Cybersecurity for Infrastructure

The center for Buildings, infrastructure and public space

Fu foundation school of engineering and applied science Columbia university

COLUMBIA | ENGINEERING

The Fu Foundation School of Engineering and Applied Science

Shamir G. Pérez Sarraff

Lizzie Song

Dante Wu

Qiong Wu

Table of Contents

Reference: "December 2015 Ukraine power grid cyberattack." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 21 Mar. 2019. Web. 23 Apr. 2019.

Introduction

- Ukraine

December 23rd, 2015
The first known successful cyberattack on a power grid

December 17th, 2016
Industroyer: Biggest threat to Industrial Control Systems(ICS) since Stuxnet, Havex, BlackEnergy, and TRITON/TRISIS

June 27th, 2017
Banks, Ministries, Newspapers and Electricity firms.
France, Germany, Italy, Poland, Russia, United Kingdom, the United States and Australia.

Reference: https://searchsecurity.techtarget.com/definition/cybersecurity

Introduction

Cybersecurity is the protection of **Internet-connected systems**

CyberSecurity for Infrastructure

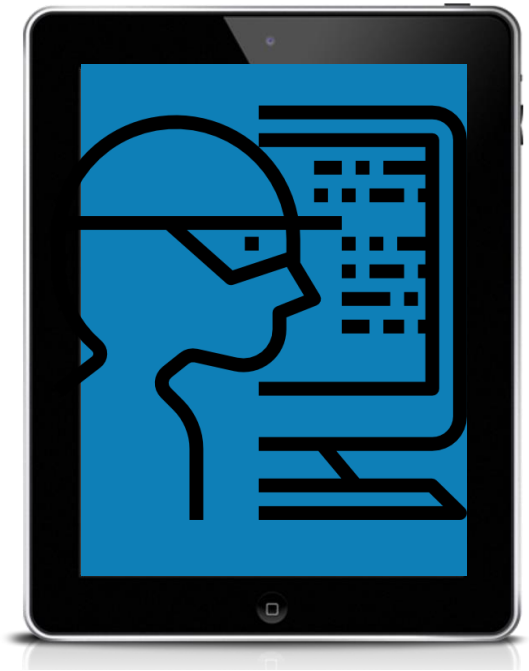
Intersection of:

Computer Science

Civil Engineering,

Criminology,

Environmental Engineering



Scope

Not only from **cyber-attack**,

But also **self-repair**.

Not only **defense**,

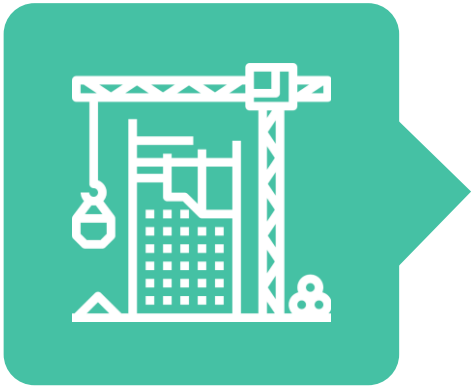
But also **updating and developing**.

Reference: Cybersecurity in the Construction Industry: Protecting Against a Growing Threat
https://www.jdsupra.com/legalnews/cybersecurity-in-the-construction-22150/

Risks in different phases: Design, Construction and Operation

Design

- Digital Documents
  - Security Information
- Malware & Data Breach
  - -Business Interruption
  - -Company Reputation
- Technology
  - -Productivity



