CONVERGENCE OF CYBER-PHYSICAL SYSTEMS (CPS)

THREAT BRIEF
CPS CONVERGENCE
CASE STUDIES
PROPOSED SOLUTIONS

Gen Tamura
August 7, 2024

Threat Brief

Alison Yakabe

Intelligence Officer
DHS Intelligence & Analysis

TLPAMBER

THREAT LANDSCAPE – COURTING CONVERGENCE

6 AUGUST 2024

TLPCLEAR

Jonathan Greig

September 22, 2022

Cybercrime | Malware

BY THE HEADLINES

One year after the Oldsmar water breach, some experts question the utility's cybersecurity

WUSF Public Media - WUSF 89.7 | By Violet Comber-Wilen
Published February 4, 2022 at 5:00 AM EST

CrowdStrike outage sparks global chaos with airline, bank and other disruptions

Over 2,500 flights were canceled and more than 8,000 were delayed in the U.S.

By Nadine El-Bawab, Josh Margolin, and Jon Haworth
July 19, 2024, 1:00 PM

Ransomware attack on food giant Dole Food Company blocked North America production

February 26, 2023 By Pierluigi Paganini

Patients struggle to get lifesaving medication after cyberattack on a major health care company

March 6, 2024, 12:31 PM PST
By Daniella Silva and Aria Bendix

The attack on Change Healthcare has upended the lives and work of patients, doctors and pharmacists because of outages in systems used for medical billing and insurance claims.

Colonial Pipeline hackers add startling new capabilities to ransomware operation

City of Oakland posts statement on ransomware attack, as hackers begin posting data online

By Jana Katsuyama | Published March 6, 2023 | Sheng Thao | KTVU FOX 2 |

FBI Attributes JBS Cyberattack To Russia-Linked 'REvil' Ransomware Operation

CBS NEWS COLORADO

JUNE 3, 2021 / 10:41 AM / CBS COLORADO

Russia-linked hacking group suspected of carrying out cyberattack on Texas water facility, cybersecurity firm says

By Sean Lyngaas, CNN
5 minute read · Published 6:07 AM EDT, Wed April 17, 2024

China-backed hackers are infiltrating Guam cyberinfrastructure. Is Hawaii next?

By Annalisa Burgos
Published: May. 28, 2023 at 12:28 PM PDT

Example

TLPAMBER 911 and 311 outages (4/17/2024, multiple fusion centers)

Open-Source Report: (U) 911 Outage In 3 States Linked To Cut Fiber Wire During Pole Installation; FCC Investigating--MMC IOI #20240418-18
General Distribution

Location(s): United States
NOC Number: NOC 0147-24 [911 Service Outages - Multiple States]

The outage of 911 systems in three states Wednesday evening was caused by the installation of a light pole, according to Lumen, a company that supports some of those systems, media reported on Thursday
Customers in Nevada, South Dakota, and Nebraska "experienced an outage" when a third-party company, unrelated to Lumen, "physically cut our fiber" while "installing a light pole," a company spokesperson said
An outage was also reported in a fourth state, Texas, but Lumen said it does not provide 911 services in Texas
Some agencies said the issue was with wireless carriers
Sarpy County 911 in Nebraska said on Wednesday night that “some wireless carriers are not able to reach 911,” and the matter was resolved about three hours later
Del Rio police in Texas also said the issue was with T-Mobile and not the City of Del Rio systems
So far, there’s no indication that the outages were caused by a cyberattack or other malicious act, law enforcement officials told NBC News on Thursday

