U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Region 1
New Hampshire
Jason Climer & Rick Rossi

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

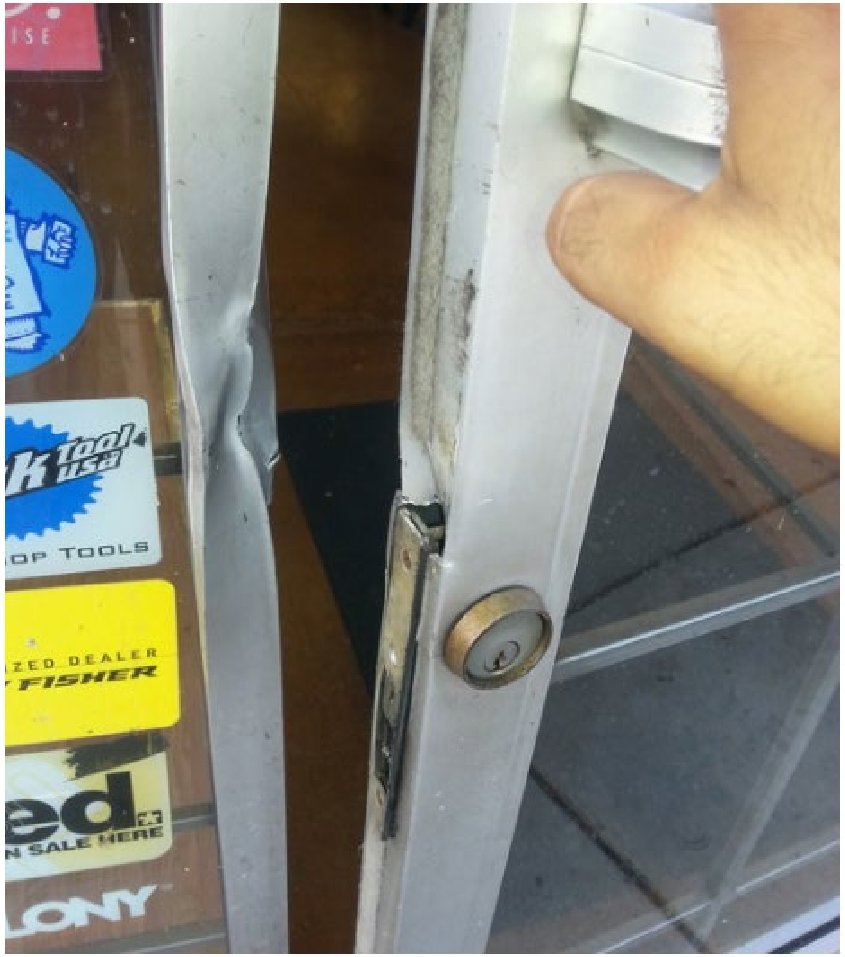
Our Work

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

Setting the Scene

Monday Morning after a Holiday Weekend…



Employee Entrance

Operational Control Area

Monday Morning after a Holiday Weekend…

DEFEND TODAY,
SECURE TOMORROW

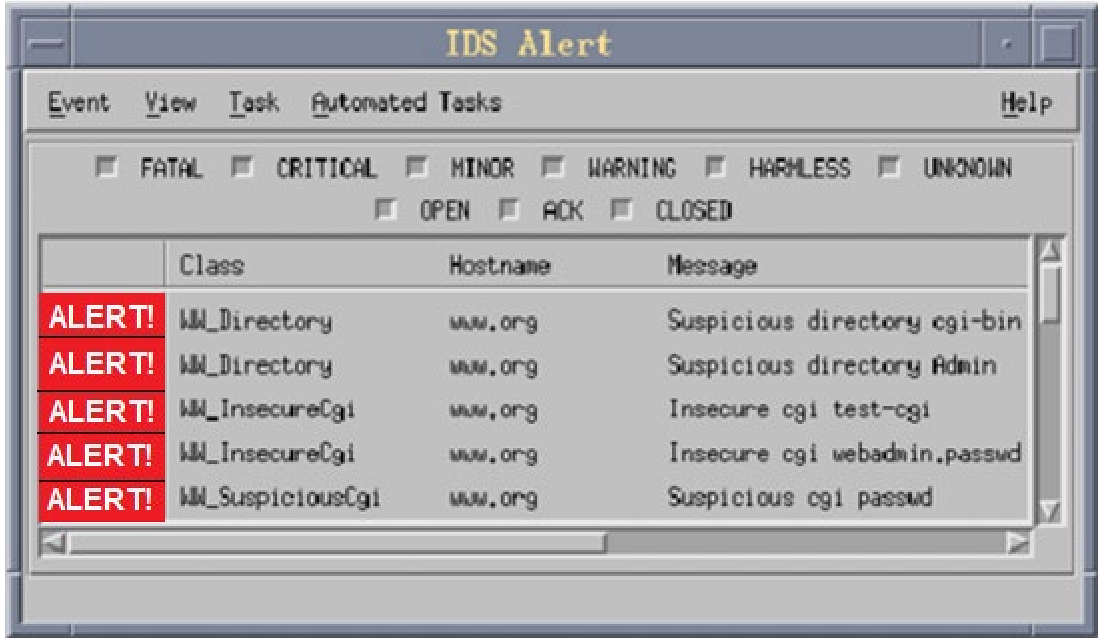
- Do you call security and the police?
- Do you inventory the compromised area to determine if anything is missing?
    - This may be your entire office including operational equipment for the water or wastewater system.
- What else would you consider doing in this situation?

Monday Morning after a Holiday Weekend…