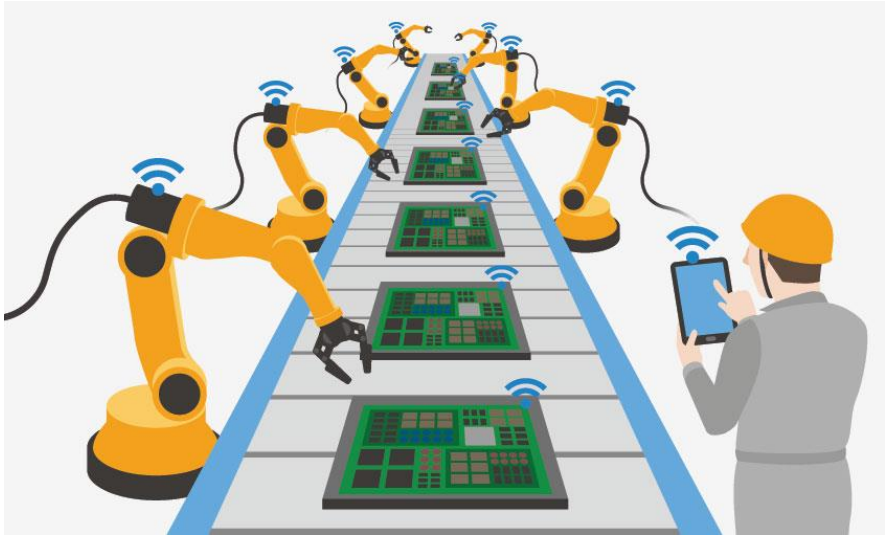
Construction

- Business
  - -Customer, contractor, and supplier lists and pricing
  - -Construction plans
  - -Competition
- Technology
  - -Property Damage
  - -Personnel Injury
- Security Information

Operation

- Personal Information
  - -Customer
  - -Employee
- Company Information
  - -Business plans and acquisition strategies

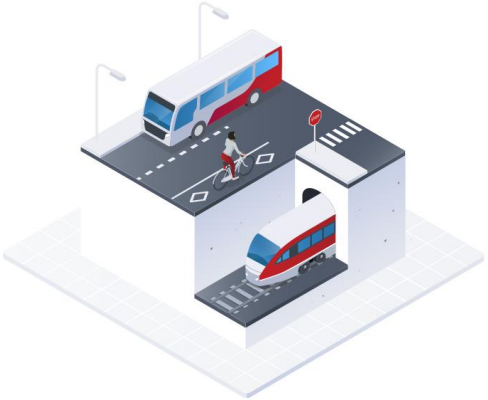
Risks in different sectors



Operational Technology (OT)

- supervisory control and data-acquisition systems (SCADA)
- industrial control systems (ICS)
- distributed control systems (DCS)
- industrial Internet of Things (IoT)

