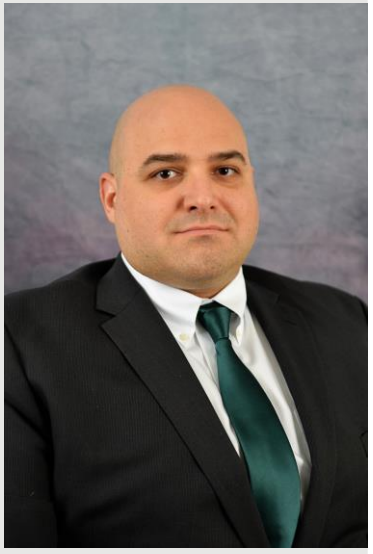
Cyber Supply Chain Risk Management and Conducting Cyber Risk Assessments

Cybersecurity and Digitalization:
Supply Chain Risks in the Electricity Sector

Agenda

- Introductions
- Cyber Supply Chain Risk
  - Vulnerabilities in devices and deployments
  - Country-of-origin
  - Practical example
- Cyber Supply Chain Risk Management
  - Asset Management
  - Industry collaboration
  - Mitigations
- Publicly available resources

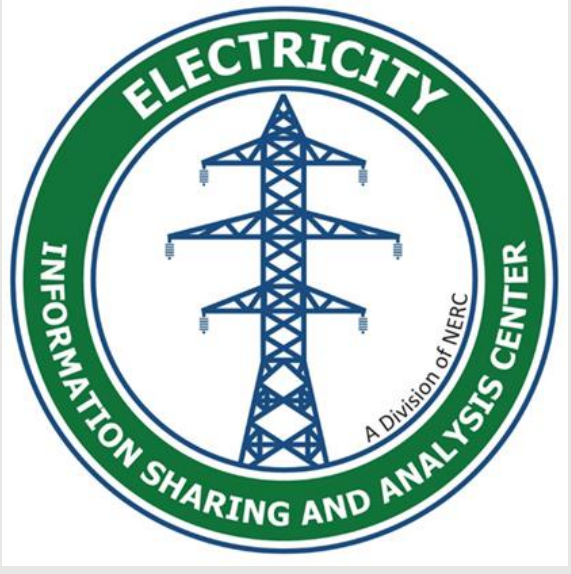
Frank Honkus



- Frank Honkus is the Director of the Cybersecurity Risk Information Sharing Program (CRISP) at the Electricity Information Sharing and Analysis Center (E-ISAC). He leads CRISP and supports the cybersecurity of energy sector through refinement of technical capabilities, reporting, and information sharing.
- Prior to joining the E-ISAC, Frank supported the Department of Energy's Office of Intelligence and Counterintelligence analyzing CRISP data for anomalous and malicious cyber activity.
- Frank was the red team lead and wrote the foundational mitigation and recovery sections for the Joint Base Architecture for Security Industrial Control Systems (J-BASICS) Joint Test, and supported the United States Cyber Command focusing on cyber threats to operations technology systems.
- Frank received his Masters in Public and International Affairs (MPIA) with a major in Security and Intelligence from the University of Pittsburgh's Graduate School of Public and International Affairs, and received a dual major in History and Political Science from the University of Pittsburgh.

About the Electricity Information Sharing and Analysis Center

- The E-ISAC was founded in 1999 and operates as a part of NERC
- The E-ISAC provides North American members a 24/7 Watch, expert in-house cyber and physical analysis, and a suite of analytical products and services, including CRISP



25 YEARS

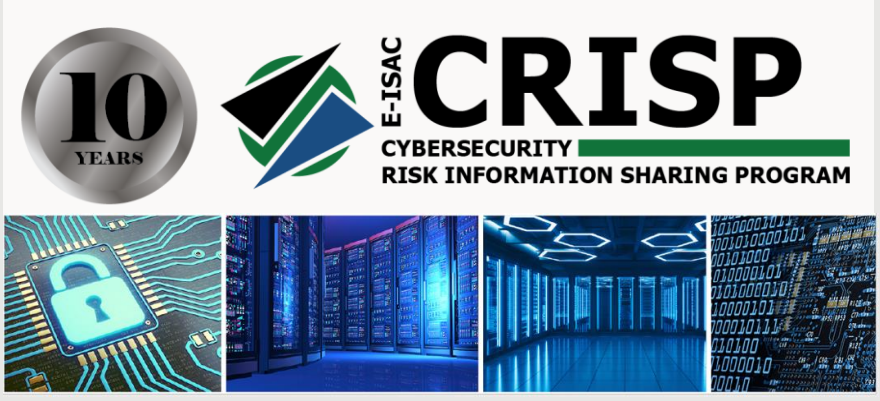
A DIVISION OF NERC

E-ISAC

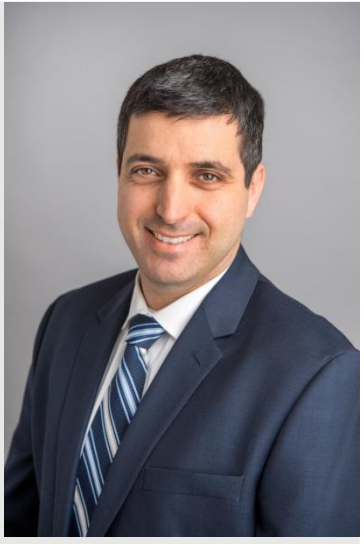
ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

