



# PRIORITIZING ACTIONS FOR MANAGING CYBER RISKS

**Debra Decker, Stimson Center**

*Based on Paper Prepared with*

*Kathryn Rauhut, Stimson Center, and Mark Fabro, Lofty Perch*


*February 2020, Vienna*

*IAEA International Conference on Nuclear Security*

# Overview

- **Trends in Risk Elements**

- Threats
- Vulnerabilities
- Consequences



**Spoiler alert:**  
Resilience is key!

- **Recommendations for Prioritizing Risk Management**

- For Licensees
- For International Organizations and Others

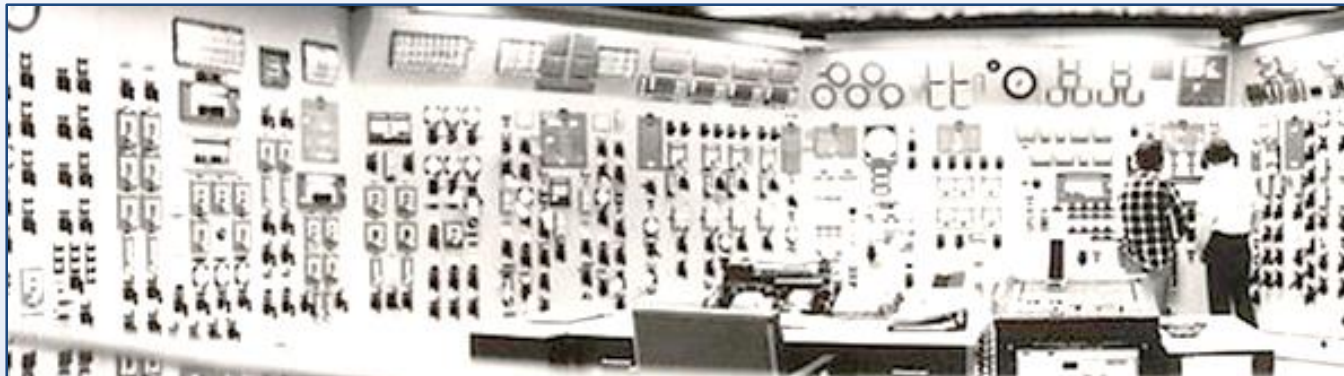
*“Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.” – EU definition*

# Threats

- Old World
  - IP theft
  - Modification/loss/acquisition of information
- New World
  - Persistent presence in critical infrastructure – both IT and OT
  - Targeted APT: State and Non-State

# Vulnerabilities

- Increasing digitization
- Supply chain and other third-party vulnerabilities
- 5G?
- AI and Distributed Ledger Technology?
- Other: Robotics, Electronic Devices....



# Consequences

- Secure, accurate, fast communication and responses needed
- Challenges!
  - Social media
  - “Deepfakes”
  - Insufficient planning/exercising

**Bottomline: Defense in depth and response management are critical!**

# Risk Management: *Licensees*

- Compliance necessary but insufficient
- Reduce vulnerabilities
  - Good cyber hygiene
    - Awareness training and certifications, automated protections, credential protection
  - Information sharing
    - But who should do and how?
    - Trusted partners?
- Broader response planning/training

# Risk Management: *IAEA+*

- More emergency practices
- Information sharing
  - Incident disclosure system like ITDB
  - Use common scoring system
- Pair with A/CPPNM RevCon
  - Develop tool to demonstrate compliance+
- More timely updates on good practices
  - Leverage others, e.g., COEs, electric utilities

# Agile management and cooperative approaches needed to address new and evolving risks!

*Thank you*

Debra Decker, Stimson Center

[ddecker@stimson.org](mailto:ddecker@stimson.org)

**“Prioritizing Actions for Managing Cybersecurity Risks”  
can be accessed in the  
IAEA 2020 ICONS Conference Report – Paper # 352  
and at [www.stimson.org](http://www.stimson.org)  
under the Nuclear Security Program**

Image Credits

Slide 1: Vogtle nuclear power plant, Georgia, USA: edited by BlatantWorld.com, and are re-released into the Public Domain

Slide 2: Control room for Unit 1, Donald C. Cook Nuclear Plant, Bridgman Michigan, USA: US Department of Energy photo