Risks in different sectors



Marine

- Computer control primarily
- Wide range of shipping community

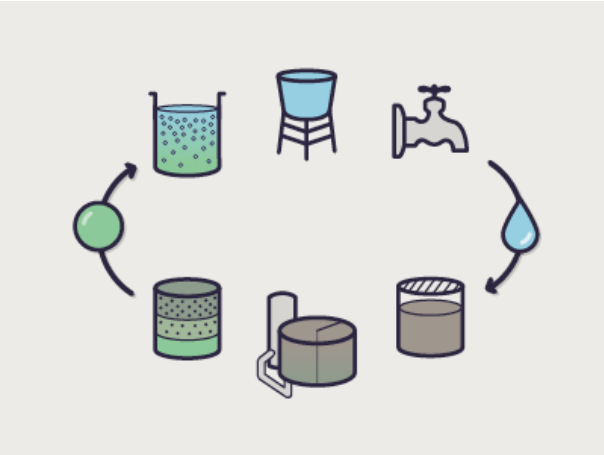
Transportation

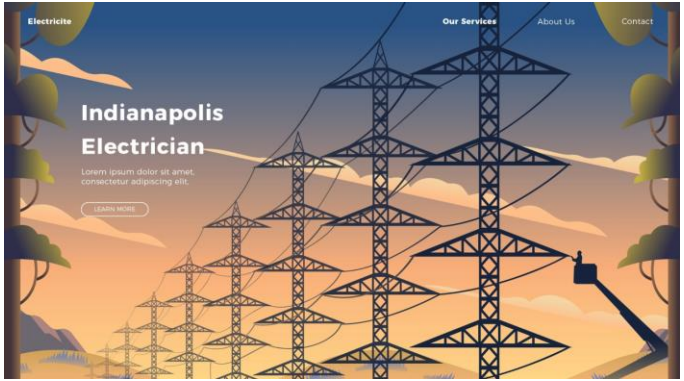
- Signal system
- Automotive computers

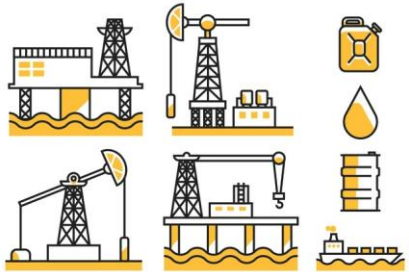
Aviation

- GPS
- Customer info

Risks in different sectors







Water

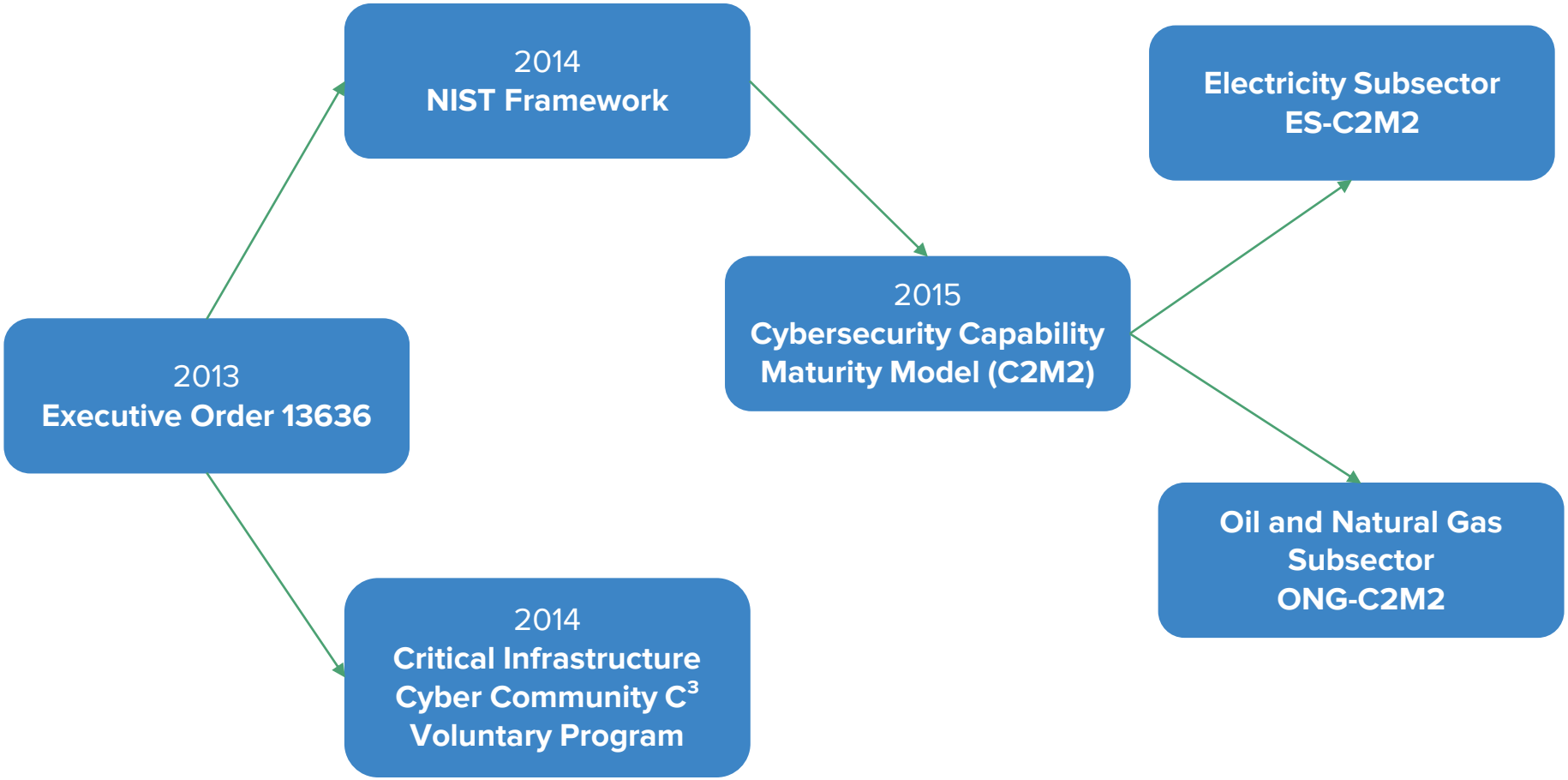
- Old SCADA system
- Lack awareness

Power Grid

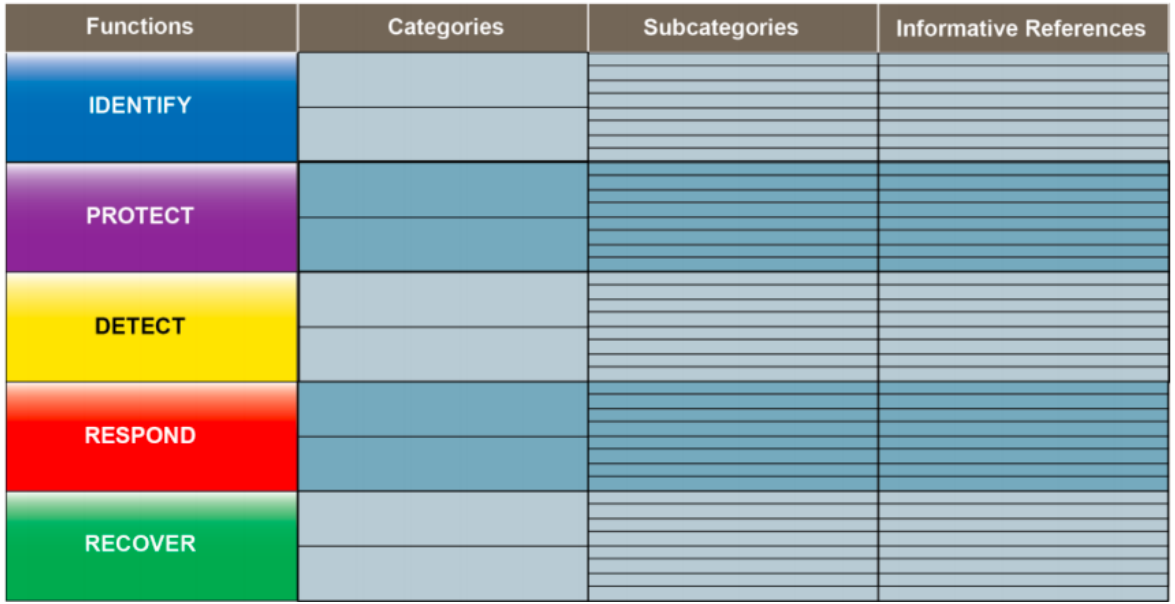
- IoT-based attack
- False power demand

Oil & Gas

- PPP model


2013
Executive Order 13636
2014
NIST Framework
2014
Critical Infrastructure Cyber Community C³ Voluntary Program
2015
Cybersecurity Capability Maturity Model (C2M2)
Electricity Subsector ES-C2M2
Oil and Natural Gas Subsector ONG-C2M2

NIST Framework



- **Framework Core**
  Functions, Categories, Subcategories, Informative References
- **Framework Implementation Tiers**
  Partial, Risk Informed, Repeatable, Adaptive
- **Framework Profile**
  Current and Target

https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

www.nist.gov/cyberframework

NIST

Search NIST | NIST MENU

CYBERSECURITY FRAMEWORK

Helping organizations to better understand and improve their management of cybersecurity risk

- Framework +
- New to Framework +
- Perspectives +
- Success Stories +
- Online Learning +
- Evolution +
- Frequently Asked Questions +
- Events and Presentations +
- Related Efforts (Roadmap)
- Informative References +
- Resources +
- Newsroom +

