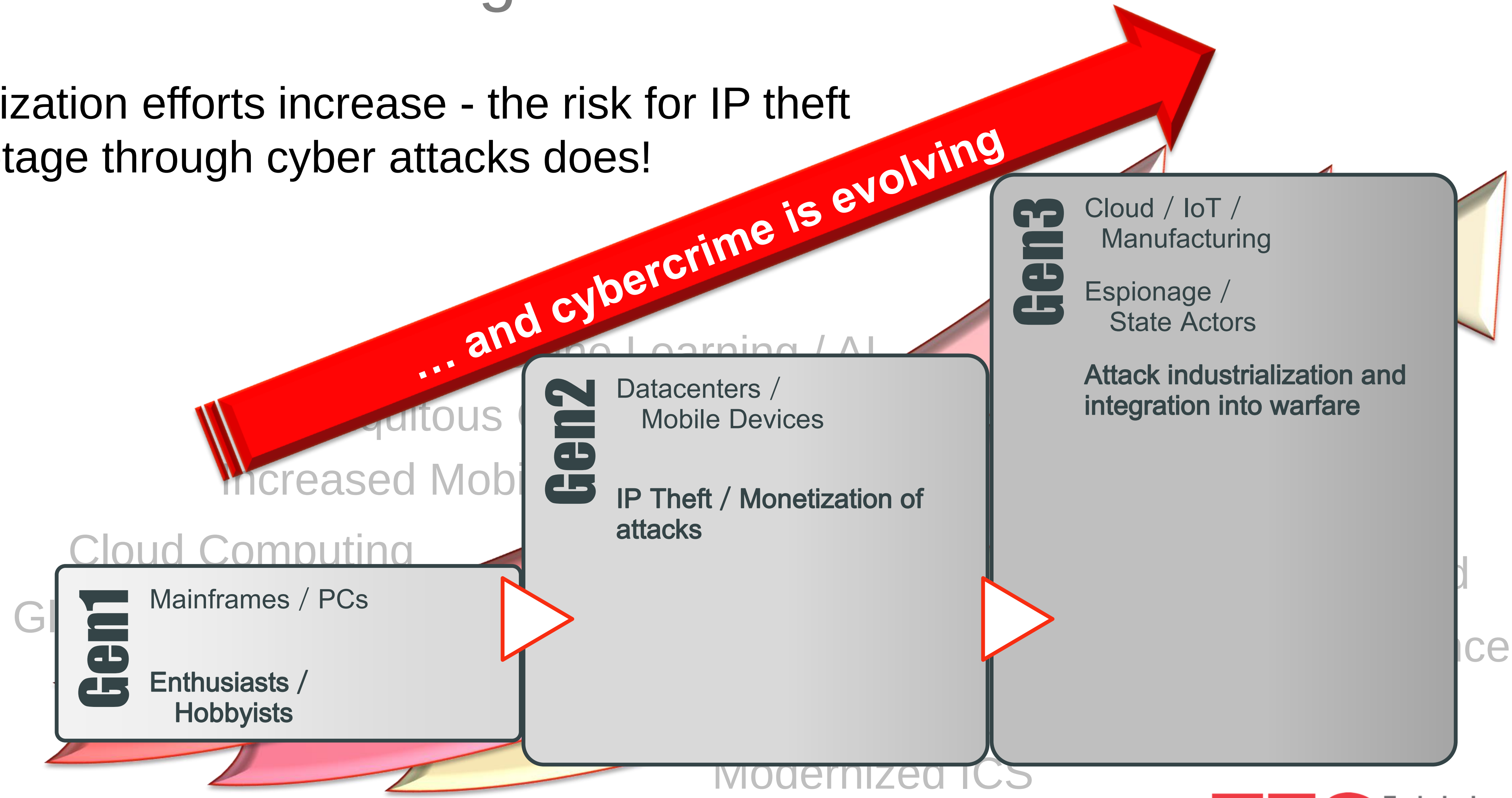
Predictive Maintenance

Advanced Analytics

Modernized ICS

IT and Manufacturing Trends

As digitalization efforts increase - the risk for IP theft and sabotage through cyber attacks does!