# Back-up Slides

# Types of Info Sharing

## - Incidents!

- Like IAEA Incident and Trafficking Database
- Common scoring systems
- Look at those deemed safety incidents from cyber

*Look to other industries, too – esp. for OT events – but <https://www.risidata.com/Database> out of date - Also, NTI cyber reg assessment out of date.*

*General Data Protection Regulation (GDPR), which provides necessary actions in response to disclosures, and repositories such as CVE [Common Vulnerabilities and Exposures] would help facilitate research in this topic.*

Negatives: The challenge is ensuring that shared information does not bolster attacker capability. Differing OT systems means lessons learned harder to do. Risk reduction may not be worth the effort

# Types of Info Sharing

- Legal and regulatory approaches
  - Look across States, IAEA undertake?
  - Pair with A/CPPNM RevCon? *Dashboard / series of metrics to enable all jurisdictions to demonstrate compliance and standards might be a good, common tool*
- Leverage others!
  - NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE)
  - Utilities, industries? *North American Electric Reliability Corporation (NERC)/Critical Infrastructure Protection (CIP) standards are mandatory for the electrical power industry*

# Types of Info Sharing

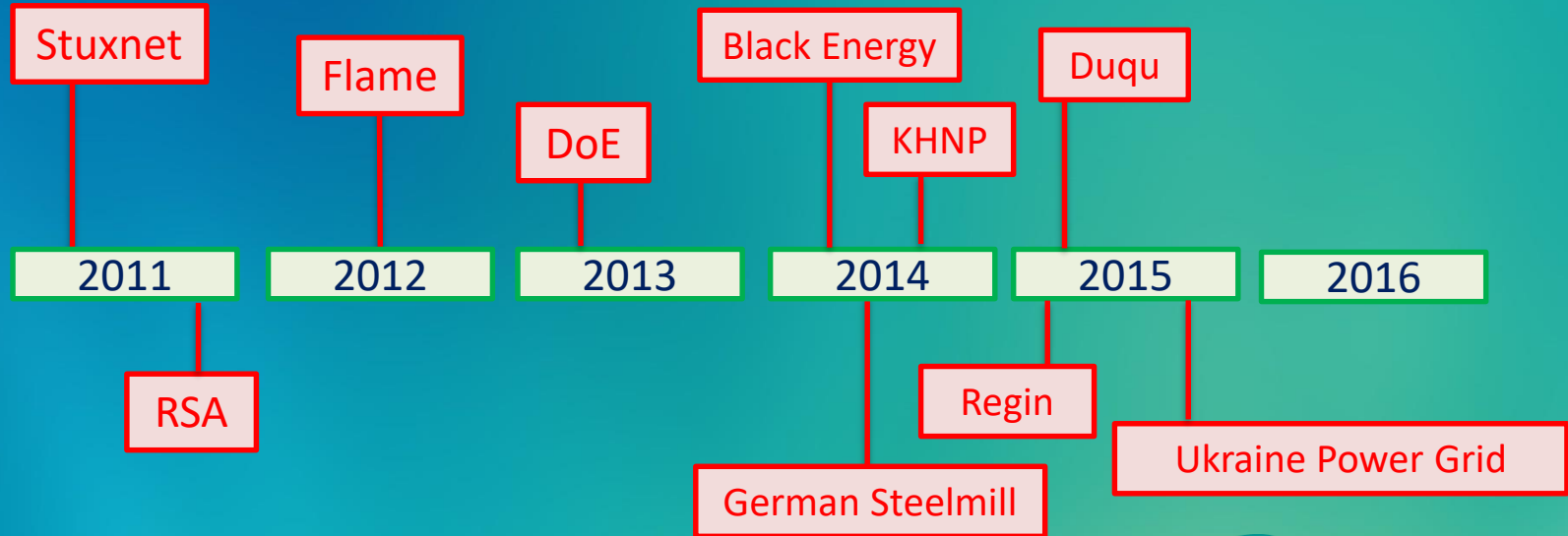
- Suppliers and supplies
  - Public certifications
  - Black/white lists

“Internationally-recognised certification of suppliers of Operational Technology, in addition to certification for IT security maturity, emerges as a practical ambition which brings the other facets together. This could serve to improve standards, make procurement decisions easier and enable a graded (and therefore more proportionate) approach, which should reduce costs in the longer term. It could also enable the cyber insurance market to reach a higher level of maturity. NGOs could assist in this ambition, so far (in the UK at least) nuclear industry group efforts have had limited success.”

