USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

DRAGOS

INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY

SAFEGUARDING CIVILIZATION

FORGING A CYBERSECURITY DEFENSE FOR UTILITIES

JASON D. CHRISTOPHER

INDUSTRIAL TECHNOLOGIES

Focused on processes that impact the real world, using industrial control systems (ICS) and operational technology (OT)

24 x 7 operations

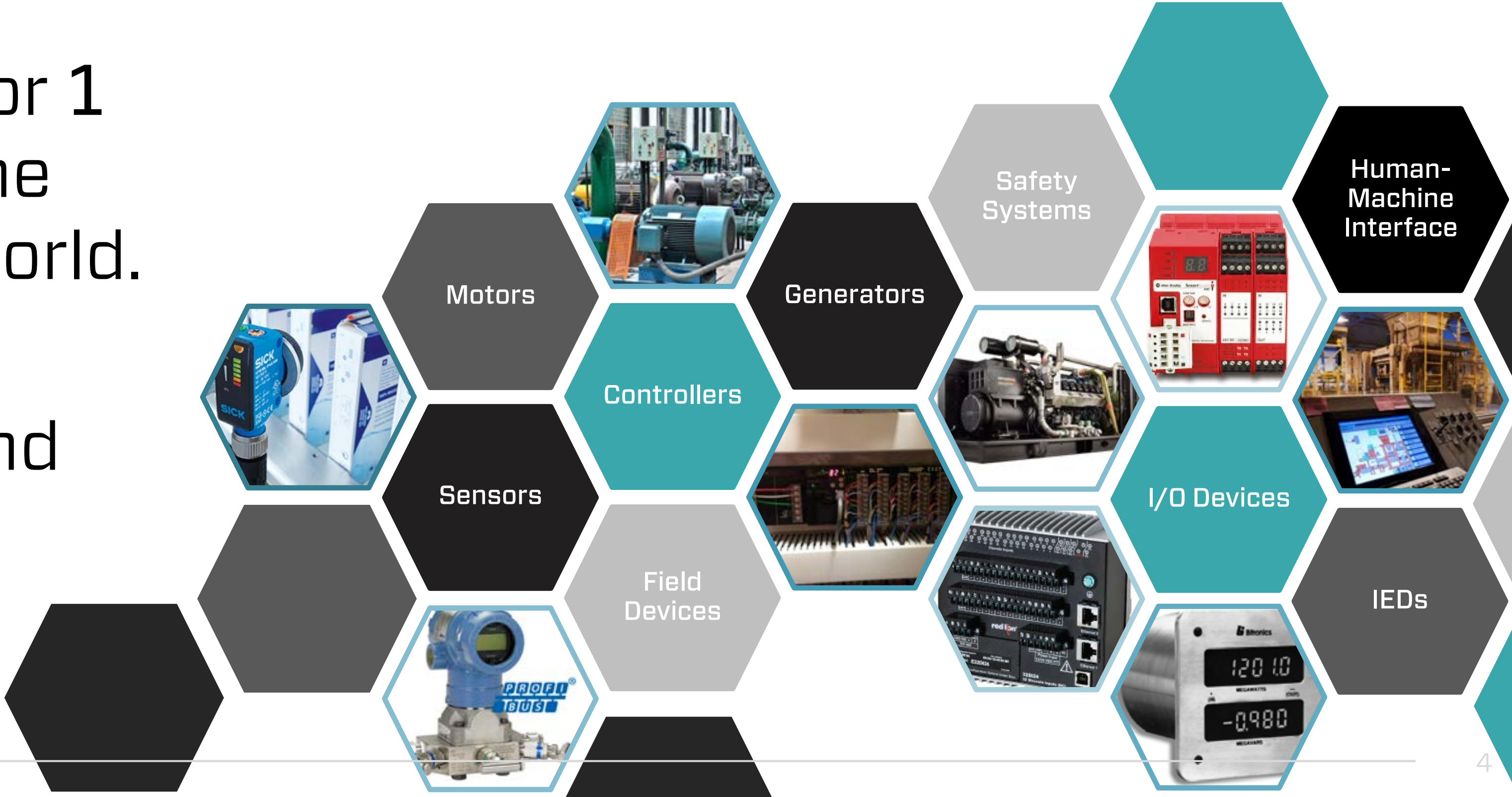
10-30 year lifecycle

16 critical infrastructure sectors

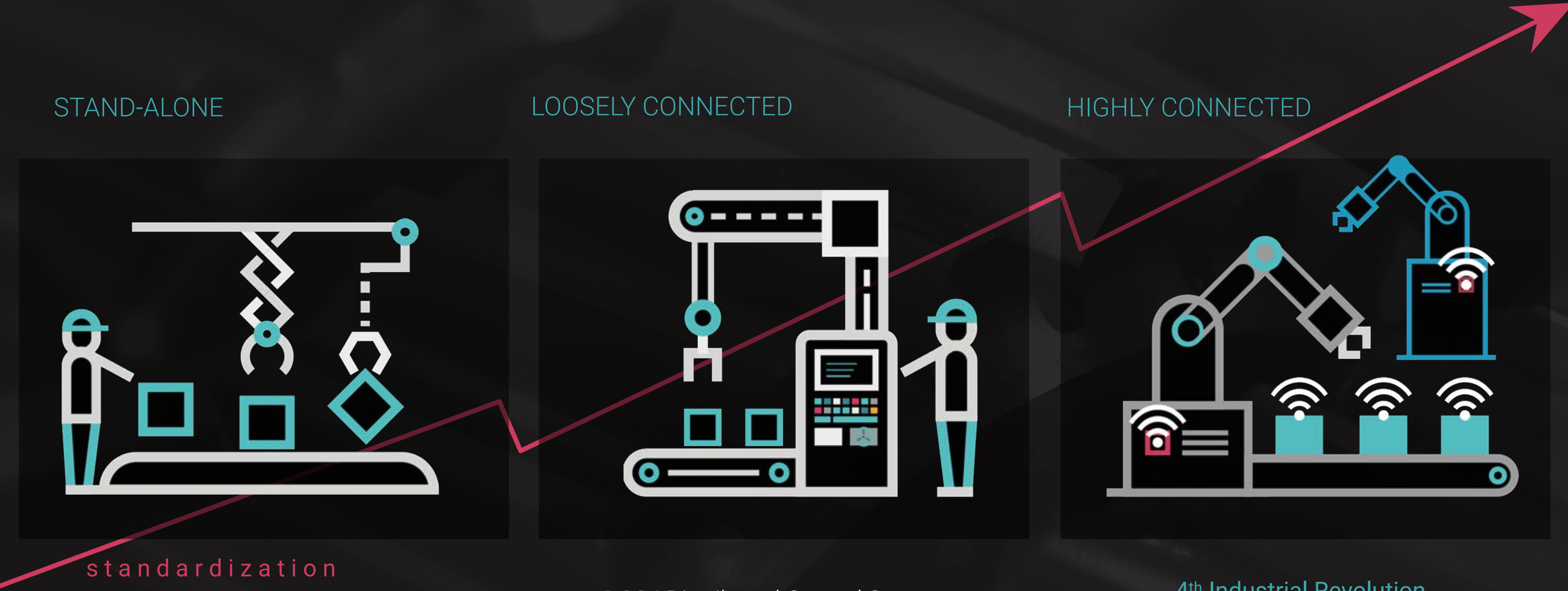
What are industrial control systems?