Gen1
Mainframes / PCs
Enthusiasts / Hobbyists

Gen2
Datacenters / Mobile Devices
IP Theft / Monetization of attacks

Gen3
Cloud / IoT / Manufacturing
Espionage / State Actors
Attack industrialization and integration into warfare

Industry Trends continue in 2018 and 2019

Atlanta Spent $2.6 Million to Recover from a $52,000 Ransomware Scare
(Wired – April 2018)

Tesla worker admitted to sabotage of manufacturing systems
(CNN Tech – June 2018)

Triton

America's Electrical Grid
has a Vulnerable Back Door and Russia Walked Through It
Wall Street Journal – January 2019

Hexion and **Momentive** Respond To Cyber-Attacks
Chemical Engineering – March 2019

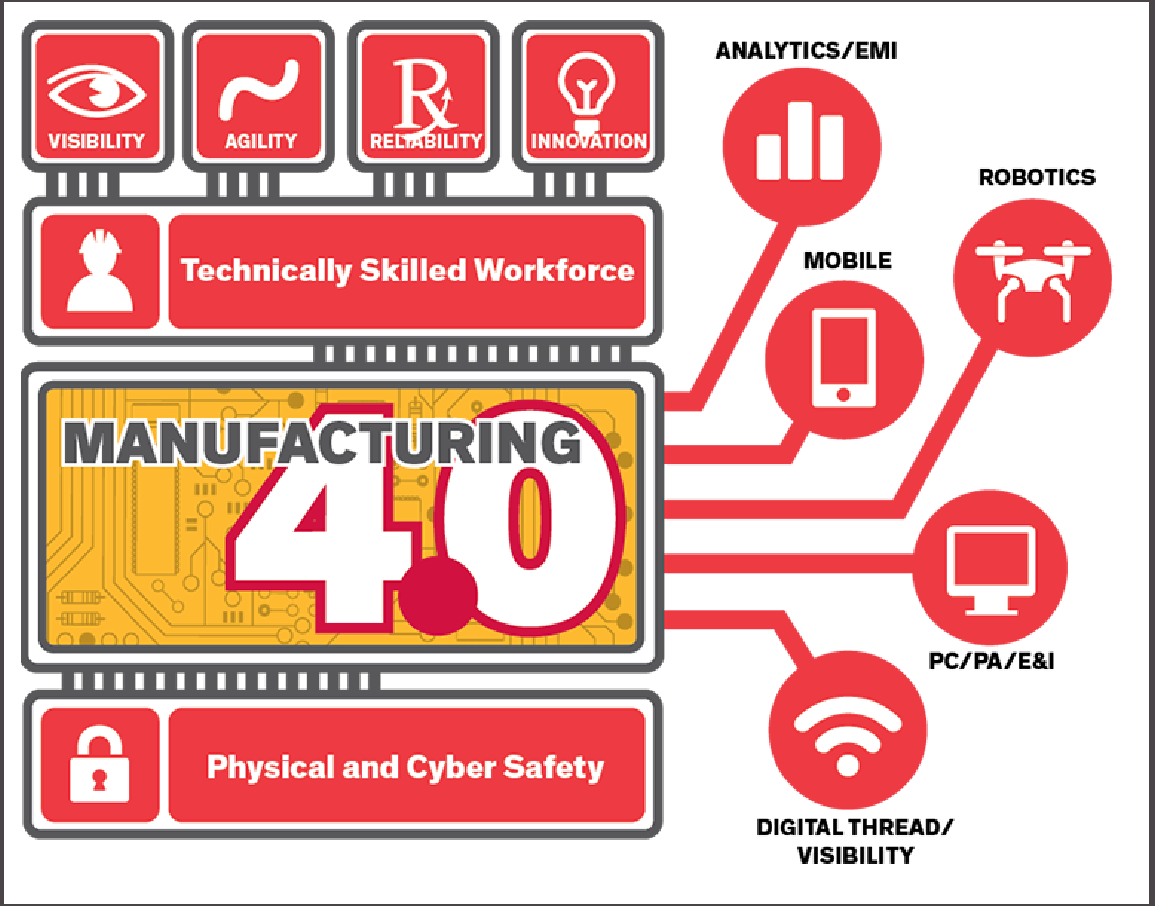
Arizona Beverages knocked offline by ransomware attack
TechCruch - March 2019

Hoya Hit By Cyber Attack In February
Japan Times – April 2019

Norway say **Norsk Hydro** cyber attack began Monday evening and escalated during the night
Reuters – March 2019

Bayer Contains Cyber Attack It Says Bore Chinese Hallmarks
Reuters – April 2019

Manufacturing giant **Aebi Schmidt** hit by ransomware
TechCrunch – April 2019



Dow Manufacturing Cyber Security Program Overview & Challenges

DOW RESTRICTED

Manufacturing Cybersecurity Program

Principles for a Manufacturing Cybersecurity Program:

- The cyber threat can never be entirely mitigated and continues to grow
- Maturity assessments and benchmarking are key tools to measure progress
- Generational plans needed, aligned with Operations and Business imperatives

Measures of Success

- Improved reliability of Plant Control systems
- Reduced risk of compromising the Safety systems
- Aligned with Process Safety → Culture Change

"A successful response must cover the full spectrum of people, process, and technology challenges that these organizations face in this area."