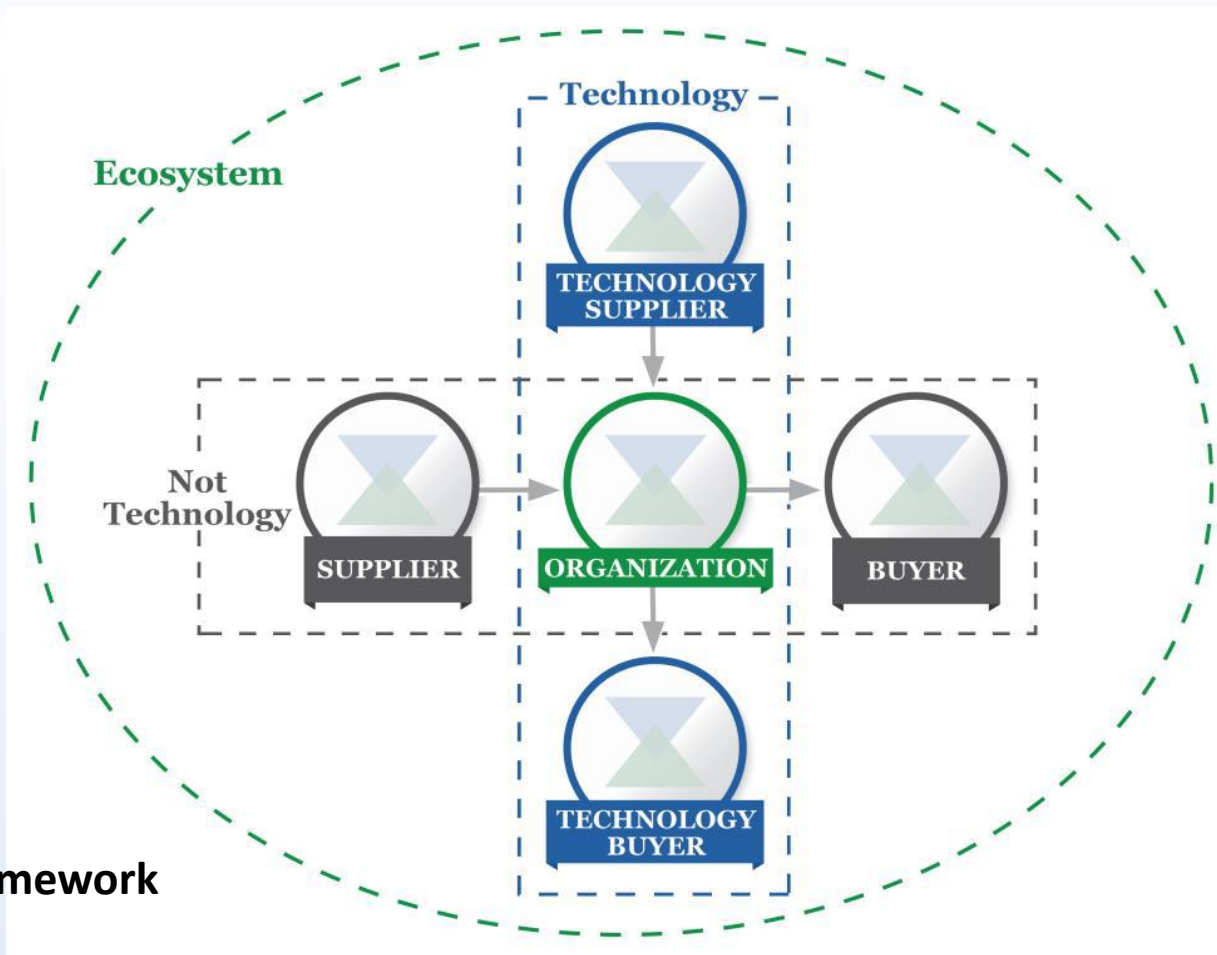
# Threat Landscape

Nuclear specific

General industry



# The Risks are Complicated!



NIST 1.1 Framework