Examples

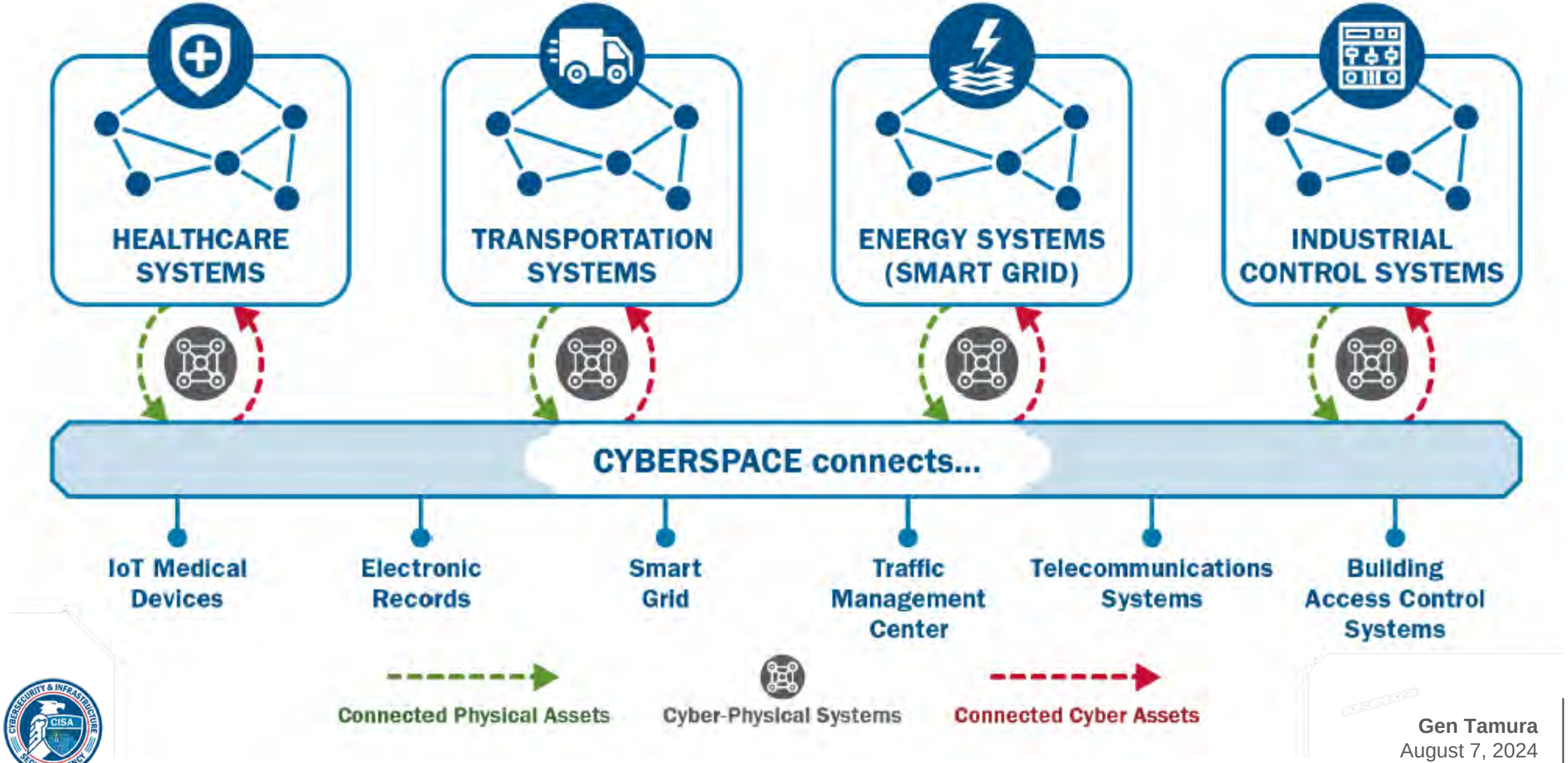
TLPCLEAR **Tracy Resident Sentenced to Serve Home Confinement and Probation for Computer Attack on Discovery Bay Water Treatment Facility** (5/13/2024, FBI)

- https://www.justice.gov/usao-ndca/pr/tracy-resident-sentenced-serve-home-confinement-and-probation-computer-attack