DEFEND TODAY,
SECURE TOMORROW

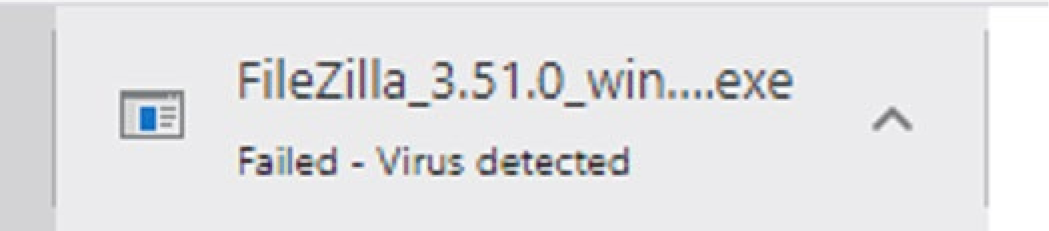
- Would you ever consider calling your IT department?
- Why would that be a consideration?
- How can you tell if the intruder inserted a thumb drive into your network?
- Conversely, does security ever get called when a cyber incident or attack happens? Why would that be relevant?

What Happens when you Reverse the Scenario?



☐ FATAL ☐ CRITICAL ☐ MINOR ☐ WARNING ☐ HARMLESS ☐ UNKNOWN
☐ OPEN ☐ ACK ☐ CLOSED

	Class	Hostname	Message
ALERT!	WW_Directory	www.org	Suspicious directory cgi-bin
ALERT!	WW_Directory	www.org	Suspicious directory Admin
ALERT!	WW_InsecureCgi	www.org	Insecure cgi test-cgi
ALERT!	WW_InsecureCgi	www.org	Insecure cgi webadmin.passwd
ALERT!	WW_SuspiciousCgi	www.org	Suspicious cgi passwd



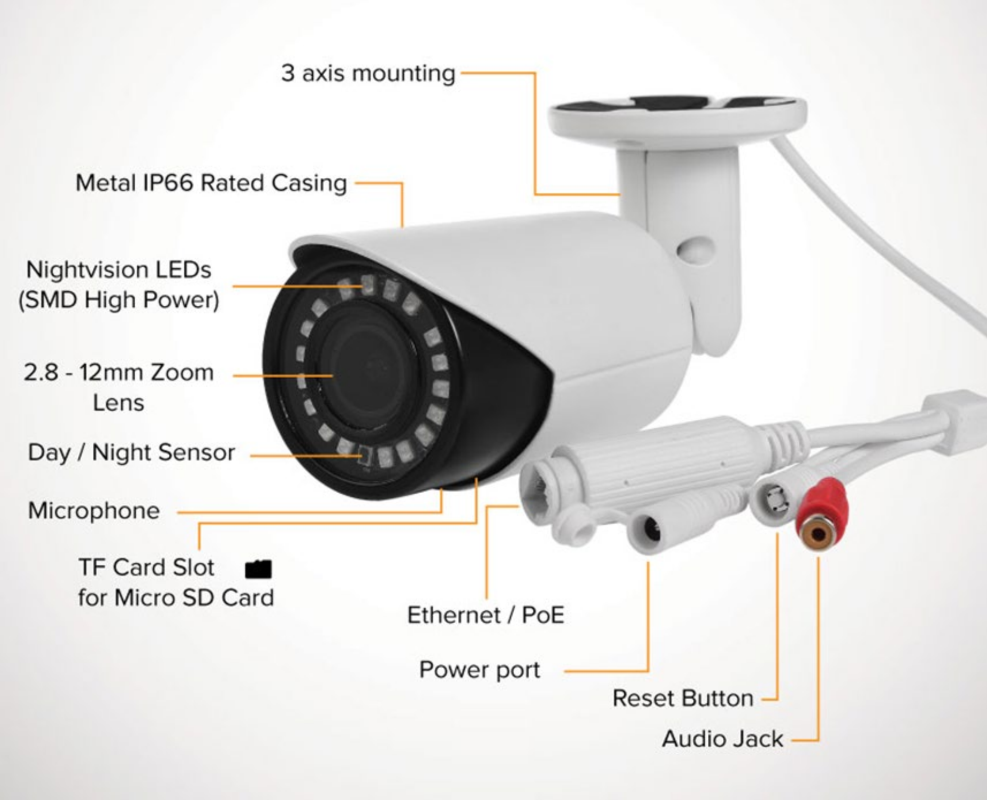
FileZilla_3.51.0_win....exe

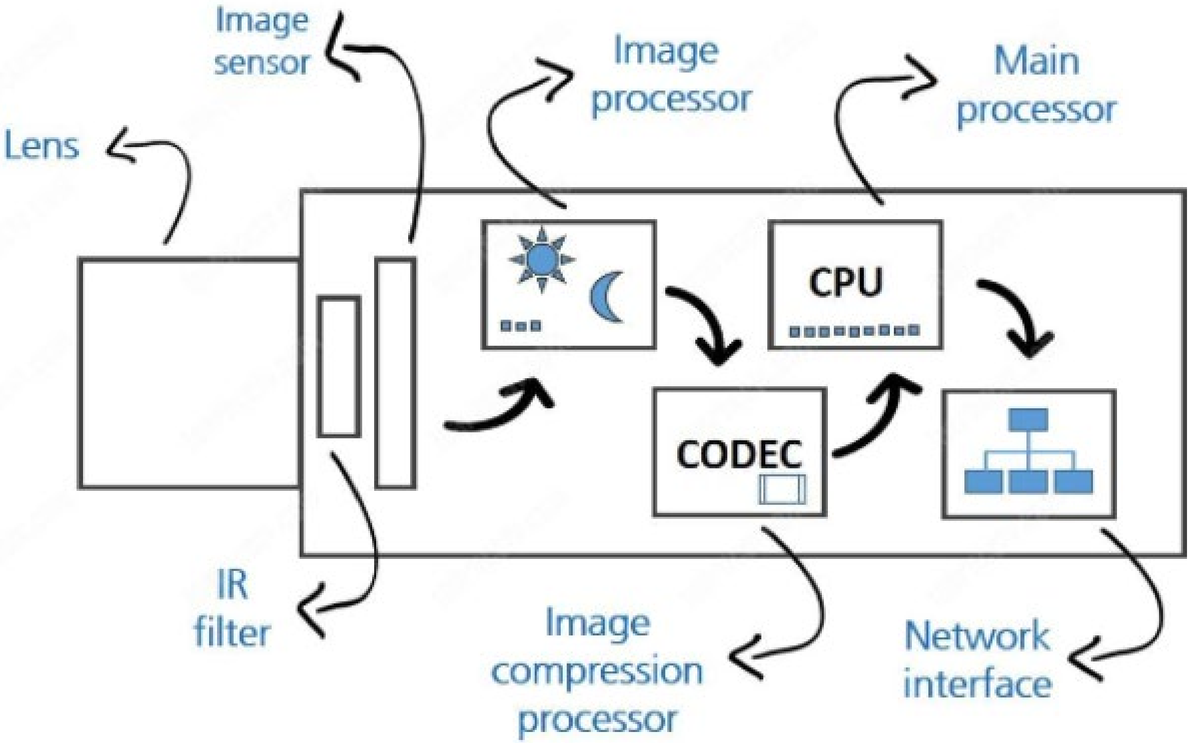
Failed - Virus detected

Would you ever consider calling physical security department?

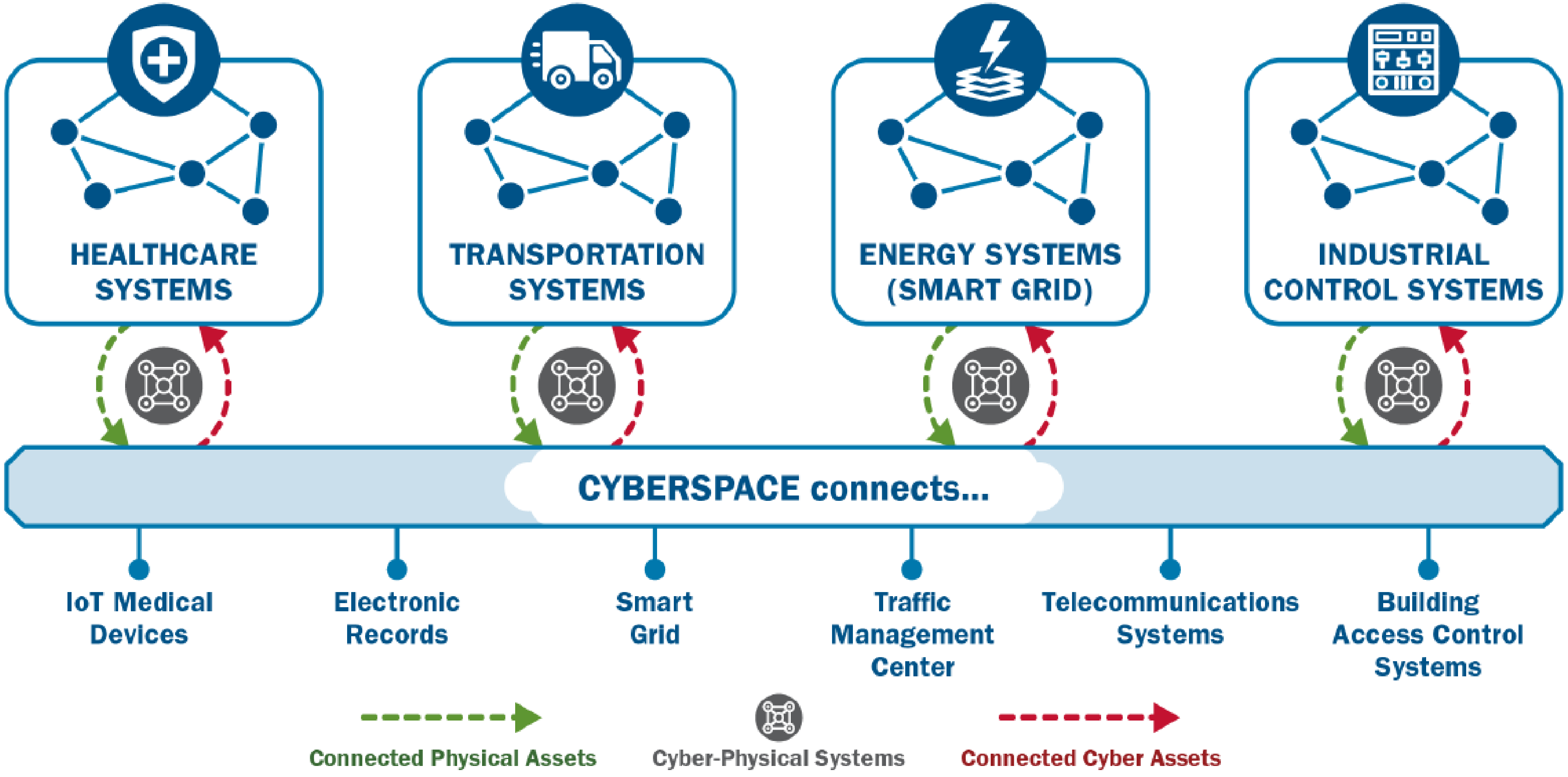
Cyber-Physical Convergence

Is this Physical Security or Cybersecurity?





A Connected Environment



HEALTHCARE SYSTEMS

TRANSPORTATION SYSTEMS

ENERGY SYSTEMS (SMART GRID)

INDUSTRIAL CONTROL SYSTEMS

CYBERSPACE connects...

IoT Medical Devices

Electronic Records

Smart Grid

Traffic Management Center

Telecommunications Systems

Building Access Control Systems

Connected Physical Assets

Cyber-Physical Systems

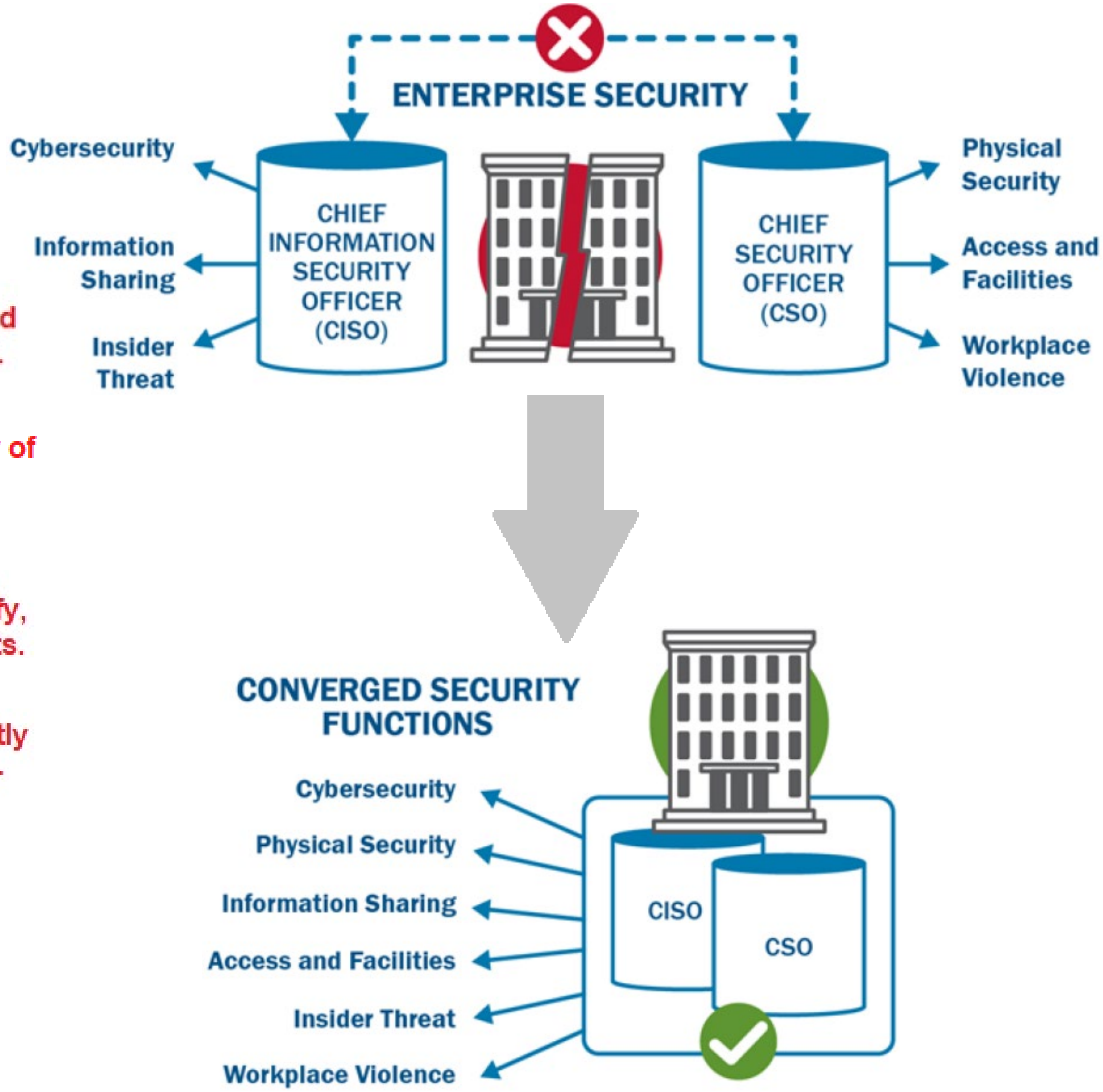
Connected Cyber Assets

The Challenge and the Solution

ORGANIZATIONAL CHALLENGE

Siloed Security Functions

- ✗ Lines of communication are unclear and impede coordination and collaboration.
- ✗ Senior leaders and teams lack visibility of interconnected physical and cyber assets.
- ✗ Organization is unable to quickly identify, prevent, and respond to complex threats.
- ✗ Security functions operate independently with limited collaboration on enterprise-wide risks.



ENTERPRISE SECURITY

CHIEF INFORMATION SECURITY OFFICER (CISO)

Cybersecurity

Information Sharing

Insider Threat

CHIEF SECURITY OFFICER (CSO)

Physical Security

Access and Facilities

Workplace Violence

CONVERGED SECURITY FUNCTIONS

Cybersecurity

Physical Security

Information Sharing

Access and Facilities

Insider Threat

Workplace Violence

CISO

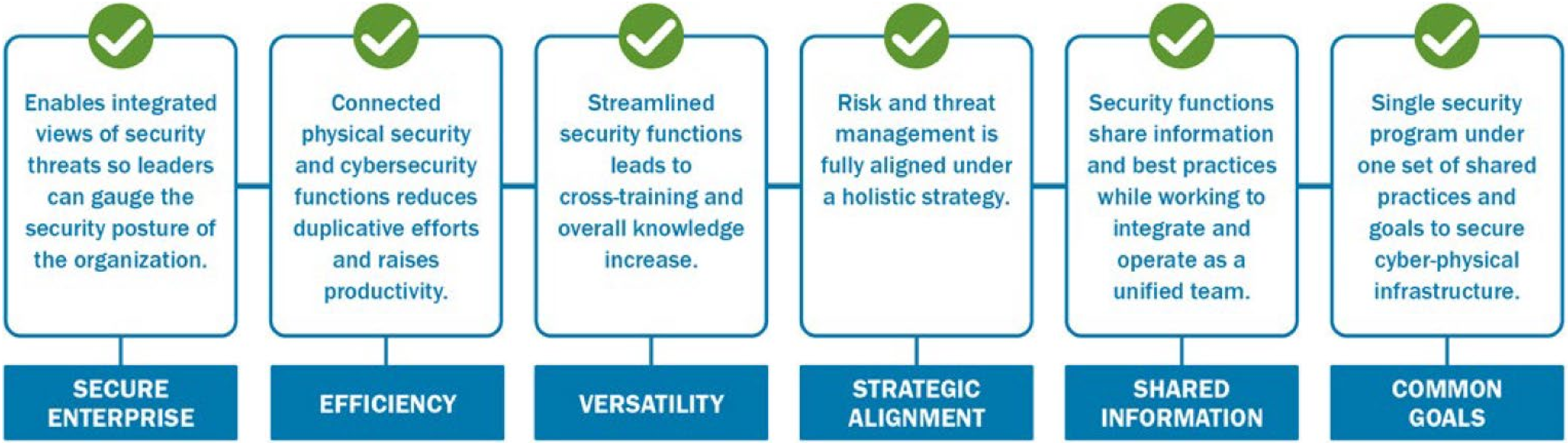
CSO

ORGANIZATIONAL SOLUTION

Converged Security Functions

- ✓ Integrated security functions address cyber-physical infrastructure security
- ✓ Senior leaders and teams communicate, coordinate, and collaborate.
- ✓ Organization is prepared to prevent, mitigate, and respond to threats.
- ✓ Holistic threat management ensures physical and cyber assets are secure.

Benefits of Convergence



Enables integrated views of security threats so leaders can gauge the security posture of the organization.

SECURE ENTERPRISE

Connected physical security and cybersecurity functions reduces duplicative efforts and raises productivity.

EFFICIENCY

Streamlined security functions leads to cross-training and overall knowledge increase.

VERSATILITY

Risk and threat management is fully aligned under a holistic strategy.

STRATEGIC ALIGNMENT

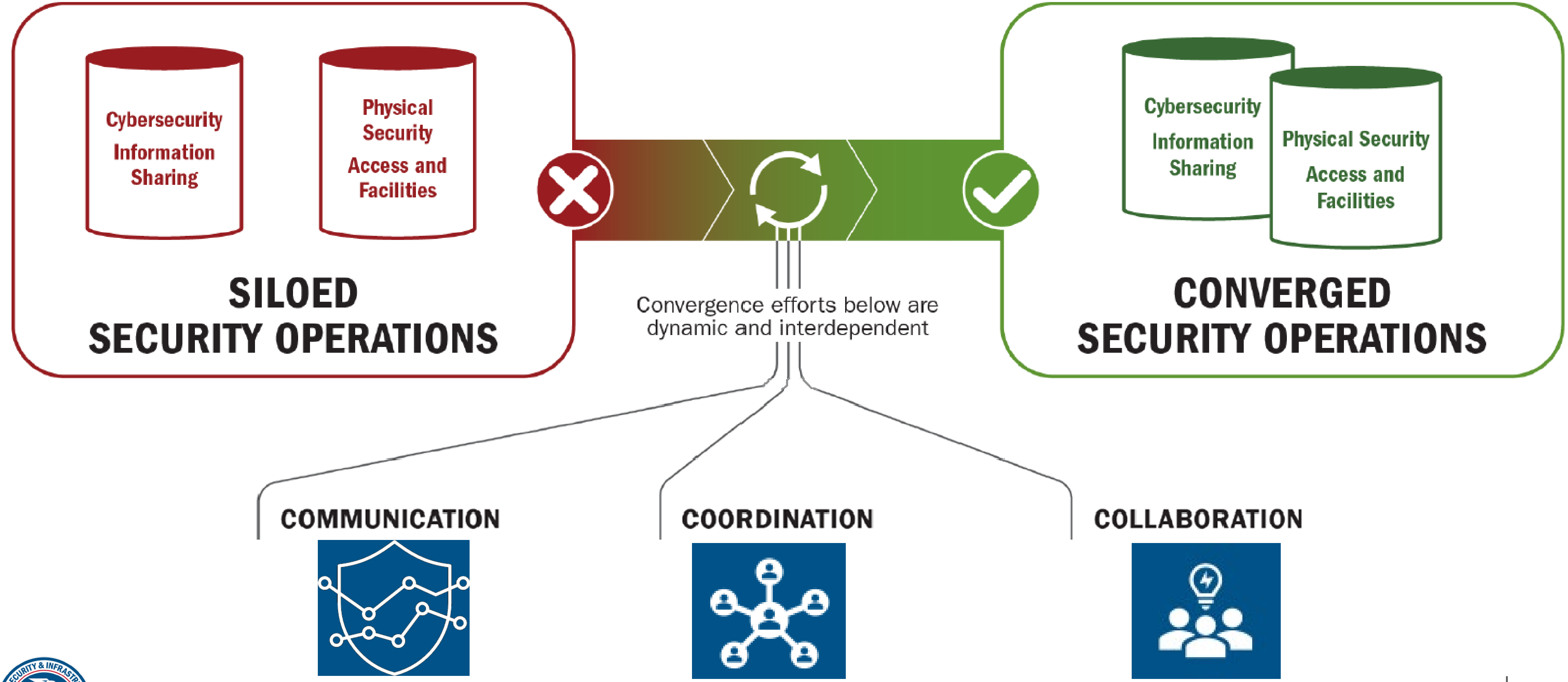
Security functions share information and best practices while working to integrate and operate as a unified team.

SHARED INFORMATION

Single security program under one set of shared practices and goals to secure cyber-physical infrastructure.

COMMON GOALS

Framework for Aligning Security Functions



No Cost Resources

Cybersecurity Programs and Resources

Preparedness Activities

- Ransomware Readiness Assessment
- Cybersecurity Training and Awareness
- Cyber Exercises and “Playbooks”
- Information / Threat Indicator Sharing
- National Cyber Awareness System

Field-based Cybersecurity Advisors (CSAs)

- Incident response coordination
- Cyber assessments
- Working group collaboration
- Public-private advisory assistance
- Public Private Partnership Development
- Threat intelligence and information sharing
- Incident Response Plan Development
- Vulnerability Disclosure Plan Development

Resources

- Cyber Essentials
- Bad Practices
- Stuff off Search
- Cybersecurity Evaluation Tool (CSET)
- StopRansomware.gov
- Catalog of Known Exploited Vulnerabilities
- STOP. THINK. CONNECT
- Joint Cyber Defense Collaborative

Jason Climer & Rick Rossi
November 22, 2021

PSA Programs and Resources

DEFEND TODAY,
SECURE TOMORROW

Capability Summary

- Vulnerability assessment
- Advisory services
- Information sharing
- Guidance/standards development
- Regulatory administration
- Inspections
- Technical assistance
- IT tools and services
- Training
- Exercises
- Coordination and management
- Capability/requirements assessment
- Security planning

Program Summary

- Soft Targets and Crowded Places
- School Safety
- Bombing Prevention
- Protective Security Advisors
- Chemical Facility Anti-Terrorism Standards (CFATS) and Chemical Security
- TRIP*wire*
- Interagency Security Committee
- Vulnerability Assessments and Regional Risk Assessments
- IP Gateway and Homeland Security Information Network-Critical Infrastructure
- Sector Expertise
- National Infrastructure Protection Plan (NIPP) Management
- Security Training & Exercises
- Incident Response & Recovery Programs

NH Contacts

CISA Contact Information

Jason Climer Protective Security Advisor	jason.climer@cisa.dhs.gov +1 202-897-7666
Rick Rossi Cybersecurity Advisor	richard.rossi@cisa.dhs.gov +1 202-770-8991

CYBERSECURITY & INFRASTRUCTURE

CISA

SECURITY AGENCY