- Eric Cosman, ARC Contributing Consultant

Manufacturing Cybersecurity Program Overview

- Established in 2017 by Dow Board members (COO, CIO) as a joint effort of Manufacturing & Engineering and Information Systems Functions
- Has a board delegated VP as Program Sponsor The program leverages in work of existing Cybersecurity expertise in Manufacturing and Process Automation that maintain the existing controls. (Leverage in OT view)
- The program consists of multi-generational initiatives at both the enterprise and the plant level with a goal to raise Dow level of protection across all plants.
- The program includes a change management and organizational component to ensure the program is sustainable into the future.
- The program is based on the US National Institute of Standards (NIST) Cybersecurity Framework (Manufacturing Cybersecurity Framework).

Manufacturing Cybersecurity Program

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
CORE

IDENTIFY Understand our installed devices and their attributes and risks, with governance to ensure integrity and management of change.

PROTECT Provide controls and training to safeguard our critical systems and infrastructure from cyber threats.

DETECT Provide anomaly and threat detection with centralized monitoring of events to enable timely and effective response to cyber events.

RESPOND Develop and implement effective actions to detected events to mitigate and eliminate cyber threats.

RECOVER Develop and implement effective actions to restore capabilities impacted by a cybersecurity event and maintain system resiliency.

Cybersecurity Framework

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
CORE

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

The framework Is implemented through a combination of …

Network Controls

End Point Controls

Standards

People

Processes

Governance

to manage risk in a multi-generational approach

Manufacturing Cybersecurity

Multi Generation Plan (MGP) -1

Identify

We need to see assets to protect them

Global Asset Inventory
- Tool to scan network for devices
- Establish Data base to store device information

Protect

We need controls to protect our assets

- Centralized Anti-Virus
- Centralized Window Patching
- System Hardening by platform Perimeter Hardening
- Enhanced Authentication for Remote Access

Detect

We need to see the threats to respond

- Security Operations Center (SOC) Integration and alerting for:
  - ➢ Anti-Virus
  - ➢ Asset Inventory Monitoring
  - ➢ Firewall Logs
  - ➢ Intrusion Detection

Respond

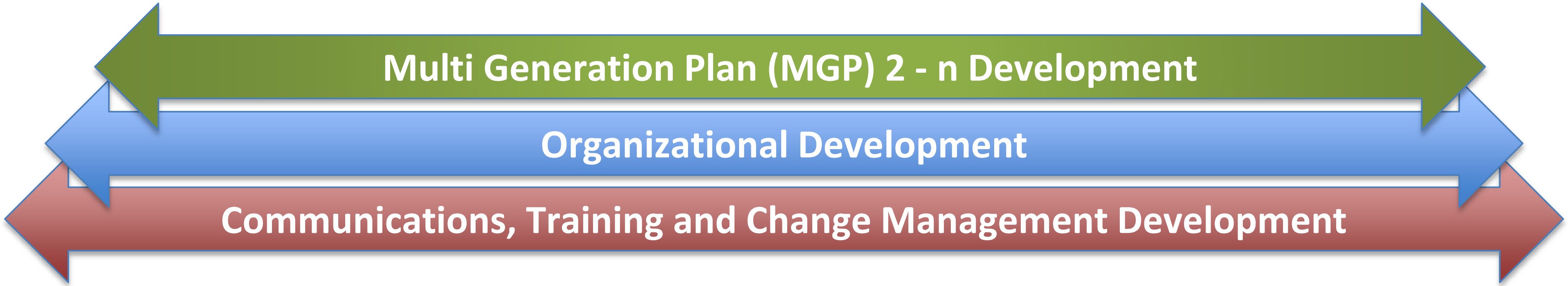
We need a coordinated response to threats

- Cyber Isolation Process
- Update the Crisis Management Response Plans for Manufacturing
- Exercise the plans

Recover

We need to be able to rapidly restore our assets

- Risk Assessment for existing backup solutions
- Business study of improvement opportunities
- Test & Exercise


Multi Generation Plan (MGP) 2 - n Development
Organizational Development
Communications, Training and Change Management Development

DOW RESTRICTED

Manufacturing Cybersecurity

Multi Generation Plan (MGP-2)

Identify

We need to see assets to protect them

Manufacturing Visibility
Network devices, Dashboards for M&E, Decommission existing legacy tools

Protect

We need controls to protect our assets

Extend Cyber Controls to NON-Standard Systems

Remote Access Technology
Uplift principles and requirements,.