When a 0 or 1 impacts the physical world.

Devices and systems include:



Evolution of Operational Technology (OT)



STAND-ALONE

3rd Industrial Revolution
Automation of Production by Electronics

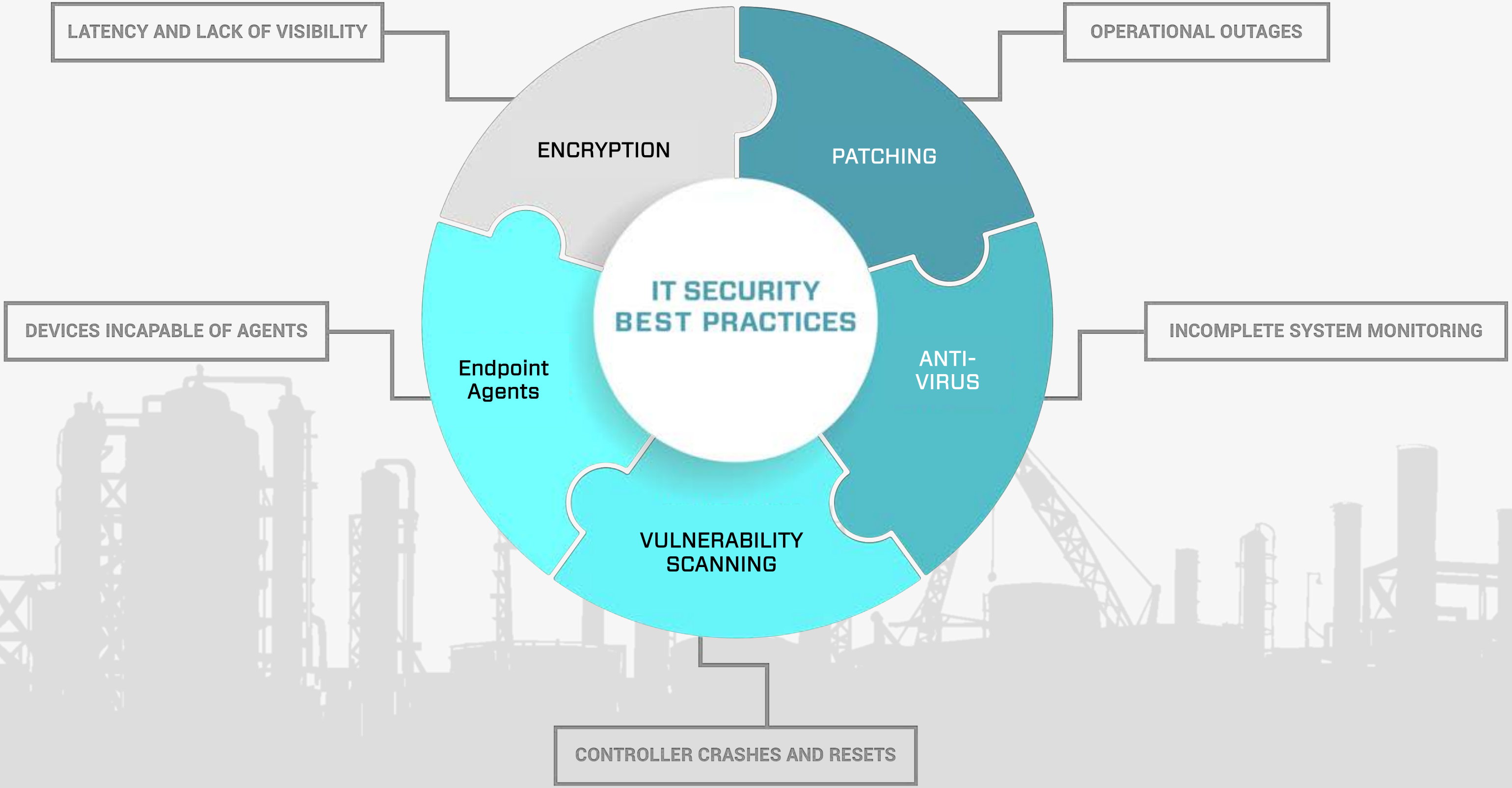
LOOSELY CONNECTED

DCS | Distributed Control System
SCADA | Supervisory Control & Data Acquisition

HIGHLY CONNECTED

4th Industrial Revolution
Smart Connected Systems
“Industry 4.0” // “Industrial IoT”