About the Cybersecurity Risk Information Sharing Program

- CRISP was created as a pilot by the United States (US) Department of Energy, and was taken over by NERC in 2014
- CRISP provides near real-time network data sharing capabilities and cyber-threat analysis to US energy sector members



Mikhail Falkovich



- Mikhail Falkovich is the Chief Information Security Officer for Consolidated Edison Company of New York, Inc., one of the nation's largest investor-owned energy companies, providing electric, gas and steam service for New York City and Westchester County, New York.
- Mikhail currently leads several collaborative efforts between the government and utility sector partners to achieve industry wide security benefits and he is the recipient of the inaugural E-ISAC Electricity Security Service Award in Honor of Michael J. Assante.
- Mikhail is on the Board of the NYM InfraGard, and has received the Sector Chief of the Year award from the InfraGard National Members Alliance.
- Mikhail is a graduate of Cornell University where he received a bachelor's and a master's degree in Electrical Engineering and built a world champion team of soccer playing robots.

About Con Edison

- Founded in 1823 as the New York Gas Light company

- Provide electric, gas, and steam service for the 10 million people who live in New York City and Westchester County

Cyber Supply Chain Risk:
Vulnerabilities

- Vulnerabilities for both hardware and software, IT and OT
- Introduction of risk in deployment to both logical and physical locations
- Risk in procurement for contracts and consultants
- Product vs. Service Provider

Cyber Supply Chain Risk: Country-of-origin

- Country-of-origin risks
  - Standards of hardware and software development
  - Regulated vs unregulated
  - Local laws
  - Implications of real-time support

Cyber Supply Chain Risk:
Hypothetical Example

- Procurement and deployment of a given technology
  - Technology procured via contracted third party and deployed to electric power security and power operations centers
  - Contract terms and conditions where technology were to be manufactured in the country where the company resided
  - While the cases of the hardware stated product of *country X*, the internal hardware was manufactured in *country Y*
  - Network security detected outbound communications between deployed technology and *country Y* infrastructure

Cyber Supply Chain Risk:
Hypothetical Example continued

- What happened?
  - Very few companies produce the hardware for these products, and most of them reside in foreign *country Y*
    - These companies routinely sell their hardware to third parties who rebox the product with their label
  - Contractor was unaware the hardware inside the case was produced by company in foreign *country Y*
    - This is normal operating procedure to procure products with "made in *country X*" but the internal hardware made in *country Y*
  - Outbound network communications flagged and blocks put in place
    - *Country Y* has laws for mandatory surveillance and software is designed to adhere to that even if outside of *country Y*

Cyber Supply Chain Risk Management:
Risk Management Strategies

- Third Party Risk Management
  - Financial, Geopolitical, Cybersecurity
  - Internal vs. external assessments
  - ISO / SOC2 reviews
- Application of cybersecurity controls
  - Assess and tier the cybersecurity risk of the technology or service
  - Assess regulatory compliance concerns
  - Set thresholds for tiered controls
  - Consistent evaluation criteria based on risk tier
- Contractual terms and conditions

Cyber Supply Chain Risk Management: Industry Collaboration

- Partnerships with government
- Building trust circles
- Benchmarking
- Solving the problem at scale
  - Common language
  - Engagement with the industry and vendor community
  - Centralization
  - Scaling
- North American Transmission Forum (NATF) Effort
  - Maintenance and development of Risk Questionnaire
  - Forum for Suppliers and Industry to collaborate and mitigate risk

Cyber Supply Chain Risk Management: Mitigations

- All-of-company effort
- Service level agreements (SLAs) with consequences
- Architectural and process controls
- Active monitoring and response to vulnerabilities
- Terms and conditions
- Set expectations outside of the contractual language
- Continued assessments of current and alternative solutions

Publicly Available Resources

- National Institute of Standards and Technology (NIST): Best Practices in Cyber Supply Chain Risk Management
  - https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf
- Cisco and NIST: Managing Supply Chain Risk End-to-End
  - https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cyber-supply-chain-risk-management.pdf
- United States Department of Homeland Security: Cyber Security Procurement Language for Control Systems
  - https://www.cisa.gov/sites/default/files/2023-01/Procurement_Language_Rev4_100809_S508C.pdf'
- NATF Questionnaire and Criteria
  - https://www.natf.net/docs/natf/documents/resources/supply-chain/natf-supply-chain-security-criteria.xlsx
  - https://www.natf.net/docs/natf/documents/resources/supply-chain/energy-sector-supply-chain-risk-questionnaire.xlsx

Frank Honkus:
Frank.Honkus@eisac.com and/or
CRISP@eisac.com

Mikhail Falkovich