Credit: N. Hanacek/NIST

This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

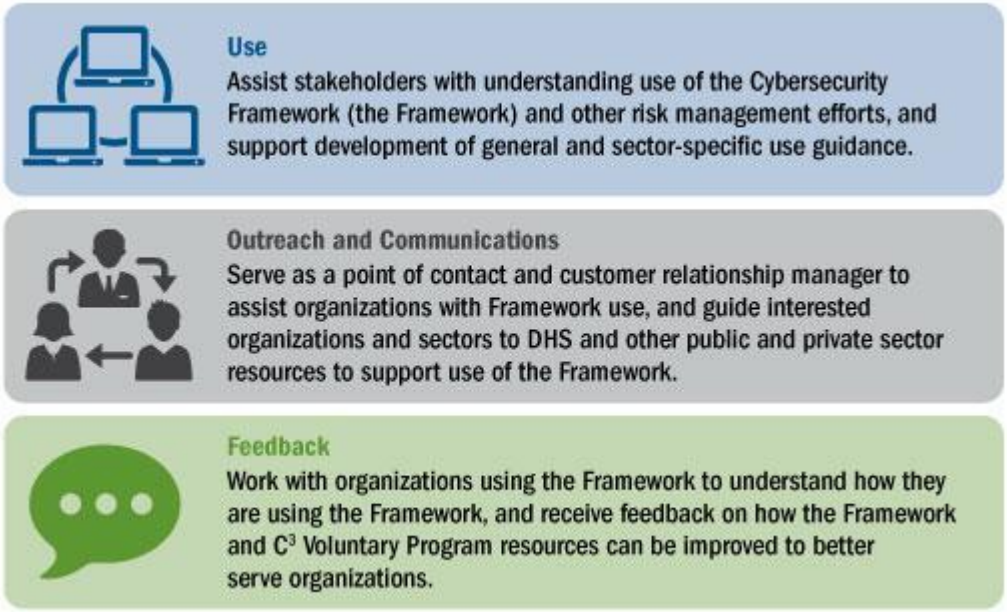
LATEST UPDATES

- Be sure to register for our upcoming "Next Up! Cybersecurity Framework Webcast: A Look Back, A Look Ahead" on April 26th.
- Version 1.1 of the Baldrige Cybersecurity Excellence Builder has just been released, check it out HERE!
- The NIST director's remarks on Cybersecurity and Privacy updates at RSA are now available

To see more Latest Updates click here

Training and Certificate

C³ Voluntary Program

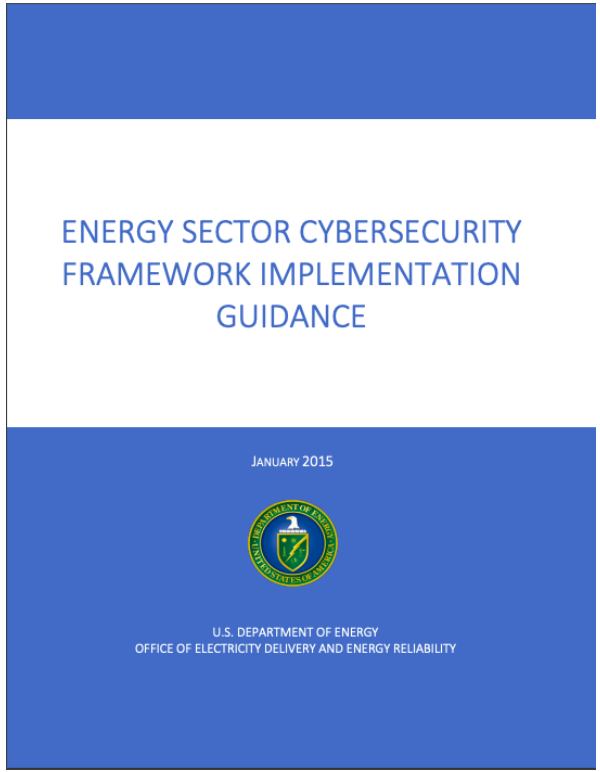


C³ Voluntary Program Engagement Channels

- Cyber Security Advisor (CSA) and Protective Security Advisor (PSA) programs
- The Critical Infrastructure Partnership Advisory Council (CIPAC) Framework
- Direct engagement between the C³ Voluntary Program and interested organizations

https://www.dhs.gov/ccubedvp

Cybersecurity Capability Maturity Model (C2M2)



- Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
- Public-Private Partnership
- evaluate, prioritize, and improve cybersecurity capabilities
- a maturity model, an evaluation tool, and DOE facilitated self-evaluations
- ES-C2M2 (electricity)and ONG-C2M2 (oil and natural gas)

https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

Security Challenges

Security Challenges

- **Overlooked Costs of Security in Digital Transformations**
  - Security is not often a central part of the transformation.
  - Security-as-afterthought approach increases the cost.
- **Protecting Operational Technology**
  - Firewalls are ineffective against attacks originating from within the network.
- **Industry Faces a Shortage in Cybersecurity Skills**

Solutions

1. **Integrate cybersecurity across OT and IT in earlier stage**
    a. integrated operation system
    b. integrated security center
2. **Identity and access management**
    a. firewalls to stop attackers
    b. device authorization
    c. network monitoring and anomaly detection

Solutions

3. **Third-party management**
    a. same standard
4. **Evolving cybersecurity regulations**
    a. national, rational, industrial
5. **Higher and smarter investment**
    a. benchmarks & emergency
6. **Greater industry-wide collaboration**