Uplift Controls on USB and Vendor Devices
Whitelisting, other technologies

Detect

We need to see the threats to respond

Advanced Threat Intelligence
Manufacturing Threat Intelligence, Advanced Cyber training for Manufacturing

Network and device anomaly detection

Respond

We need a coordinated response to threats

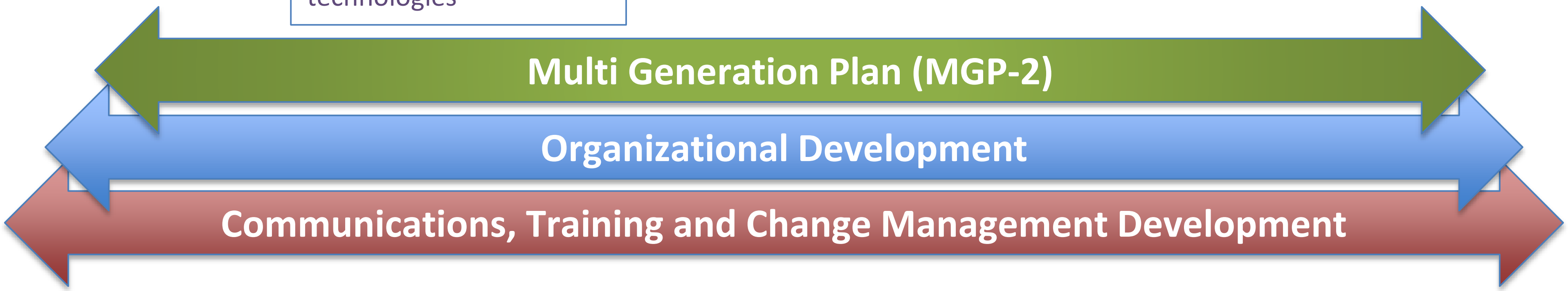
Manufacturing Visibility
Enables faster, more effective response plans