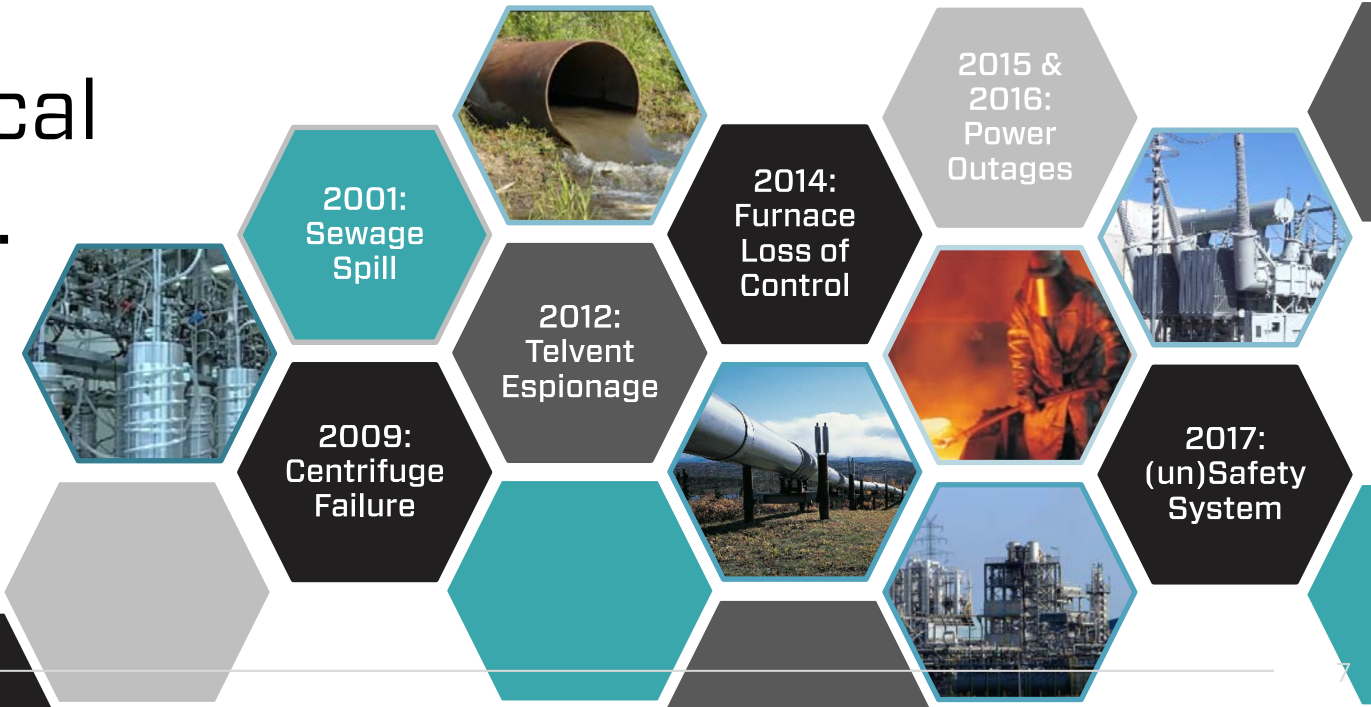
Traditional IT Security Issues in OT


LATENCY AND LACK OF VISIBILITY
OPERATIONAL OUTAGES
ENCRYPTION
PATCHING
IT SECURITY BEST PRACTICES
DEVICES INCAPABLE OF AGENTS
INCOMPLETE SYSTEM MONITORING
Endpoint Agents
ANTI-VIRUS
VULNERABILITY SCANNING
CONTROLLER CRASHES AND RESETS

Real-world cyber-based industrial-impacts

AGAIN

Think physical processes…



2001: Sewage Spill

2009: Centrifuge Failure

2012: Telvent Espionage

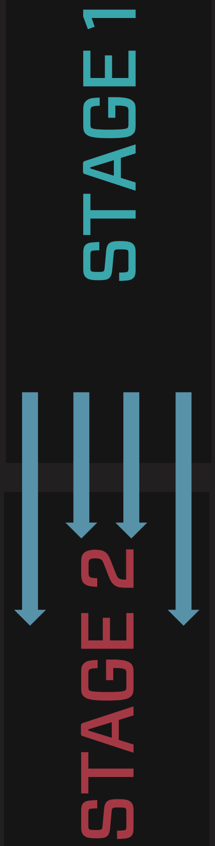
2014: Furnace Loss of Control

2015 & 2016: Power Outages

2017: (un)Safety System

INDUSTRIAL ATTACKS: IT and OT

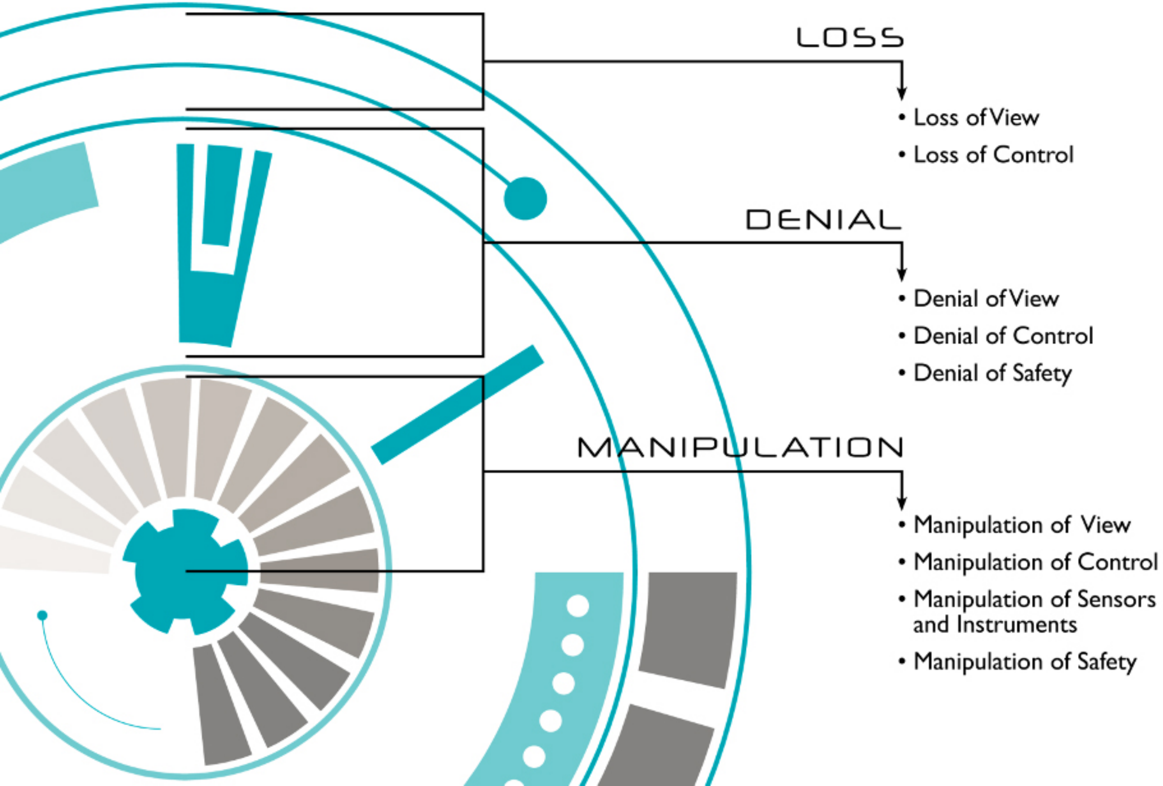
Corporate IT



Stage 1 and Stage 2 work together to impact industrial processes, stretching across both IT and OT networks

DRAGOS

Industrial Process Impacts



LOSS

- Loss of View
- Loss of Control

DENIAL

- Denial of View
- Denial of Control
- Denial of Safety

MANIPULATION

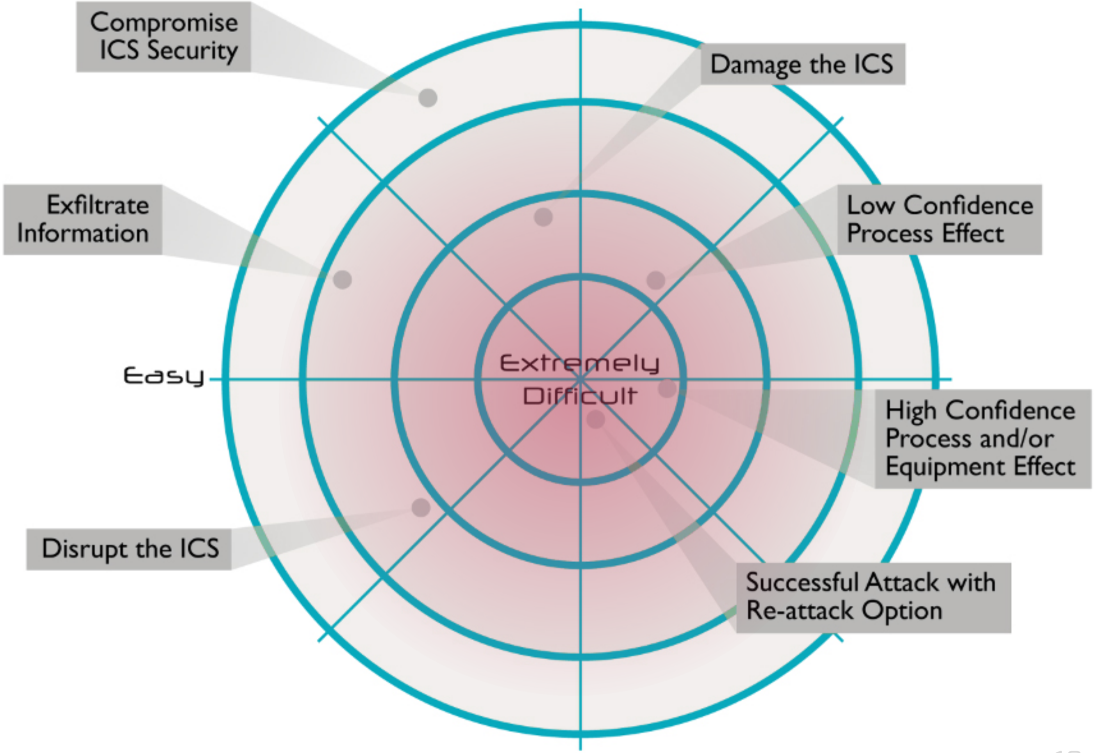
- Manipulation of View
- Manipulation of Control
- Manipulation of Sensors and Instruments
- Manipulation of Safety

For ICS-specific capabilities, the impact would be focused on *operational* impacts.

ICS Attack Difficulty

The knowledge involved in ICS attacks, with physical impact, includes:

- IT security
- OT security
- OT-specific protocols
- Engineering processes
- Incident response
- Disaster recovery



Compromise ICS Security
Damage the ICS
Exfiltrate Information
Low Confidence Process Effect
Easy
Extremely Difficult
High Confidence Process and/or Equipment Effect
Disrupt the ICS
Successful Attack with Re-attack Option

WannaCry

150+ countries

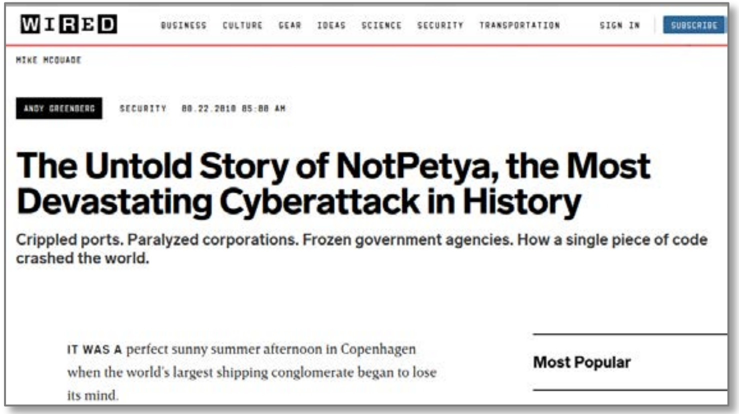
230+ companies

Animated map from New York Times, accessed 2020-03-30: https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

NotPetya…
Not Ransomware

"Wiper disguised as ransomware," with increased collateral damage beyond any initial targets.

+$10B	in estimated damages
2M	computers impacted in 2HRs
+65	countries involved in response


WIRED
BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY TRANSPORTATION SIGN IN SUBSCRIBE

MIKE MCQUADE

ANDY GREENBERG SECURITY 08.22.2018 05:00 AM

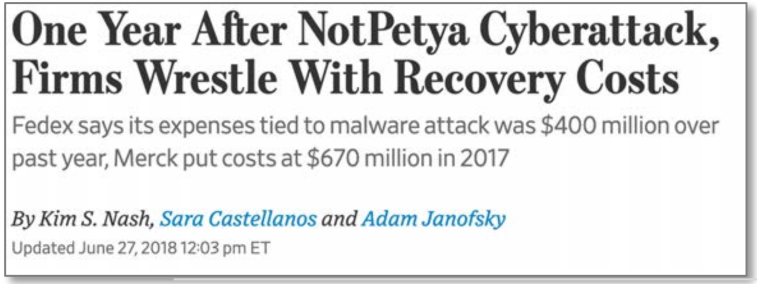
The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

IT WAS A perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind.

Most Popular

FedEx MAERSK MERCK Mondelēz International SAINT-GOBAIN Reckitt Benckiser



One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs

Fedex says its expenses tied to malware attack was $400 million over past year, Merck put costs at $670 million in 2017

By Kim S. Nash, Sara Castellanos and Adam Janofsky

Updated June 27, 2018 12:03 pm ET

The ICS Security Crucible

Very high temperatures

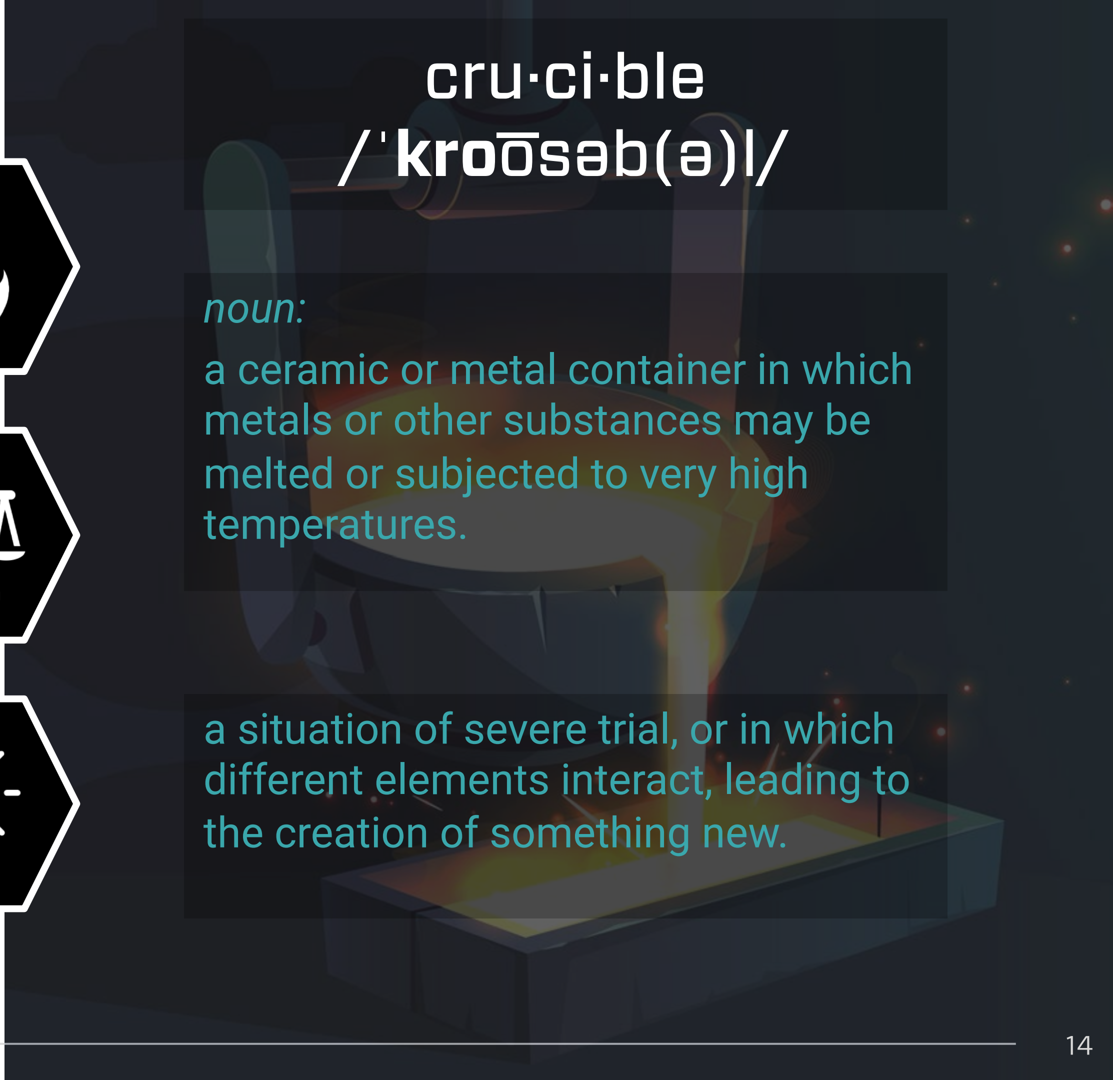
These programs need tons of energy to achieve success.

Situation of severe trial

Managing competing interests and resources across operations

Creating something new

A sustainable, business-oriented & goal-busting ICS security program



cru·ci·ble

/ˈkro͞osəb(ə)l/

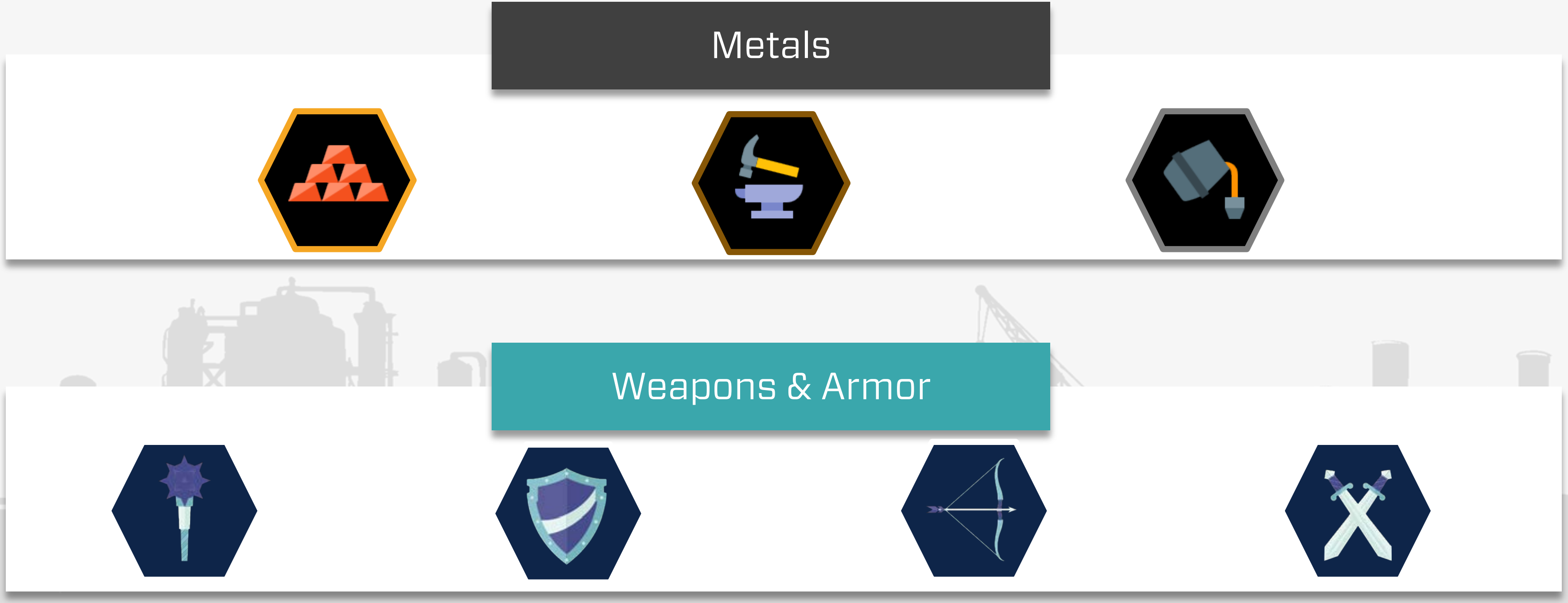
noun:

a ceramic or metal container in which metals or other substances may be melted or subjected to very high temperatures.

a situation of severe trial, or in which different elements interact, leading to the creation of something new.

DRAGOS

Forging an ICS Security Program



Metals

Weapons & Armor

starting with BRONZE

- Initial defenses may be resource-constrained
- No documentation, no lessons learned
- Loss of “lotto winners” could cripple the program

strengthen using IRON

- Moving beyond ”oral history” to written law
- Partnered with multiple stakeholders
- Resources are less scarce

further refine with STEEL

- People are trained, ready, and exercised
- Executives are active participants in ICS security
- Capabilities are “double-checked” and reviewed

THE CYBER ARSENAL

Assess criticality

Link ICS security to critical processes, systems, and devices

Segments & Zones

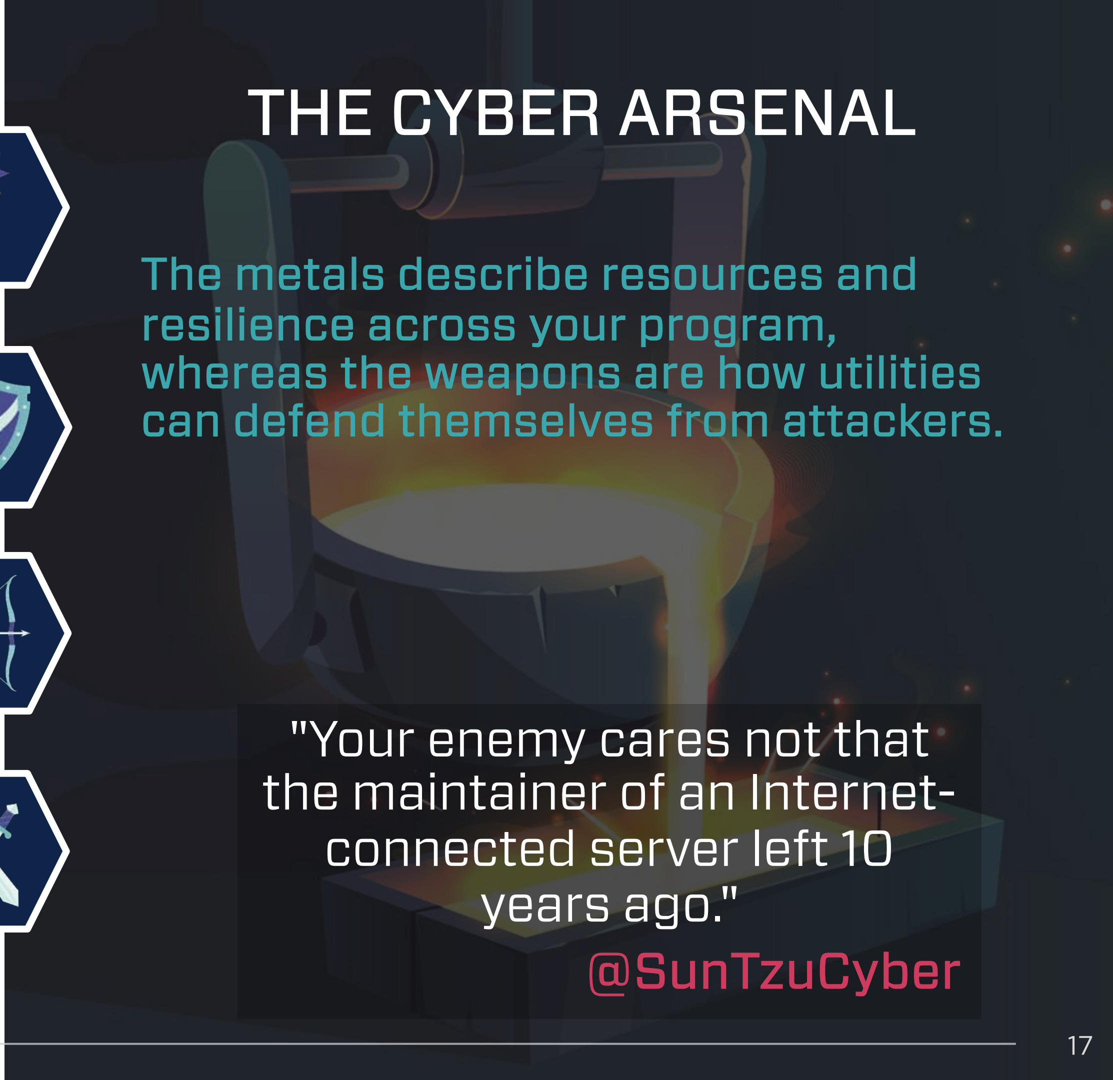
Invest in strong perimeters around the crown jewels

Hunt evil...

Log and monitor across both IT & OT environments

Incident Response

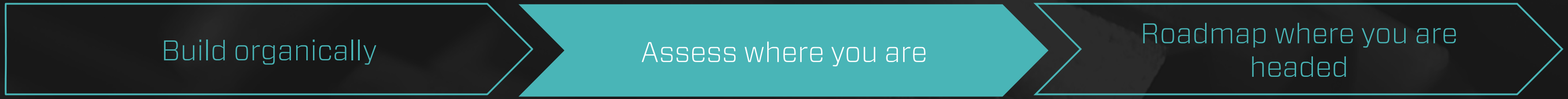
Build and train incident response and recovery teams



The metals describe resources and resilience across your program, whereas the weapons are how utilities can defend themselves from attackers.

"Your enemy cares not that the maintainer of an Internet-connected server left 10 years ago."
@SunTzuCyber

What metal is right for your program?



Build organically

- Do you have a champion?
- Can you scale a team?
- Can you *effectively* use your tools?

Assess where you are

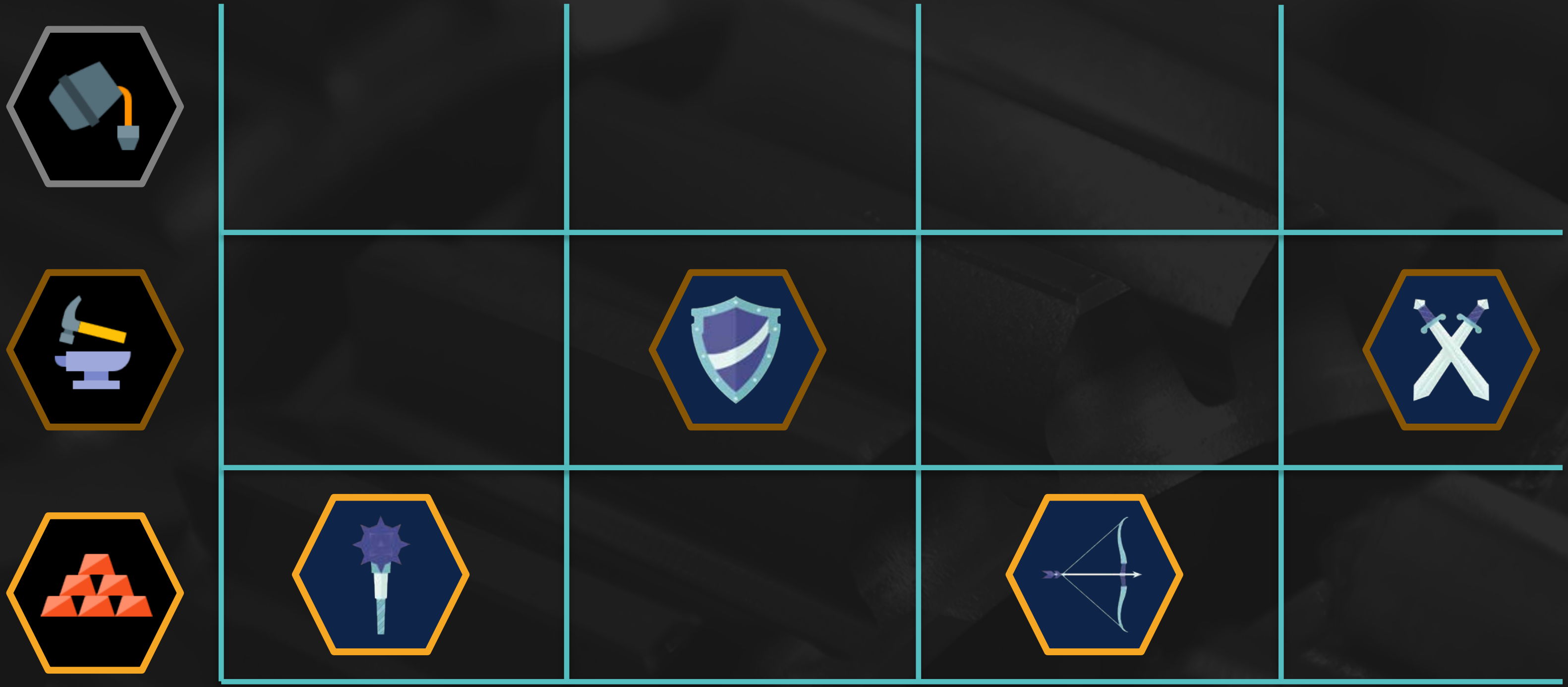
- Be honest. Brutally so.
- Think about processes, people, and technology
- Include discussions about things like "the lotto winner" or executive engagement.

Roadmap where you are headed

- Map back to criticality and impacts.
- Talk in terms of business risk.
- Roadmaps help address current gaps and build budgets.

What metal is right for your program?

What metal is right for your program?



What metal is right for your program?

What standard is right for your program?

IDENTIFY

PROTECT

DETECT

RESPOND
RECOVER

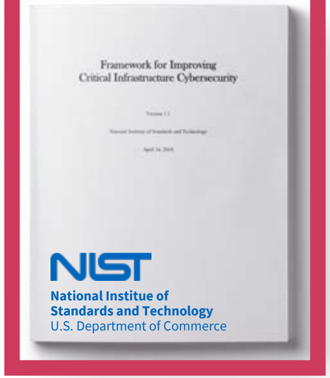
HOW...?

WE USED A MATURITY MODEL

The ICS Security Crucible is applying standards & maturity models across business units, with executive support.

...so how do we get there?

And start with literally *any* standard



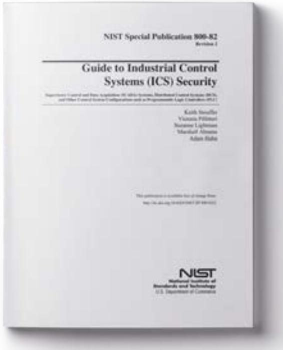
Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

National Institue of
Standards and Technology
U.S. Department of Commerce



NIST Special Publication 800-82
Revision 2

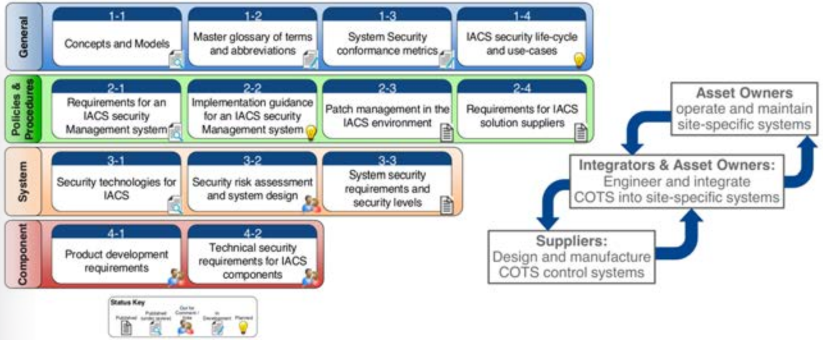
Guide to Industrial Control
Systems (ICS) Security

Keith Stouffer
Victoria Pillitteri
Suzanne Lightman
Marshall Abrams
Adam Hahn

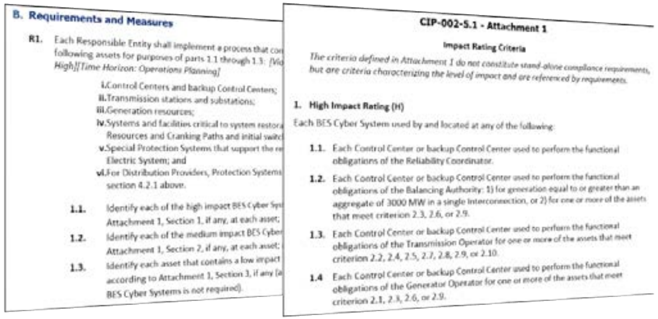
National Institute of
Standards and Technology
U.S. Department of Commerce

CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

Version 1.1
February 2014



General
1-1 Concepts and Models
1-2 Master glossary of terms and abbreviations
1-3 System Security conformance metrics
1-4 IACS security life-cycle and use-cases
Policies & Procedures
2-1 Requirements for an IACS security Management system
2-2 Implementation guidance for an IACS security Management system
2-3 Patch management in the IACS environment
2-4 Requirements for IACS solution suppliers
System
3-1 Security technologies for IACS
3-2 Security risk assessment and system design
3-3 System security requirements and security levels
Component
4-1 Product development requirements
4-2 Technical security requirements for IACS components
Status Key
Published
Published (under review)
Out for Comment / Vote
In Development
Planned
Asset Owners operate and maintain site-specific systems
Integrators & Asset Owners: Engineer and integrate COTS into site-specific systems
Suppliers: Design and manufacture COTS control systems



B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that con
following assets for purposes of parts 1.1 through 1.3: [Vio
High][Time Horizon: Operations Planning]

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restora
Resources and Cranking Paths and initial switc
v. Special Protection Systems that support the re
Electric System; and
vi. For Distribution Providers, Protection Systems
section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Sys
Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber
Attachment 1, Section 2, if any, at each asset;

1.3. Identify each asset that contains a low impact
according to Attachment 1, Section 3, if any (a
BES Cyber Systems is not required).

CIP-002-5.1 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

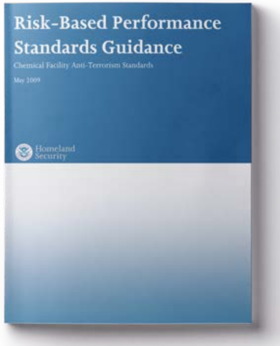
1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

NEI 08-09 [Rev. 6]

Cyber Security Plan for
Nuclear Power Reactors

April 2010



Risk-Based Performance
Standards Guidance

Chemical Facility Anti-Terrorism Standards

May 2009

Homeland
Security

industrial internet
CONSORTIUM

www.iiconsortium.org

Industrial Internet of Things
Volume G4: Security Framework

IIC:PUB:G4:V1.0:PB:20160926

AWESOME.

SO WE CAN USE THE RIGHT TOOLS

Find (or be) a champion

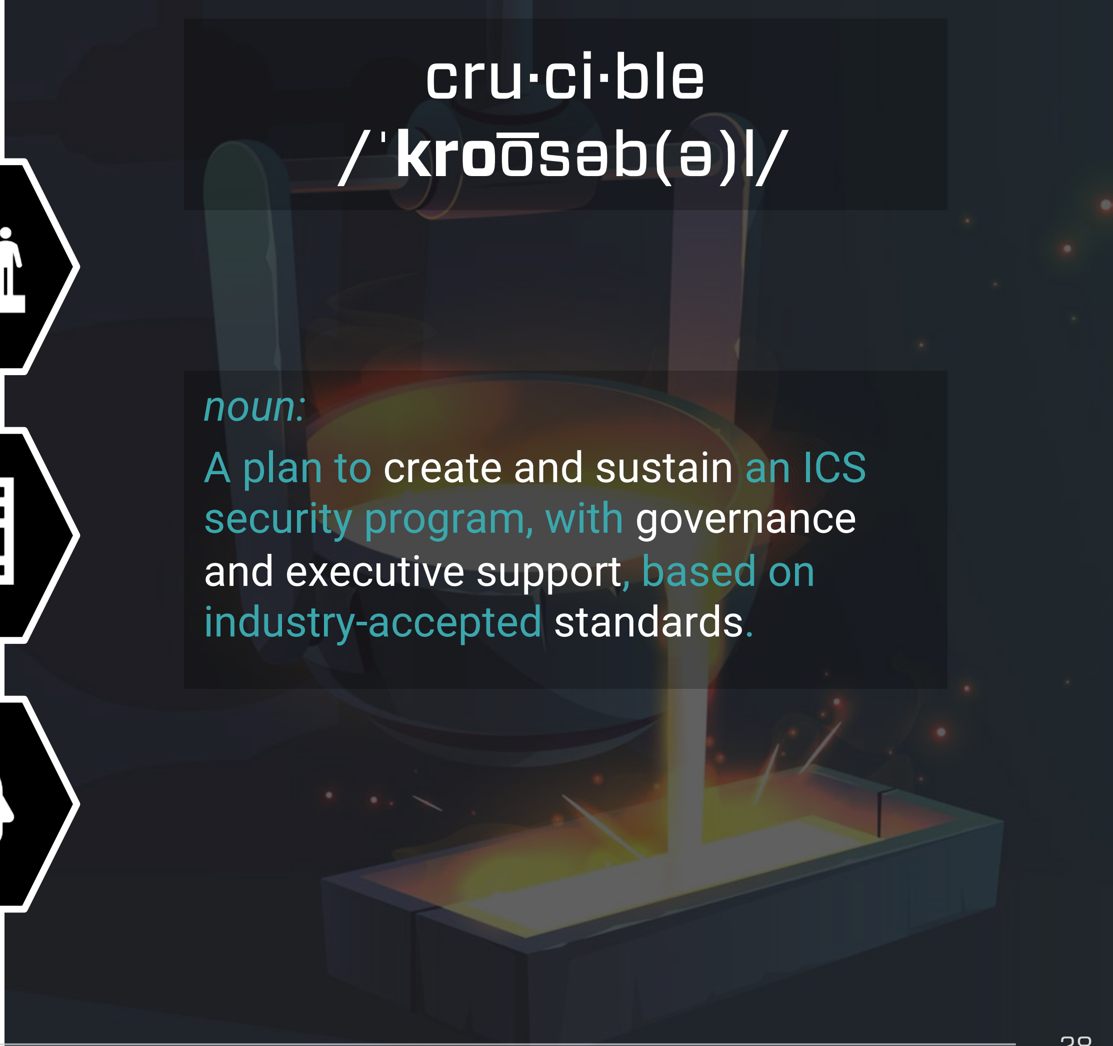
Management, IT, OT, legal, HR– you are not alone.

Roadmap the destination

Make an honest evaluation of where you are & where you are headed

Adopt ICS standards

ICS security needs to be "how we do business," not "that weird thing over in the corner."



cru·ci·ble

/ˈkro͞osəb(ə)l/

noun:

A plan to create and sustain an ICS security program, with governance and executive support, based on industry-accepted standards.

PREVENTION IS IDEAL.
DETECTION IS A MUST.*

*detection without response, however, is of little value

Dragos’ Year in Review provides insights and lessons learned from our team’s first-hand experience hunting, combatting, and responding to ICS adversaries throughout the year.

DRAGOS

2019 YEAR IN REVIEW

ICS VULNERABILITIES

ICS VULNERABILITIES REPORT

Provides an analysis of ICS-specific vulnerabilities and discusses impacts, risks, and mitigation options for defenders

DRAGOS

2019 YEAR IN REVIEW

THE ICS LANDSCAPE AND THREAT ACTIVITY GROUPS

ICS THREAT LANDSCAPE REPORT

Provides insights on the state of ICS cybersecurity, the latest trends and observations of ICS-specific adversaries, and proactive defensive recommendations.

DRAGOS

2019 YEAR IN REVIEW

LESSONS LEARNED FROM THE FRONT LINES OF ICS CYBERSECURITY

LESSONS LEARNED FROM THE FRONT LINES REPORT

Provides a synopsis of trends observed within the industry and lessons learned from Dragos’ proactive and responsive service engagements

THANK YOU

@jdchristopher

linkedin.com/in/jdchristopher