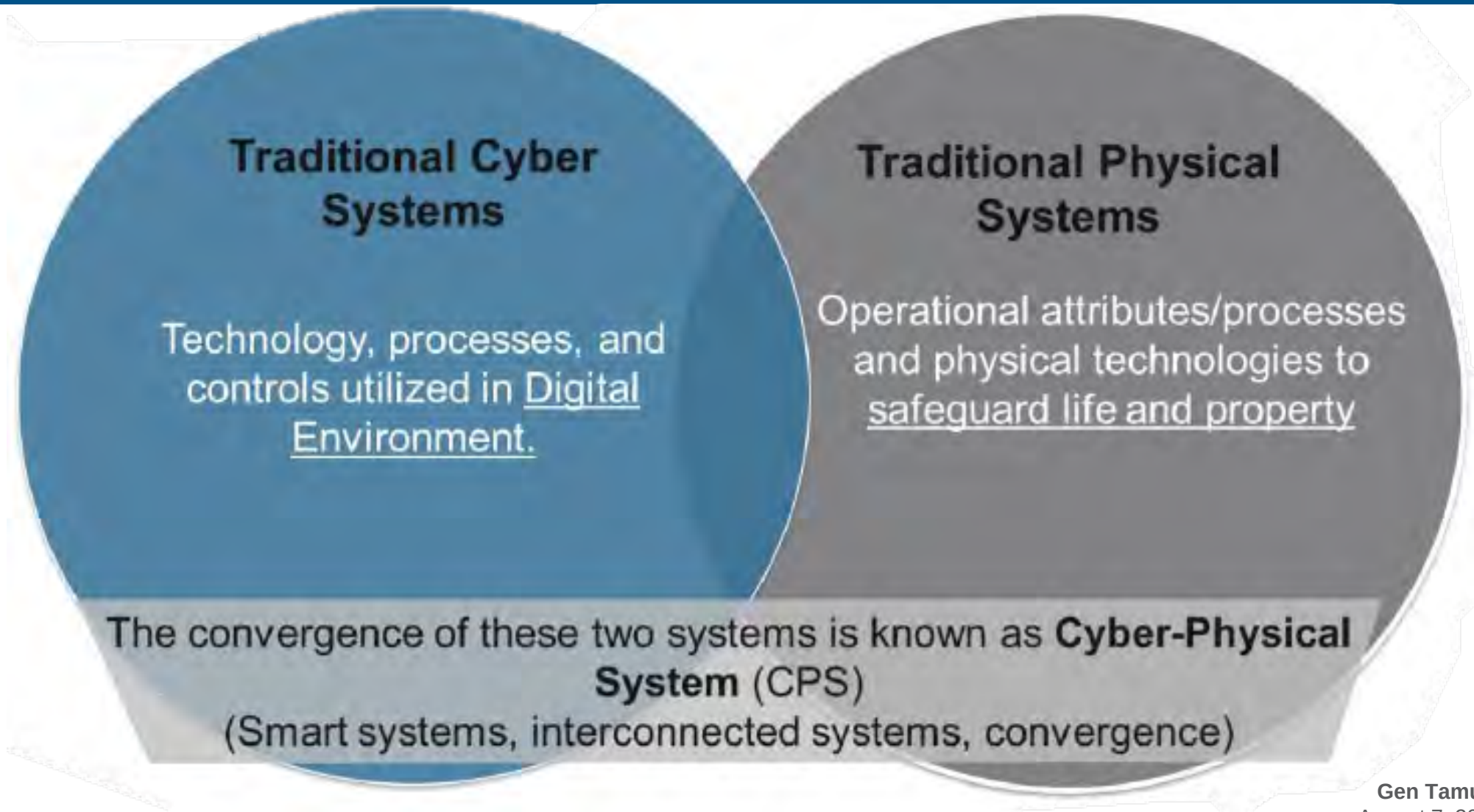
TLPCLEAR **Gray Market Components Found at Transportation Sector Entity** (12/2018, DHS I&A)

ALISON.YAKABE@HQ.DHS.GOV

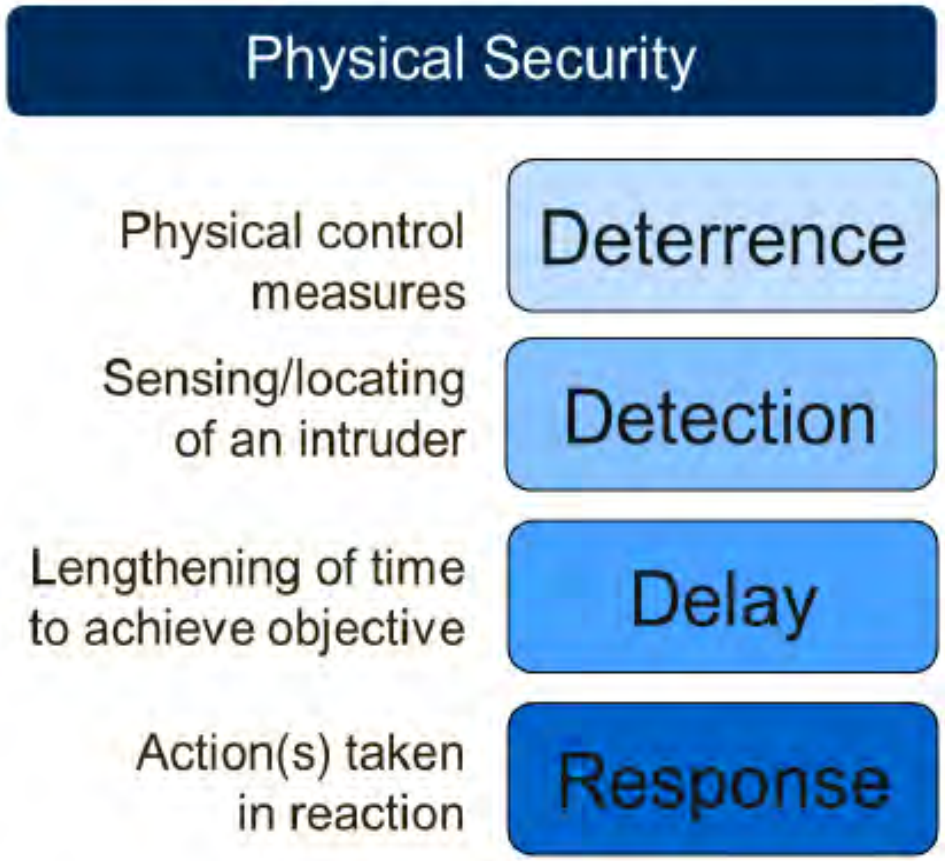
The Importance of Convergence

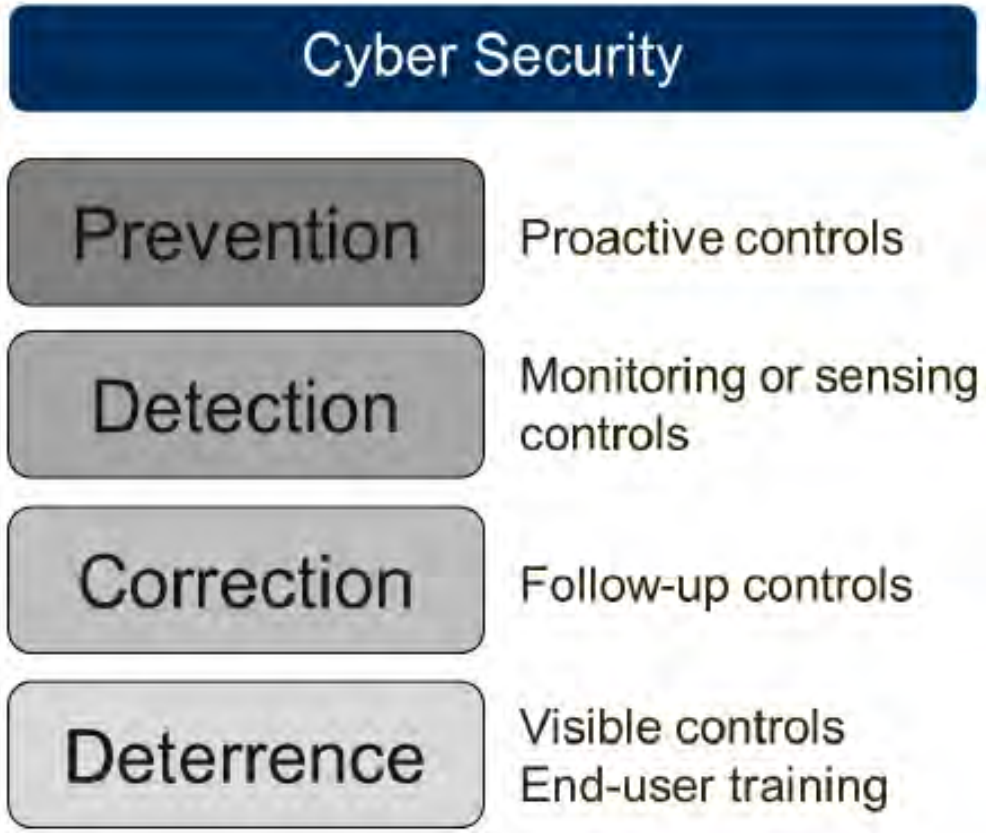


Risk Overview



Holistic Security





How do we align these?

Large Foreign Shipping Company

What can we learn from it?

•**Patch management**: Although the company had regularly installed software updates and patches, it had not installed the patch for the specific vulnerability that NotPetya used.

•**Backups**: Backups of its systems were not up-to-date and were not kept in an isolated location.

•**Network segmentation**: Attackers could move from one system to another causing damage to multiple systems.

•**Software integrity**: It is possible that it was delivered through a forged software update.

Large U.S. Energy Company

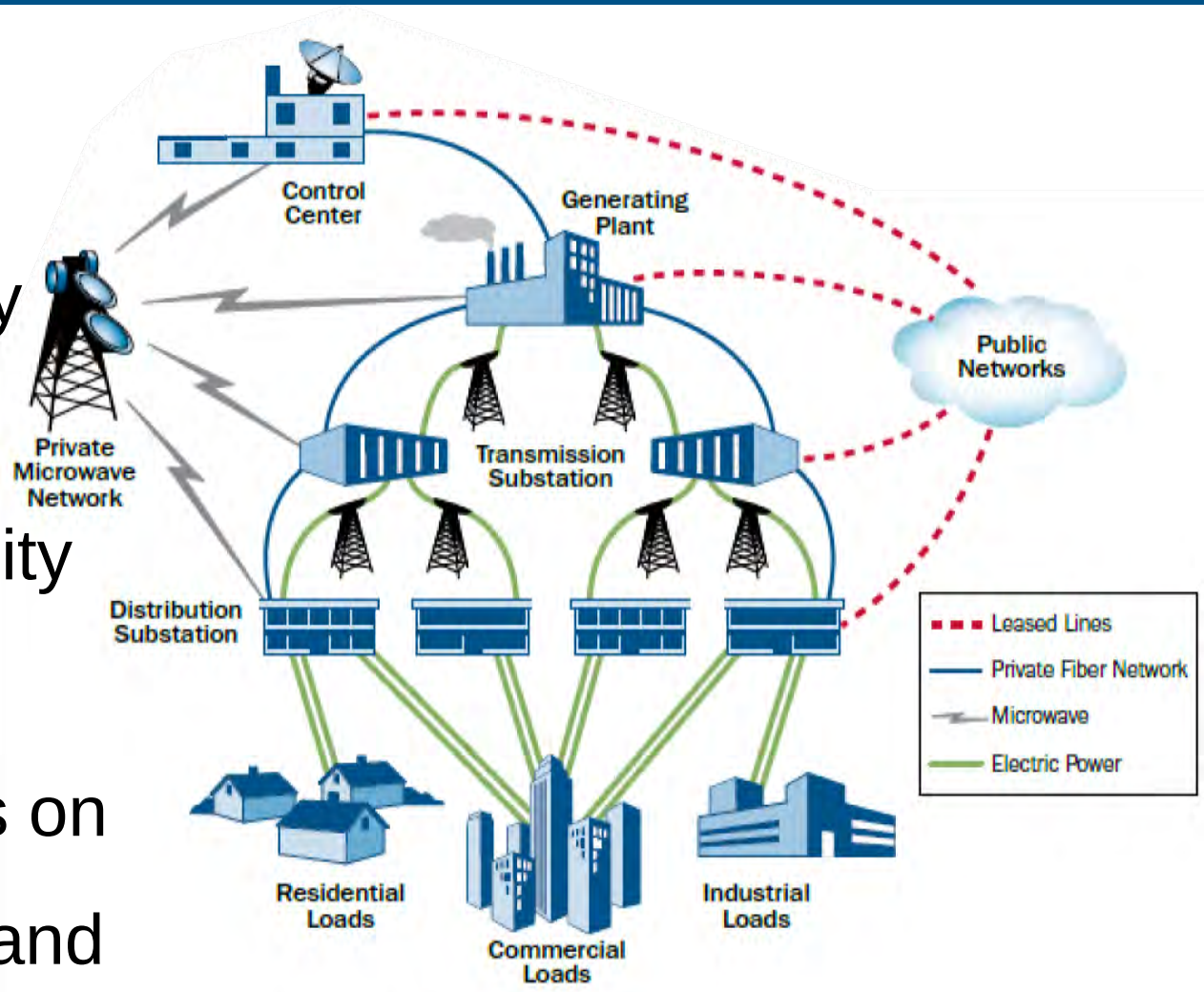
- Problems
  - Lack of Incident Plans
  - Mitigation For The Introduction Of Malicious Code
  - Protection Manager Not Identified in a Timely Manner

- **Solutions**
  - **Develop Robust Incident Plans**
  - **Acceptable use Policy of Cyber Assets and Removable Media**
  - **Keep Documentation of Manager and Any Delegations Up-to-date**

U.S. Power Grid Operator

Key Impacts:

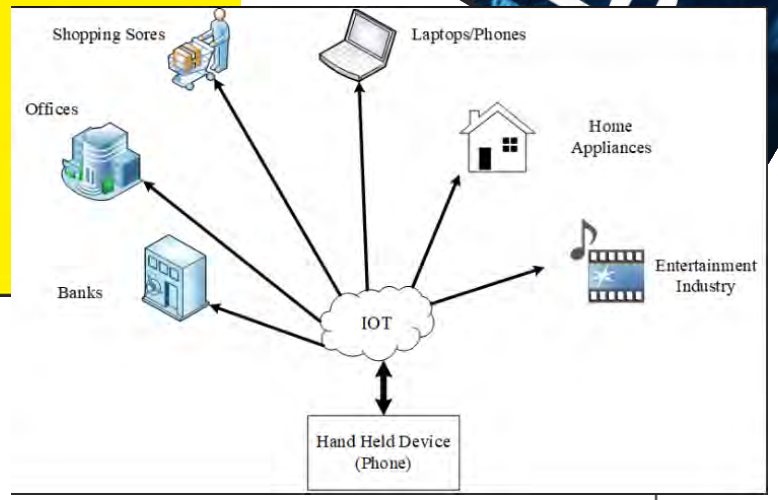
- **Disruption** of communication and control systems, affecting grid stability and management.
- **Increased** scrutiny on existing security measures and protocols.
- **Prompted** industry-wide discussions on improving vulnerability management and network security practices



Devices Impacted by Ripple20 Vulnerabilities

Lessons Learned:

1. Importance of Regular Vulnerability Assessments
2. Timely Software Updates
3. Robust IoT Security Measures



Challenges and Barriers

Communication Gaps

Initiate a Dialogue

Enable communication with security leaders. Engage with upper management to discuss what convergence might look like within your organization—successful convergence relies on support from senior leaders.

Review Leadership Roles

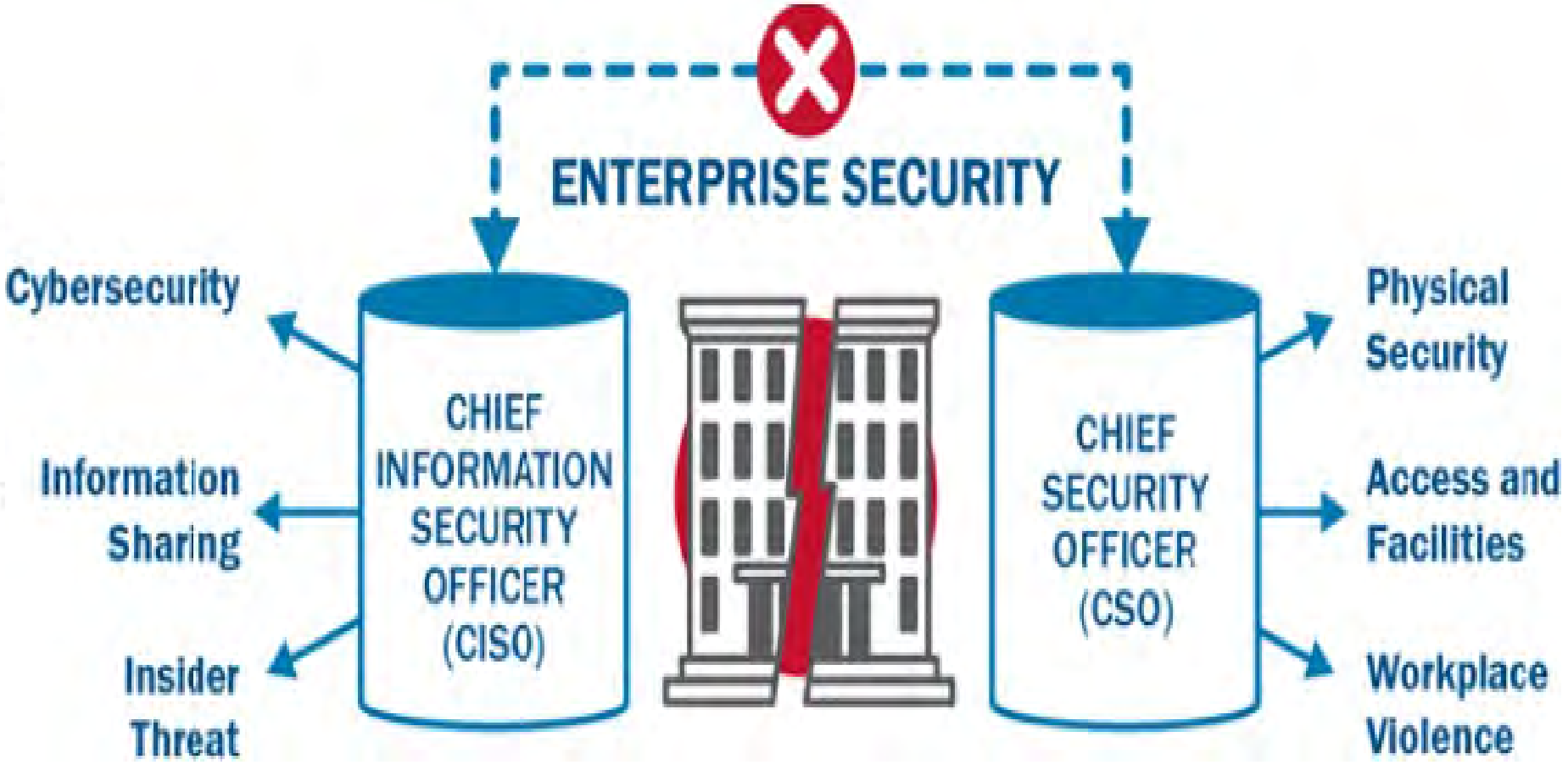
Discuss whether your current leadership structure can be realigned.

Establish a Convergence Team

Identify key players, such as CSO, CISO, physical security, IT, cybersecurity, and facility managers.

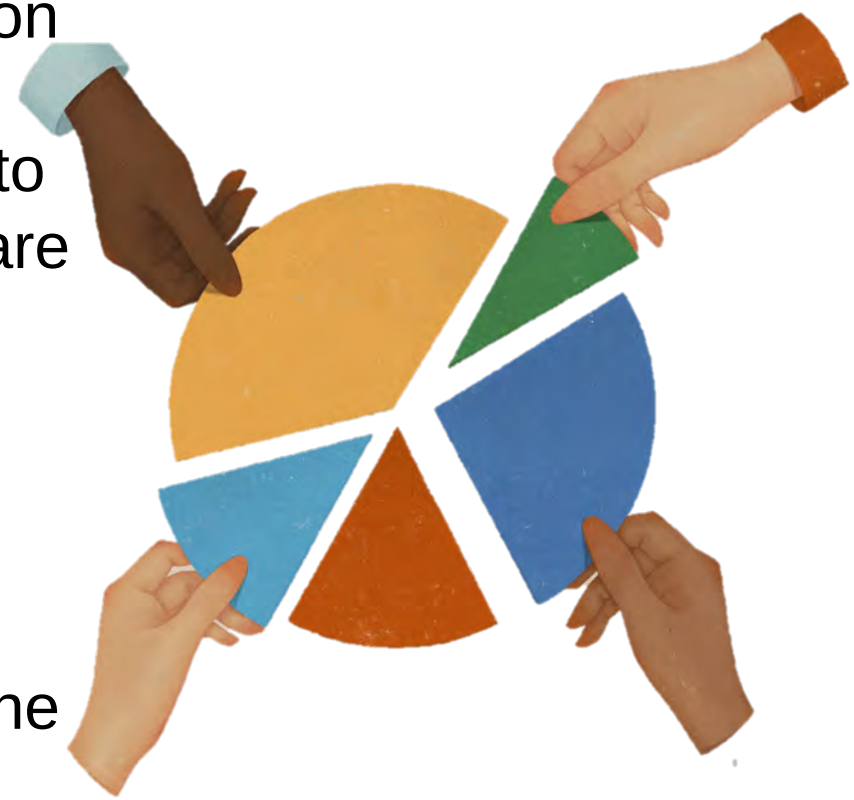
Enable Information Sharing

Engage with team members across all security functions to identify points of convergence.



Resource Allocation

Formalize Convergence Teams Roles and Responsibilities:
Establish a structure for a team coordination and integration
Identify Linked Assets:
Coordinate with team members across security functions to assess cyber and physical assets and identify those that are linked.
Conduct A Vulnerability Assessment:
identify gaps in security and risk mitigation and determine where gaps can be closed through convergence
Determine A Baseline:
Leverage initial assessments and gap analysis to determine the baseline for security and incident management



Proposed Solutions

Security Assessments

1.Identifying Vulnerabilities: Assessments help in identifying new and existing vulnerabilities in your systems, which can be exploited by attackers. This addresses weaknesses prior to are exploitation.

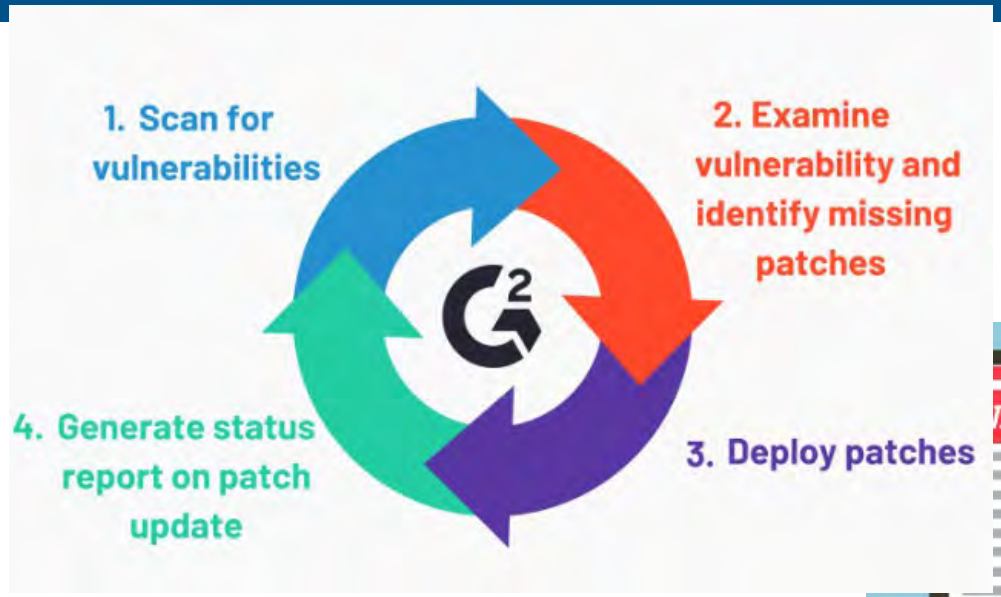
2.Improving Resilience: By assessing your security posture, you can improve your organization's ability to withstand and recover from cyber and physical attacks. This continuous improvement is key to building resilience.

3.Risk Management: Assessments allow for the continual evaluation to allocate and prioritize.

4.Adapting to Changes: Assessments help your organization adapt to new threats in your operational environment, ensuring that measures remain effective.

Best Practices

- Regular Vulnerability Scanning:
- Patch Management
- Risk Assessment and Automated Tools and Solutions
- Regular Penetration Testing
- Employee Training and Awareness



Unified Policies

Information Sharing

- ✓ **Creating a Culture of Collaboration**
- ✓ **Establishing Clear Communication Channels**
- ✓ **Developing Standard Operating Procedures (SOPs)**
- ✓ **Implementing Cross-Functional Teams**
- ✓ **Providing Training and Awareness Programs**
- ✓ **Leveraging Technology**
- ✓ **Encouraging a No-Blame Culture**

Interactive Poll/Survey

"How integrated are your cyber and physical security functions?“

- Options:
  - Not integrated
  - Partially integrated
  - Fully integrated

"What is the biggest challenge your organization faces in converging security functions?”

- Options:
  - Communication gaps
  - Resource allocation
  - Lack of expertise
  - Others (please specify)

"What additional insights or experiences would you like to share about converging cyber and physical security functions in your organization?

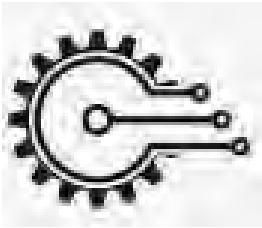
Desired Outcomes

1.Conduct a Security Assessment: Evaluate your security posture, identify vulnerabilities, and assess the integration of cyber and physical security functions.

2.Foster Interdepartmental Communication: Establish communication channels between cyber and physical security teams to share insights and coordinate efforts.

3.Develop and Implement Unified Security Policies: Create policies that address both cyber and physical security concerns.

4.Invest in Technology: Utilize integrated platforms and tools that facilitate the convergence of cyber and physical security.



5.Provide Training and Awareness Programs: Educate employees about the importance of converging functions and their role in maintaining a secure environment.

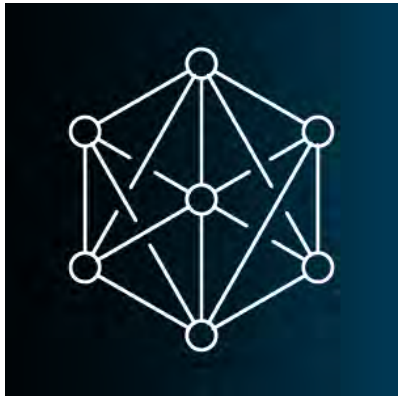
Long-term Impact

- Improved Resilience
- Reduced Risk
- Enhanced Trust and Confidence
- Cost Savings

Conclusion

1. **Enhance Collaboration:** Break down silos between teams and foster a culture of inclusivity and communication.
2. **Update Security Protocols:** Regularly review and update your security protocols to reflect the latest best practices.
3. **Invest in Technology:** Leverage advanced technologies to facilitate the integration of cyber and physical security.

Questions?



For more information:
www.cisa.gov

Questions?
Email: gen.tamura@cisa.dhs.gov
Phone: 808-445-2161


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY