
13TH ANNUAL LEADERSHIP EVENT
CYBER SECURITY SUMMIT
cybersecuritysummit.org
RESILIENCE UNLOCKED
TITLE SPONSOR
Island
#cybersecuritysummit #css13

Critical Infrastructures: Proactive Security & Resilience

Addressing the evolving and sophisticated cyber-physical threats to critical infrastructures.

Matthew Vatter

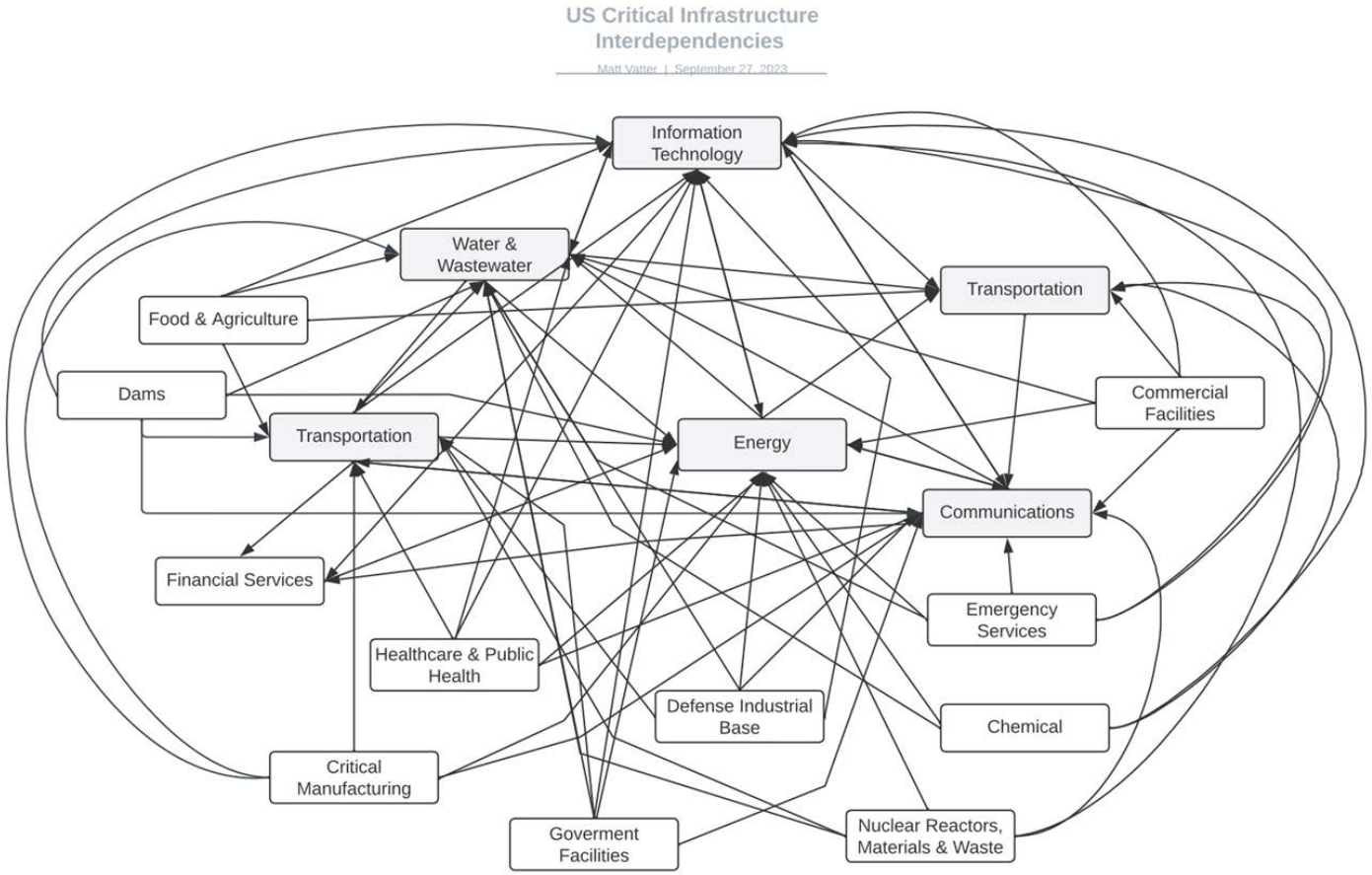
Chief Compliance Officer
Accelerate2Compliance

Today’s Agenda

1. Introduction
2. Understanding Critical Infrastructure
3. The Significance of Proactive Security
4. Building a Resilient Framework
5. The Role of Technology
6. Regulatory Framework and Compliance
7. The Human Factor: Training and Awareness
8. Future Challenges and Opportunities
9. Conclusion and Q&A

Understanding Critical Infrastructures

- 16 Interdependent Sectors
- Public and Private sector responsibilities
- Collaborative information share and security (ISACs, NIPP)
- Danger of Siloed Threat intelligence



The Significance of Proactive Security

National Security

- Disruption inhibits functionality of critical systems and services degrading the ability to protect ourselves

Economic Stability

- Disruption destabilizes finical systems, supply chains and erodes consumer confidence

Public Safety

- Failures and attacks can result in loss of life, environmental damage, population displacement

Mitigation of Potential Threats

- Proactivity identifies threat and vulnerabilities before they can be exploited, reducing damage and disruption

Resilience

- Proactivity enables systems to better withstand and recover from disruptions regardless the cause

Deterrence

- Proactivity makes-well protected infrastructures a more difficult target and ones less likely worth the resources required for success

Building a Resilient Framework

Resiliency	vs.	Redundancy
Ability to adapt to, recover from and continue functioning in the presence of disruptions, adversity or unexpected challenges/events		Involves creating duplicate or back-up systems, components or resources that provide immediate substation in the event of failure or disruption

What are resilient Critical Infrastructures?

- Physical and digital systems rapidly identify, mitigate and recover from incidents
- Institutional culture anticipates threat
- Cross-sector entities share technology and intelligence
- All-hazards approach to preparedness, response and recovery

The Role of Technology

IoT, AI, Machine learning and Predictive Analysis

- Do the mundane and redundant things more efficiently
- Rapid and continual analysis gets us closer to predictive response
- Machines interacting across sectors allows for a broader data set
- ICS and SCADA ‘talking’ to each other

Privacy and Ethical Considerations

- Interconnected IoT collects and uses personal and proprietary data
- Modeling Bias
- Proactive response and threat to due process

Regulatory Framework and Compliance

NIST, CIP, NIPP and other relevant regulations

- Frameworks developed by industry and government
- Flexible but standardized
- Collaborative by design
- Federal, State, tribal, local and International considerations

The Importance of Regulatory Compliance

- Establishes measured expectations and consistency across sectors
- Identifies minimum standards for operational architectures
- Enforces mutually supportive technical and administrative controls

The Human Factor: Training and Awareness

The importance of a trained workforce

- Building a security-aware culture
- Encouraging proactive security behaviors
- Refine the role of the "human in the loop"
- Ability to solve complex problems vs. institutional experience
- Gamers mindset

Stock Image

Future Challenges and Opportunities

Trends in cyber and physical security

- Migration from reactive to proactive security, threat intelligence
- AI to replace mundane and complex data related functions
- Proliferation of interconnections and dependencies
- Increasing complexity of systems – example: automated EVs in the transportation network

Emerging Technologies and their implications

- What is used for good is also used for evil
- Greater automation in communications requires near perfect support systems (energy)
- Decentralization and nodal architecture can lead to self-regenerating systems
  - New families of smart tools to enable this

Conclusions

People are the key to proactive security

Critical Infrastructures are the backbone of our society

Emerging technology will challenge and support efforts

Smart regulation integrates effort and resources across all sectors

Image courtesy of The Mandarin

Image courtesy of Chancery Group

Thank You

Matt Vatter
Chief Compliance Officer
Accelerate2Compliance
+1 763-271-9635
https://accelerate2compliance.com
Matt@accelerate2complaince.com

References:

Supply chains: To build resilience, manage proactively (Article) May 23, 2022, accessed online: https://www.mckinsey.com/capabilities/operations/our-insights/supply-chains-to-build-resilience-manage-proactively

Security Challenge for the Electricity Infrastructure (Article) for the Electric Power Research Institute, by Massoud Amin, 2002, Supplement to *Computer (provided by author)*

The Current State of Threat Intelligence, Olivia Powell, October 9,2023 accessed online: https://www.cshub.com/threat-defense/articles/the-current-state-of-threat-intelligence

PG&E Lays 350 Miles Of Underground Powerlines For Wildfire Protection and Improved Reliability In California, October 16, 2023 accessed online: Intelligent Undergrounding | T&D World