Recover

We need to be able to rapidly restore our assets

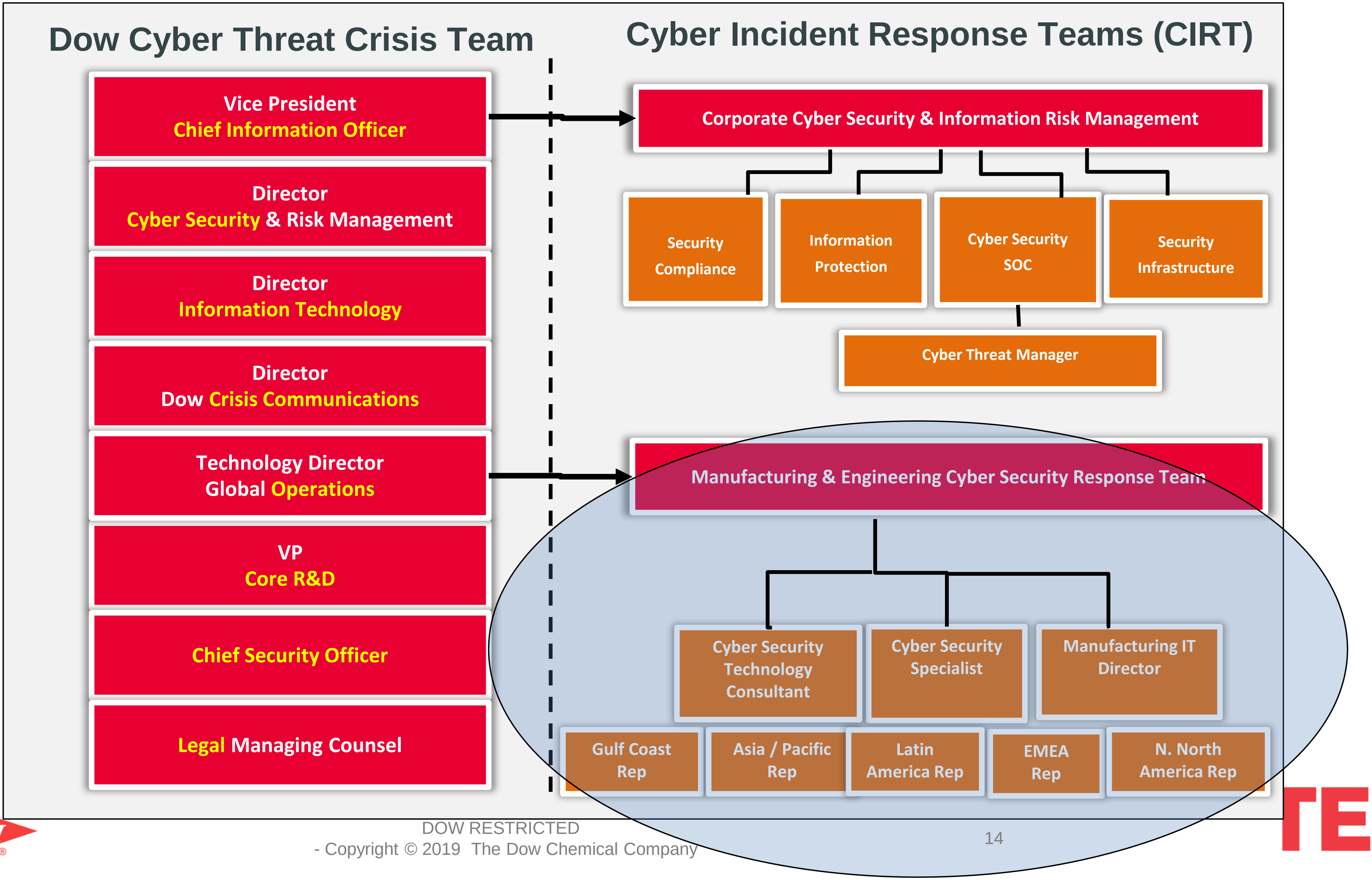
Back-up and Recovery
Uplift back-up solutions

Use Test & Exercise results to improve recovery process


Multi Generation Plan (MGP-2)
Organizational Development
Communications, Training and Change Management Development

DOW RESTRICTED

Corporate Organization – IT and OT Response Teams



Dow Cyber Threat Crisis Team

Vice President
Chief Information Officer

Director
Cyber Security & Risk Management

Director
Information Technology

Director
Dow Crisis Communications

Technology Director
Global Operations

VP
Core R&D

Chief Security Officer

Legal Managing Counsel

Cyber Incident Response Teams (CIRT)

Corporate Cyber Security & Information Risk Management

- Security Compliance
- Information Protection
- Cyber Security SOC
  - Cyber Threat Manager
- Security Infrastructure

Manufacturing & Engineering Cyber Security Response Team

- Cyber Security Technology Consultant
- Cyber Security Specialist
- Manufacturing IT Director

Gulf Coast Rep | Asia / Pacific Rep | Latin America Rep | EMEA Rep | N. North America Rep

Manufacturing & Engineering Cyber Security Response Team Tasks (OT-Area)

- Support response to corporate or regional cyber incident
- Plan and ensure we have a robust response to cyber threats, incidents, and incursions
- **Drive business continuity preparedness**
- Be advocates for cyber preparedness in your region / area
- **Drill, prepare, improve**

A Cybersecurity Role in Manufacturing

The **Cyber Delivery Specialist in Manufacturing** is responsible for the ensuring the adequate implementation of Manufacturing 4.0 and Cybersecurity solutions at supported locations with close engagement to corporate IT. Responsibilities include:

- Ensures Manufacturing 4.0 / Cybersecurity work processes, standards and procedures are effectively applied within assigned plants.
- Tracks and communications Manufacturing 4.0 / Cybersecurity performance
- Support site-wide Manufacturing IT systems as required
- Initiate and Lead cybersecurity audits
- Participates in cyber event investigations
- Identifies, escalates and resolves potential cyber risks at the site level

DOW

TES Technical Expertise & Support

Plant Engagement Model

The goal is to improve cybersecurity while minimizing the impact on the operation of the plant.

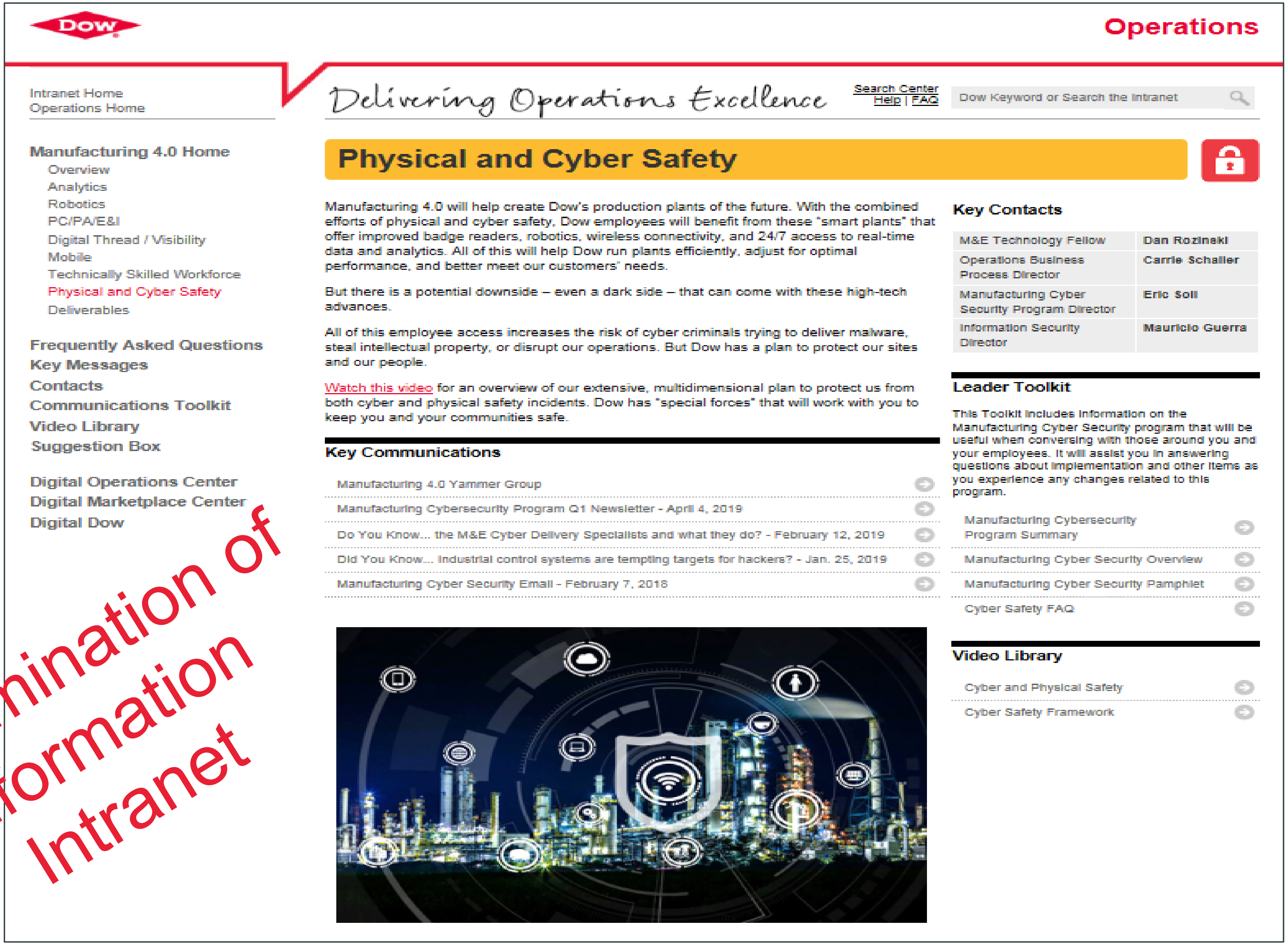
The local controls in MGP-1 require a software installation on computers and should be implemented together to minimize operational disruption.

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

- Assess the current state of cybersecurity at the plant level.
- Identify and inventory all networked computing devices.
- Collaborate with plant personnel to create a deployment plan of improvements.
- Deploy asset management, anti-virus and Windows patching tools per the approved plan.
- Document completed improvements and outstanding risks.

TES Technical Expertise & Support

Dissemination of Information Intranet



DOW

Operations

Intranet Home
Operations Home

Manufacturing 4.0 Home
- Overview
- Analytics
- Robotics
- PC/PA/E&I
- Digital Thread / Visibility
- Mobile
- Technically Skilled Workforce
- Physical and Cyber Safety
- Deliverables

Frequently Asked Questions
Key Messages
Contacts
Communications Toolkit
Video Library
Suggestion Box

Digital Operations Center
Digital Marketplace Center
Digital Dow

Delivering Operations Excellence

Search Center
Help | FAQ

Dow Keyword or Search the Intranet

Physical and Cyber Safety

Manufacturing 4.0 will help create Dow's production plants of the future. With the combined efforts of physical and cyber safety, Dow employees will benefit from these "smart plants" that offer improved badge readers, robotics, wireless connectivity, and 24/7 access to real-time data and analytics. All of this will help Dow run plants efficiently, adjust for optimal performance, and better meet our customers' needs.

But there is a potential downside – even a dark side – that can come with these high-tech advances.

All of this employee access increases the risk of cyber criminals trying to deliver malware, steal intellectual property, or disrupt our operations. But Dow has a plan to protect our sites and our people.

Watch this video for an overview of our extensive, multidimensional plan to protect us from both cyber and physical safety incidents. Dow has "special forces" that will work with you to keep you and your communities safe.

Key Communications

- Manufacturing 4.0 Yammer Group
- Manufacturing Cybersecurity Program Q1 Newsletter - April 4, 2019
- Do You Know... the M&E Cyber Delivery Specialists and what they do? - February 12, 2019
- Did You Know... Industrial control systems are tempting targets for hackers? - Jan. 25, 2019
- Manufacturing Cyber Security Email - February 7, 2018

Key Contacts

M&E Technology Fellow	Dan Rozinski
Operations Business Process Director	Carrie Schaller
Manufacturing Cyber Security Program Director	Eric Soll
Information Security Director	Mauricio Guerra

Leader Toolkit

This Toolkit includes information on the Manufacturing Cyber Security program that will be useful when conversing with those around you and your employees. It will assist you in answering questions about implementation and other items as you experience any changes related to this program.

- Manufacturing Cybersecurity Program Summary
- Manufacturing Cyber Security Overview
- Manufacturing Cyber Security Pamphlet
- Cyber Safety FAQ

Video Library

- Cyber and Physical Safety
- Cyber Safety Framework

TES Technical Expertise & Support

DOW RESTRICTED
- Copyright © 2019 The Dow Chemical Company

Dissemination of Information Newsletter

Technical Components

IDENTFY	**Inventory / Asset Management:** Complete local sites. **Security Compliance:** A reporting tool is information on managed plant assets th with the cybersecurity minimum standa
PROTECT	**Anti-Virus / Patch Management:** Co pilot for Emerson process control sy and two plants in Knoxville. Service equipment for the pilot is being in **Device Hardening:** ABB has be integrated in the next Dow CDC Siemens Technical Team to d **Secured Remote Access:** F authentication (MFA) on ma been completed. The prod implementation in 2Q 201 **Perimeter Hardening:** T limiting high risk service firewall rules for MOD rollout has begun. 3 access is completed
DETECT	**Intrusion Detecti** progress. Cisco F configured. **SOC Integrati** components (i.e. (SOC) has been comple **Firewall Logging:** All manufacturing exploits and alerts are monitored by the Do
RESPOND	**Cyber Isolation:** Mass firewall change mechanism has documentation and training is in progress. **CIRT Integration:** Cyber Incident Response Team (CIRT) processes and c lists are updated for Manufacturing, and an exercise to test the process is underway. **Cyber Crisis Management:** In April 2018, a manufacturing scenario was tested by the Crisis Leadership Team (CLT) using the Cyber Crisis Management process, and learning was documented. A second test is planned for the first half of 2019 to continue refine our response.
RECOVER	**Risk Assessment – Backup Resilience:** MET control systems backup procedures were reviewed with potential gaps and opportunities documented. Development of a strategy to address is in progress.

DOW

Manufacturing 4.0 – Cybersecurity Program

Seek Together

Q1 2019 Newsletter

The Manufacturing Cybersecurity program is a collaborative initiative between Dow Operations, Manufacturing IT and Information Security and is focused on increasing the cybersecurity profile in our global Operations.

This newsletter highlights the MGP-1 progress for Technical Components, Organization, Human Change, Implementation, as well as a preview of the MGP-2 planning.

Implementation

- Implementation metrics have been defined and are now being produced regularly.
- Pre-assessments surveys were completed for all priority 1 plants.
- Cybersecurity Assessments survey created that align with the ES&S SVA process
- **Early Program Win:** When network connections were established due to Orion spin activities, the firewall controls installed as part of MGP-1 detected and alerted the SOC that ultiple sites on the non-Dow network had been infected with malware and were attempting into Dow plants which facilitated an immediate response and remediation.

oyment of local plant controls:

us for 2019 and those facilities deemed highest priority by

bersecurity controls.

9% of all manufactu

yber Delivery Specialist

TES Technical Expertise & Support

Program Challenges

- **Technical debt impact on cybersecurity**
  - *Firewalls, network hardware, computer software have a shorter lifecycle than plant equipment and need to be maintained in a digital/connected environment*
- **Speed of staffing of local resources**
  - *Staffing of Cyber Security Roles is directly related to the speed of implementations*
  - *Need to finalize the long-term local support for cyber security and Mfg 4.0*
- **Business Continuity / Disaster Recovery**
  - *Need to consider business continuity in case of a manufacturing system loss*
  - *Need to further develop off-site back-ups enterprise wide*
- **Corporate Structures & Concepts**
  - *Enable organizational awareness on Cyber Security threads*
  - *Create agile organization to react on threats and potential incidents*

Local Challenges

- Resources demand (financial as well as personal)
- Organization, how to connect top down efforts with bottom up efforts (transport and implementation of results from local security assessments into corporate wide standards guidelines,)
- Collaboration of IT and OT functions. Industry 4.0 and digitalization require holistic view
- Communication (right level of transparency and target audience in the dissemination of cyber incidents in respective and across enterprises)
- Do we need mandatory notification process and reporting obligation (similar as in health area)
- Cyber security assessment of existing assets (registration of inventory, remote access, lifecycle of assets, segregation, defense in depth,)
- Sharpen awareness of operations personal on potential cyber attack scenarios

TES Technical Expertise & Support

Potential Measures from Manufacturing View

- Drills
- Up to date emergency response plans
  - mitigation
  - business continuity
  - recovery
- Definition of last line of defense in safety relevant applications (hard wired remote stop, inherent safe design, mechanical protections)
- Cyber security as common cause failure
  - all security devices from one vendor
    - component diversity
- Integration of cyber security aspects in existing management systems
  - Management of Change process

Protection Measures at Plant Level

Indications for Potential Cyber Attacks for Plant Operations Personal

- Watch out on Operator Screens of DCS System: Graphics and Graphical representations whether the controlled process shows confusing or absurd information, pictorial changes which cannot be explained, popping up attempted blackmail or extortion with monetary impact to create a hostage situation, remote control attempts, visible mouse and keyboard operations not initiated by the operator
- Failure of telecommunication systems (IP- Phone, Cellphone, etc.)
- (Sudden) Access Restrictions on the DCS System
- Unusual, Unknown or contra dictionary DCS or MES System messages, which never have been popped up during normal operations or in your PLC tableaus as well as on the Dow workstation while running IP21 or other PI Software emulation
- Unusual behavior of equipment (machines, motors) or other plant components in the field (e.g. centrifuges/compressors, agitators operate outside of normal range - faster/slower/oscillating – unexplainable set point changes
- No / limited operability of the DCS System and the related Human Machine interface (tablets, screens, keyboards, mouse)
- Frozen Screens
- Process values in the DCS System do not match / relate with/to the visible local plant operational status
- Displayed process values from sensors/instruments on DCS or MES screen far out of normal operating range or operating procedures

- Unusual slow or no response times (lag time) in the real process after parameter (set point) change
- Very long DCS or MES system response times
- Information from other Dow locations or from other news sources about cyber attacks
- Unexpected changes/variations of process parameters (unusual and/or sudden rate of change in process values)
- Freezing of process values (displayed on screen)
- Unusual deviation of material streams into reactor feeds (e.g. batch reactors, or feed streams in continuous plants)
- Variations/Deviations in online and offline quality control data through non comprehensible or not-authorized recipe changes in the DCS or even bill of material changes in the MES System
- Unexpected or unusual changes/variations of pressure, temperatures, levels or other sensor raw data in DCS screen display or on local field instrument *displays*
- Plant Safety- and Interlock Protection System (IPS) not operating or malfunctioning
- Unexpected or Unusual activation of relief devices (as indication of malfunctioning of the Plant Safety- and Interlock Protection System (IPS)

DOW RESTRICTED

Thank You

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER