2021 CHEMICAL SECURITY SEMINARS

December 8, 2021

#ChemicalSecurity

CHEMICAL SECURITY SEMINARS

Cyber-Physical Convergence in the Private Sector

Sandra Parker
Dow, Inc.

Bradford Willke
CISA Infrastructure Security Division

Moderator: Todd Klessman
CISA Chemical Security

#ChemicalSecurity

2021 Version

Physical – Cyber Convergence

Sandra Parker
Global Improvement Director
Manufacturing Cybersecurity

Seek Together™

Our Strategy

Our company's cybersecurity capability is deployed in a risk-based, layered approach following the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework and industry standards.

Anchoring Activities

Protecting our Assets

- Tools and Processes for enabling foundational components and visibility in the manufacturing environment.

Educating our Employees

- General Cyber Training
- Internal Technical Training

Cyberattack Preparation

- Standards integration with manufacturing cyber components
- Drills/Exercises/Benchmarking

THE "SECURITIES"

"Dow is committed to providing a safe and secure workplace for all our employees and stakeholders," said John Sampson, sr. vice president Operations.

"As the digital revolution continues to grow it will be important for our cyber security infrastructure to grow with it. That is why Operations, Information Systems and our security teams are closely collaborating to coordinate our efforts to ensure Dow is ready to meet the challenges of doing business in the 21st century – keeping our workplace safe and secure, and providing our customers with the products they need without interruption."

FRAGMENTATION IS THE SILENT KILLER OF RISK MANAGEMENT PROGRAMS

Security Risk Assessment

- Risk = Consequence x Likelihood x Vulnerabilities
  - Can't achieve Zero Risk
- Integrated Security Risk Assessment (physical and virtual)
- 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
- Holistic Intelligence and situational awareness
- Risk Management (Insider Threat, "purple teaming")
- Event & Incident Management
- Identity Management & Governance
- Compliance visibility

DIGITAL TRANSFORMATION

- **ADAPTABILITY**
  - 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
- **SECURITY BY DESIGN**
  - As we move into a more digital convergence in the OT space - Security by Design is an area that we must take into account from the Initial phase of ideation, through pilot

Collaboration with Businesses and Processes

- Using standard tools and processes to communicate manufacturing incidents:
  - Share Key Learnings
  - Share Corrective Actions
  - Broad Distribution Across All Sites
- Business Continuity Planning Integration

Importance of Educating our Manufacturing Employees

- Our first defense is our people making the right decisions
- There is human interaction and choice in every cyber event
- Educating them on what to look for and how to respond will enable them to make the right choices - preventing the impact of cyber incidents (i.e., lost productivity, shutdown of production, etc.)
- A cybersecurity general awareness training course is an effective way to train.

Support and Sustaining Our Environments

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

A plant engagement model is one way 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

Resources can be internal or outsourced. Familiarity with a plant environment is essential.

Seek

Together™

SUPPORTING INTEGRATED PREPAREDNESS AND RESILIENT INFRASTRUCTURE…

AND THE CYBER-PHYSICAL CONVERGENCE IN THE PRIVATE SECTOR

Infrastructure Security Division
Bradford Willke, Senior Advisor for Cyber-Physical Convergence

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

PARTNERSHIP DEVELOPMENT

INFORMATION AND DATA SHARING

CAPACITY BUILDING

INCIDENT MANAGEMENT & RESPONSE

RISK ASSESSMENT AND ANALYSIS

NETWORK DEFENSE

EMERGENCY COMMUNICATIONS

What does a "convergence" mindset mean for…

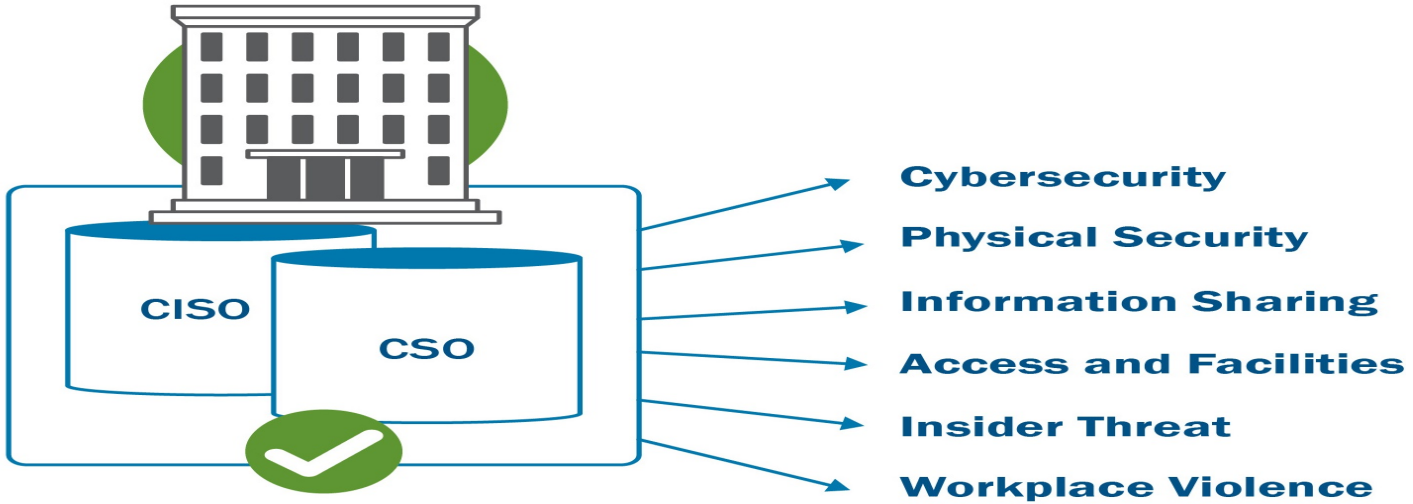
- Law enforcement and/or intelligence interaction?
- Incident response, business continuity, and consequence management?
- 24/7 monitoring (i.e., security operations)?
- Organizational structure of security forces?
- Information sharing and analysis?

Integrated Preparedness and Security

Today's threats are a result of hybrid attacks targeting both physical and cyber assets… creating more opportunities for integrated preparedness and collaboration across security disciplines.

Converging Enterprise Security Functions

CONVERGED SECURITY FUNCTIONS AS AN ORGANIZATIONAL PRACTICE



Key Questions

- What known PHYSICAL risks worry the CYBER team?
- How can CYBER add value to the PHYSICAL security mission?
- Why should the PHYSICAL team care about CYBER security?
- What known CYBER risks worry the PHYSICAL team?
- How can PHYSICAL add value to the CYBER security mission?
- Why should the CYBER team care about PHYSICAL security?

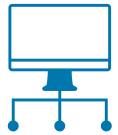
Smart Technology and Emerging Risks

Cyber-Physical Systems (CPS):


Autonomous Vehicles


Smart Cities


Unmanned Aircraft Systems


SCADA Systems

Converged Incidents – Ransomware:

	Attacker	Impact
1 Colonial Pipeline	Darkside	▪ Widespread fuel disruptions, price surges, and panic buying
2 Kaseya	REvil	▪ 200+ businesses without cloud and software management services
3 Hexion and Momentive Chemical Companies	LockerGoga	▪ Hardware and network disruptions, loss of information ▪ Hexion estimated $5 million in loses/day

Cyber-Physical Convergence Pillars

Pillar 1

Cyber-physical **threats and vulnerabilities converging** to cause disruption to critical infrastructure service delivery, essential supply and operating chains, and national critical functions

Pillar 2

Integration of cyber and physical security management in planning, operations, incident, and contingency response

Pillar 3

Cyber-physical systems – complex IT/OT, technology-enabled, digitally transformed environments supporting or delivering infrastructure services

Common Lines of Effort

Raise the profile of cyber-physical systems; their cyber, physical, personnel, industrial, chemical, operational, etc., security requirements; and integrate planned and executed

Support integrated security planning, operations, and contingency/incident response via evidence-based, analytically-driven guidance and resources

Spotlight issues to the critical infrastructure community where there is an under-focus or no focus at the convergence point

Support investment, capacity building, stress tests/assessments of security and resilience for cyber-physical systems, integrated preparedness, and resilient infrastructure

Drive innovation to make the cyber-physical convergence a defined knowledge management domain with identifiable subject matter expertise

Useful Resources

#Chemlock

cisa.gov/chemlock

Cyber Resource Hub

- **Cyber Hygiene (CyHy) Scanning**
- **CSET®**
- **Validated Architecture Design Review (VADR)**

cisa.gov/cyber-resource-hub