Portland State
Hatfield School of Government

Cybersecurity Community Development

NSA Grant Initiative 2021-8 option 3

Multi-State Critical Infrastructure Coalition

- Mark O. Hatfield Cybersecurity & Cyber Defense Policy Center
  - *Professor Birol A. Yeşilada, P.I. & Center Director*
  - *Professor Barbara Endicott-Popovsky, Co-P.I. & Center Associate Director*
  - *Professor Tuğrul Daim, Co-P.I. & Center Associate Director*
  - *Ran Hinrichs, Project Director for Tabletop Exercises*

(National Center Of Academic Excellence in Cybersecurity Research)

September 2023

Project Overview

- FUNDING 2-year $2M 6-States Distributed Teams
- OBJECTIVE, Scope, Stakeholders
  - Establish a cybersecurity critical infrastructure community
  - In the extended Pacific Northwest (WA, ID, OR, MT, HI, CO)
  - With the Electric Grid, 1st Responders, Legislators, Funding Agencies
- RISKS
  - Insufficient Funding, talent shortage, compliance
  - Coordination across all six states (priorities / challenges)
  - Evolving Threat Landscape, technology challenges
- MITIGATIONS
  - Top Cybersecurity Experts perform 2-year pilot

Focal Groups

Deliverables,
Success
Metrics

Policy
&
Funding
Recommendations

Cyber Security
Framework

Tabletops

Technology
Roadmaps

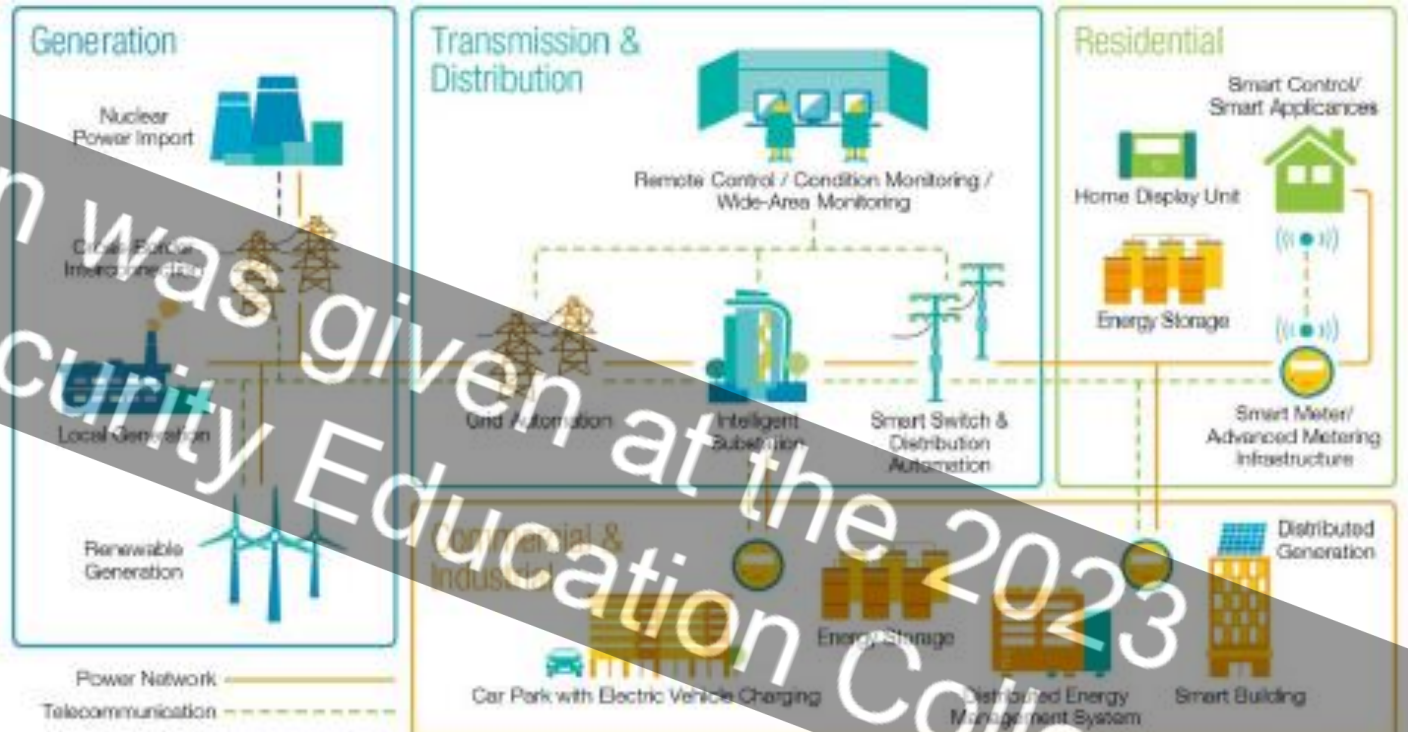
Influence
Analysis

Portland State
Hatfield School of Government

Tasks

- Identify key consultants to focus and lead efforts
  - Inventory assets
  - Profile business environment
  - Examine governance structure
  - Review procedures and strategies
- Evaluate protection capability through **Tabletops**
  - Evaluate Incident Response Plans
  - Size Training and Education Programs
  - Test data security, information protection, maintenance
- Detect capabilities through **Technology Roadmaps**
  - Seeing the unseen, anticipating future events
  - Leveraging AI, zero-trust, quantum, IoT swarm, globalism
- Analyze stakeholders' ability to respond
  - Relevancy, position, influence, salience

OVERVIEW OF FUTURE SMART GRID TECHNOLOGIES ACROSS THE POWER SYSTEM



Key Recommendations

Promote involvement of power authorities.
Enhance academic-industry-government partnerships across regions
Increase tailored tabletop exercises.
Address critical infrastructure vulnerabilities with technology roadmap
Engage emergency management, first responders and the State and National Guard
Innovate and escalate education for the workforce using cooperative learning models
Use successful state models as examples
Practice continuous Improvement.

Tabletops

Simulation activity of a hypothetical cyberattack

Roles, objectives, tool, scenario

Plan

Conduct

Examine understanding, protocols, critical thinking through injects

Evaluate

SWOT: Strengths, Weakness, Opportunities, Threats

Report

Data, Feedback, Insights

Follow-up

Address Governance, Tools Investment

TIMELINE
TABLETOPS (TTX)

Planning
- Dr. Endicott-Popovsky formed Pacific NW Collaboratory
- Hawaii delivered lessons learned and set standards
- Four tabletops chosen, MT, CO, ID, WA

Tabletop Montana
- Governor engagement with head of National Guard, University of Montana.
- Participants: 20 of the 26 electric distribution cooperatives
- NUARI Decide Platform was 60+ participants

Collaboratory
- Every three months over Zoom with state reporting.
- NSA Data Sensitivity, NUARI Decide Platform, CyberEd
- Booz Allen President of Security, First Responders

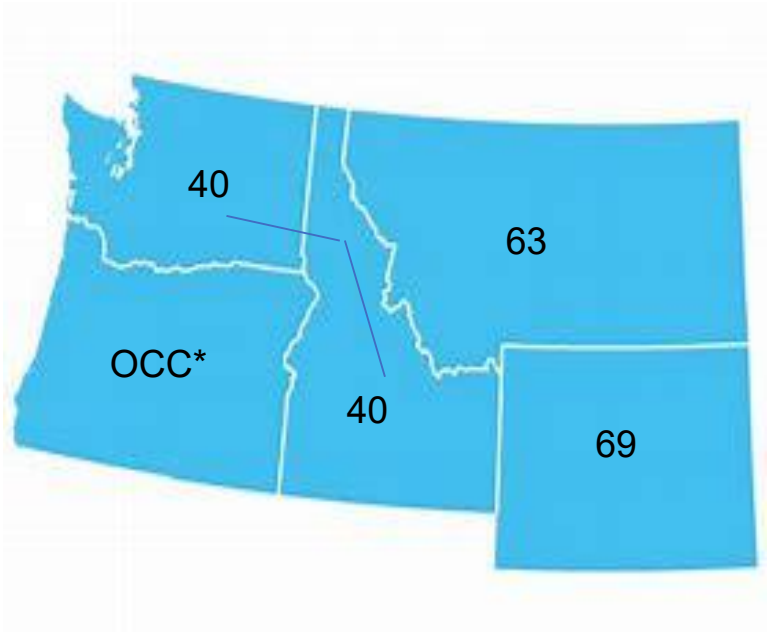
Tabletops
- WA/ID – Interstate and Intrastate EMT and P-SAPS WSU
- CO – Electric Grid Profile, University Colorado, Colorado Springs
- Colorado River Basin in contrast to Bonneville Power Authority.

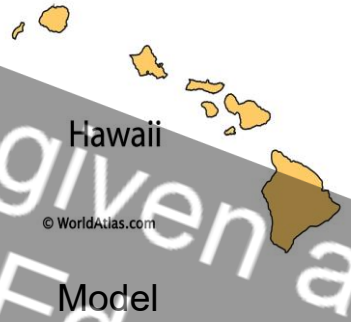
Results
- Quantified key stakeholders
- Scope of the microgrid, gaps and vulnerabilities
- Policy, investment, regional planning

Year 2 | Feb | April | Workshops | July | August

Tabletops Findings

- Each state is different
- First responders need included
- Analog and Digital tabletops required
- All state tabletops effective
- All regional tabletops needed
- Readiness is strong, awareness is limited
- Deeper relationships with BPA and WAPA needed
- Leverage existing models (HI)

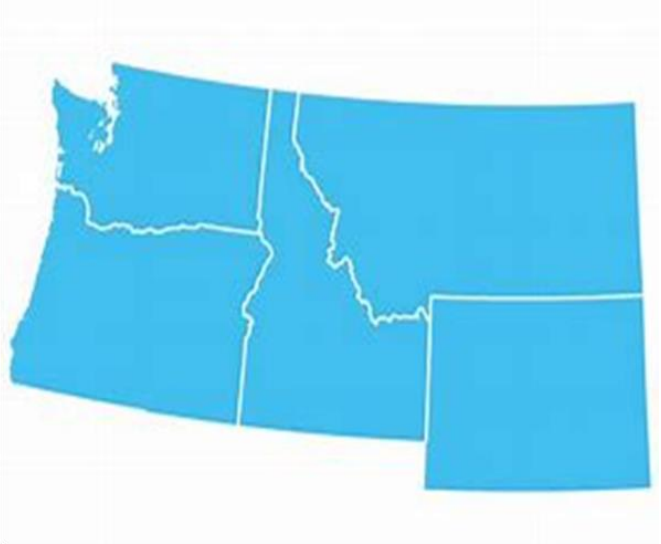




Model

*OCC_ Oregon Cybersecurity Center

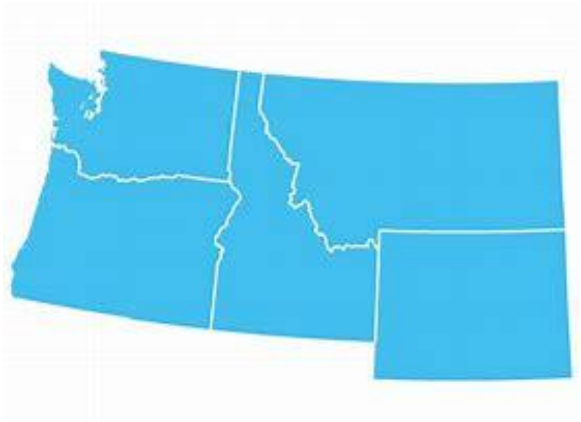
Tabletops Recommendations



- Promote Involvement of power authorities
- Enhance partnerships across regions
- Prioritize and address critical infrastructure vulnerabilities immediately
- Engage EMT, FR, and National Guard from outset
- Develop resiliency and cooperative learning in the workforce
- Tailor tabletops for each state and run again
- Leverage the Pacific Northwest Collaboratory

Data Sensitivity

Heightened Awareness and Training



Rationale

- Unprecedented insight into vulnerability
- Creates increased adversarial exploitation
- Identifies strategic significant

Action Plan

- Review classification framework
- Tailor security protocols:
  advanced encryption, restricted access control, AI enhanced monitoring
- Educate the stakeholders

Exercise Framework

Planning Timeline Milestones

	Intro	Kick Off	C&O	IPM 1 and IPM 2	MPM	MSEL Sync	FPM	EX and AAR
Simple complexity	Introductory Call	EX – 16 weeks	EX – 12 weeks	EX – 8 to 11 weeks	EX – 7 weeks	EX – 4 weeks	EX - 2 weeks	EXercise Date
Med complexity	Introductory Call	EX – 25 weeks	EX – 20 weeks	EX – 18 to 14 weeks	EX – 12 weeks	EX – 8 weeks	EX - 3 weeks	EXercise Date
High complexity	Introductory Call	EX – 60 weeks	EX – 56 weeks	EX – 52 to 36 weeks	EX – 24 weeks	EX – 10 weeks	EX - 4 weeks	EXercise Date

Introductory Call
- Introductions
- Program Background
- Commit to an Exercise
- Initial Design Document (IDD) review

Concepts and Objectives
- Exercise concept
- Exercise objectives identified
- Identification of planning team members
- Planning timeline, milestones, and meeting dates

Mid Planning Meeting
- Well-developed scenario and event list to include injects
- Roster development
- Guidelines and Concerns
- Identify/Draft exercise documentation
- Exercise logistics

Final Planning Meeting
- Initial review in DECIDE
- Exercise Evaluation Review
- Final document/material approval
- Identified issues resolved
- Task assignments and logistical elements confirmed
- Exercise and training day invites

Initial Call (Intro) → Kick Off → C&O → IPM 1 → IPM 2 → MPM → MSEL → FPM → Exercise & AAR

Kick Off
- Introduce Planning Team
- Review the IDD
- Assess scope of exercise
- Discovery questions

Touchpoint meetings will be held between these milestone meetings at agreed upon intervals to support overall planning progression.

Initial Planning Meeting 1 –Exercise Overview
- Clearly defined objectives and aligned capabilities
- Initial capability targets and critical tasks
- Exercise Evaluation
- List of participating organizations and extent of play
- Identification and availability of all source documents
- Refined exercise planning timeline

Initial Planning Meeting 2 – Transition to Planning
- Scenario variables (threat, scope, venue, conditions)
- Exercise structure and schedule
- Exercise staffing/ Identification of subject-matter experts
- Exercise logistics

MSEL Sync Meeting
- Key event injects and delivery timeline identified
- Exercise Staffing Plan
- Revisions of draft scenario-based documentation
- Exercise Evaluation Targets
- Timeline for completion

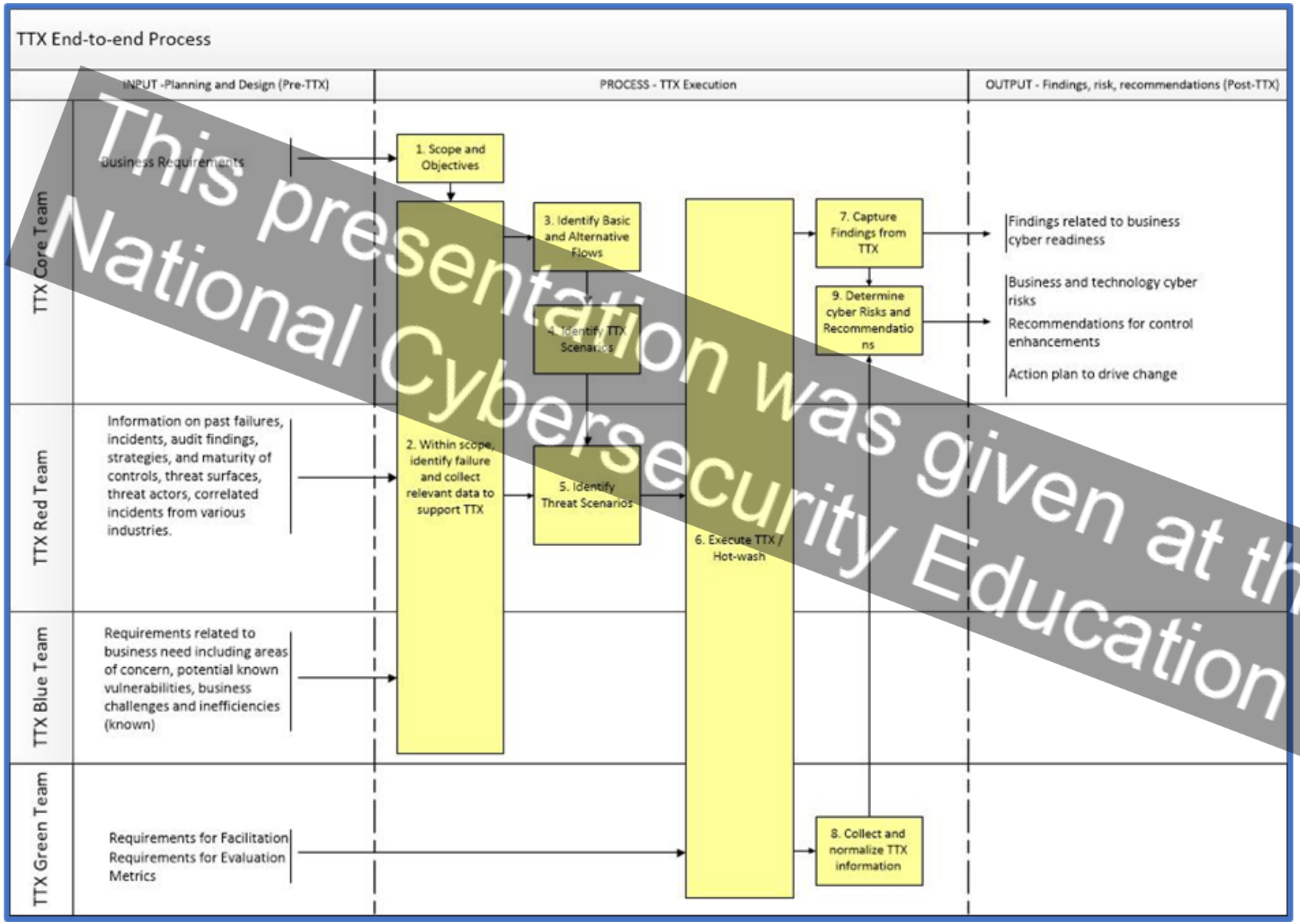
Exercise
- Conduct exercise according to plan using DECIDE®
- Hotwash

After Action Review and Report
- Draft review 1 week post exercise
- Final review approx. 3 weeks post exercise

DECIDE PLATFORM

Portland State
Hatfield School of Government

Portland State
Hatfield School of Government



Analog

Intuitus

Tabletop versus Roadmap

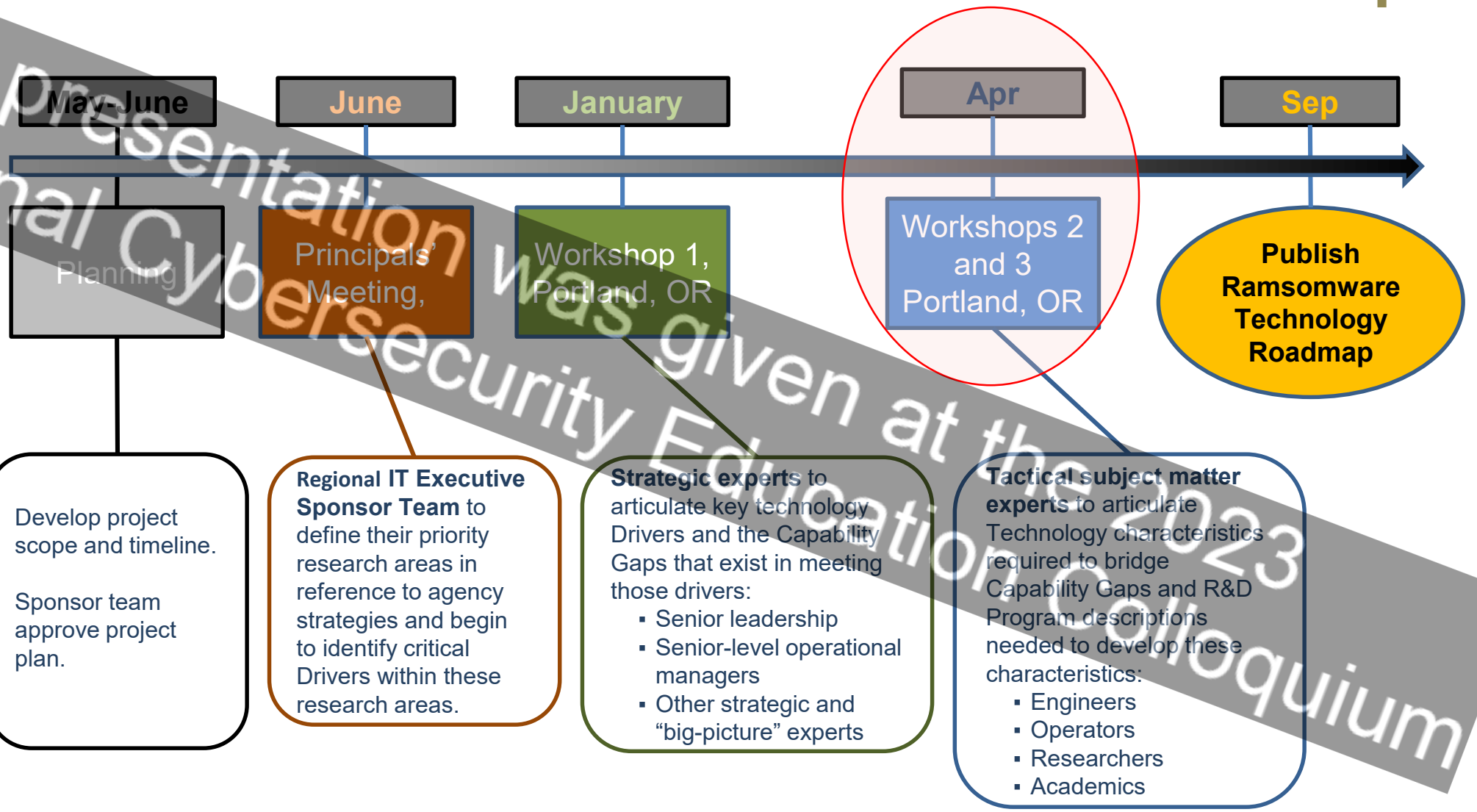
Tabletop	Technology Roadmap
Run by cybersecurity experts	Run by technology roadmap experts
Simulated exercise to evaluate response	Planning methods to coordinate technological investments
Uses hypothetical cyber-attack scenarios	Uses literature review, process analysis exercises with experts in the field
Operational focus on protection, detection and response	Strategic technology management perspective
Game scenarios for action response	Analytical evaluation of tool sets
Conducted on site with stakeholders	Conducted over Zoom with IT and OT

Pacific Northwest Power Grid Ransomware Readiness Technology Roadmap

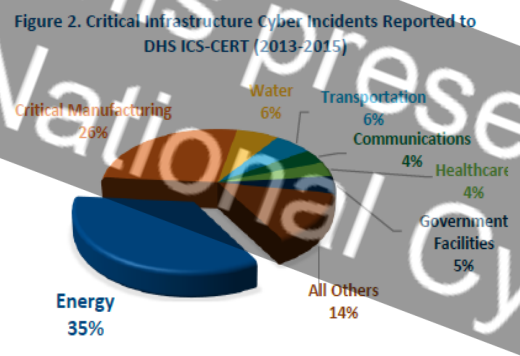
Workshop 2:
Technology and
Research and Development

April 18, 2023

Research Timeline



Ransomware & Energy Sector



[4]

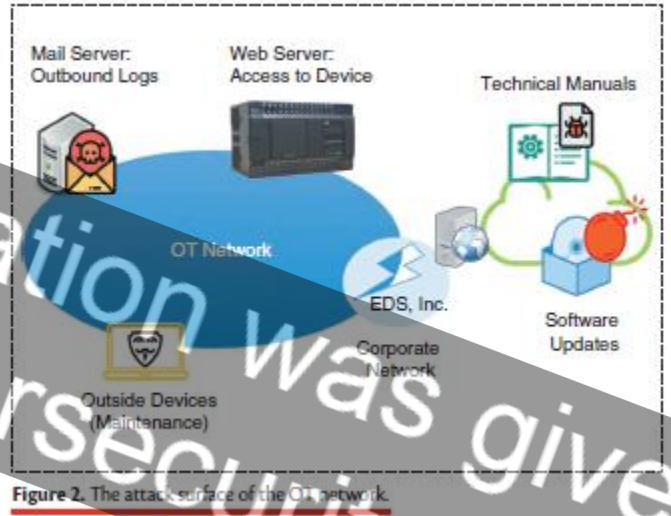
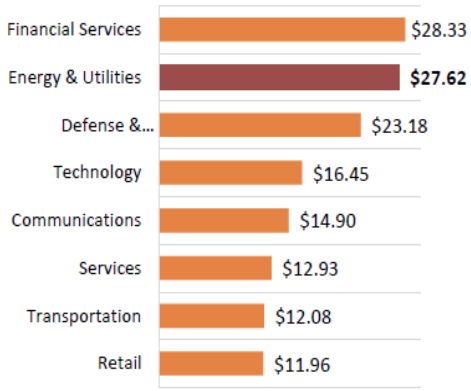


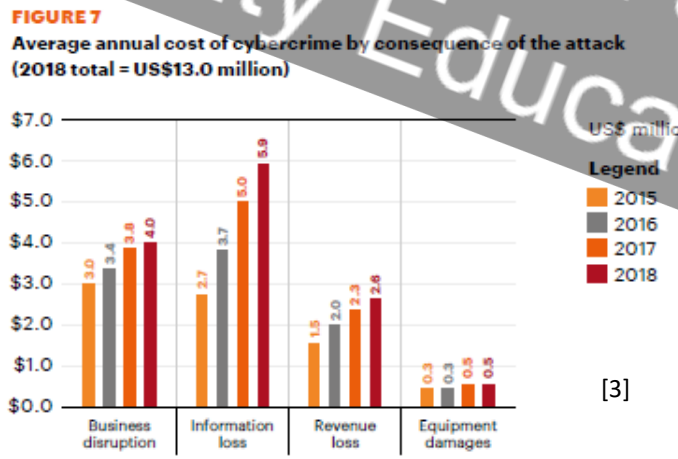
Figure 2. The attack surface of the OT network.

[2]

[1]



[4]



[3]

[1] "Snapshot." Accessed: Jan. 02, 2023. [Online]. Available: https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response

[2] "Nicol - 2021 - The Ransomware Threat to Energy-Delivery Systems.pdf."

[3] "Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf."

[4] B. Walker, "DOE Multiyear Plan for Energy Sector Cybersecurity _0.pdf," 2018.

Roadmap: **Roadmap Title**

Drivers

Drivers: Critical factors that influence organizational decisions, operations, and strategic plans, i.e., existing or pending regulations and standards, market conditions, consumer behavior, organizational goals and culture, etc.

Capability Gaps

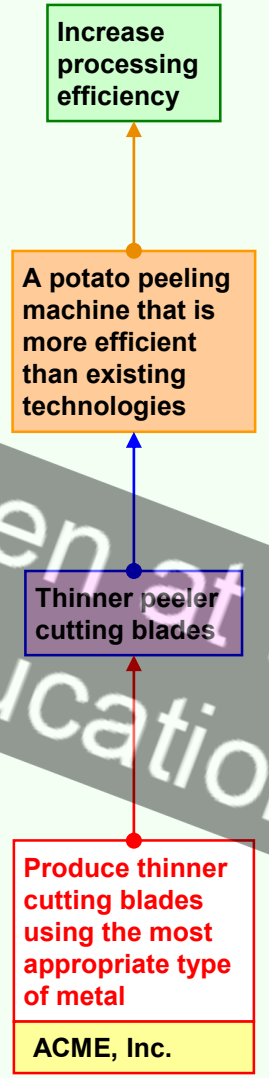
Capability Gaps: Barriers or shortcomings that stand in the way of meeting Drivers.

Technology Characteristics

Technology Characteristics: Specific technical attributes of a product, model, system, etc., that are necessary to overcome Capability Gaps. To be included in the technology roadmap these will either be: Commercially Available but facing technical barriers needing to be addressed; or Commercially Unavailable and needing to be developed.

R&D Programs

R&D Programs: Descriptions of programs to generate new ideas for products and services, develop models and prototypes, evaluate these in laboratory settings, demonstrate them in the field, and conduct engineering and production analyses to deliver the needed Technology Characteristics. The generic abbreviation "R&D" is to be understood as including, when appropriate, design, deployment, and demonstration in addition to research and development.



What are the reasons to change?

What are the barriers to change?

What are the technological solutions needed to overcome barriers?

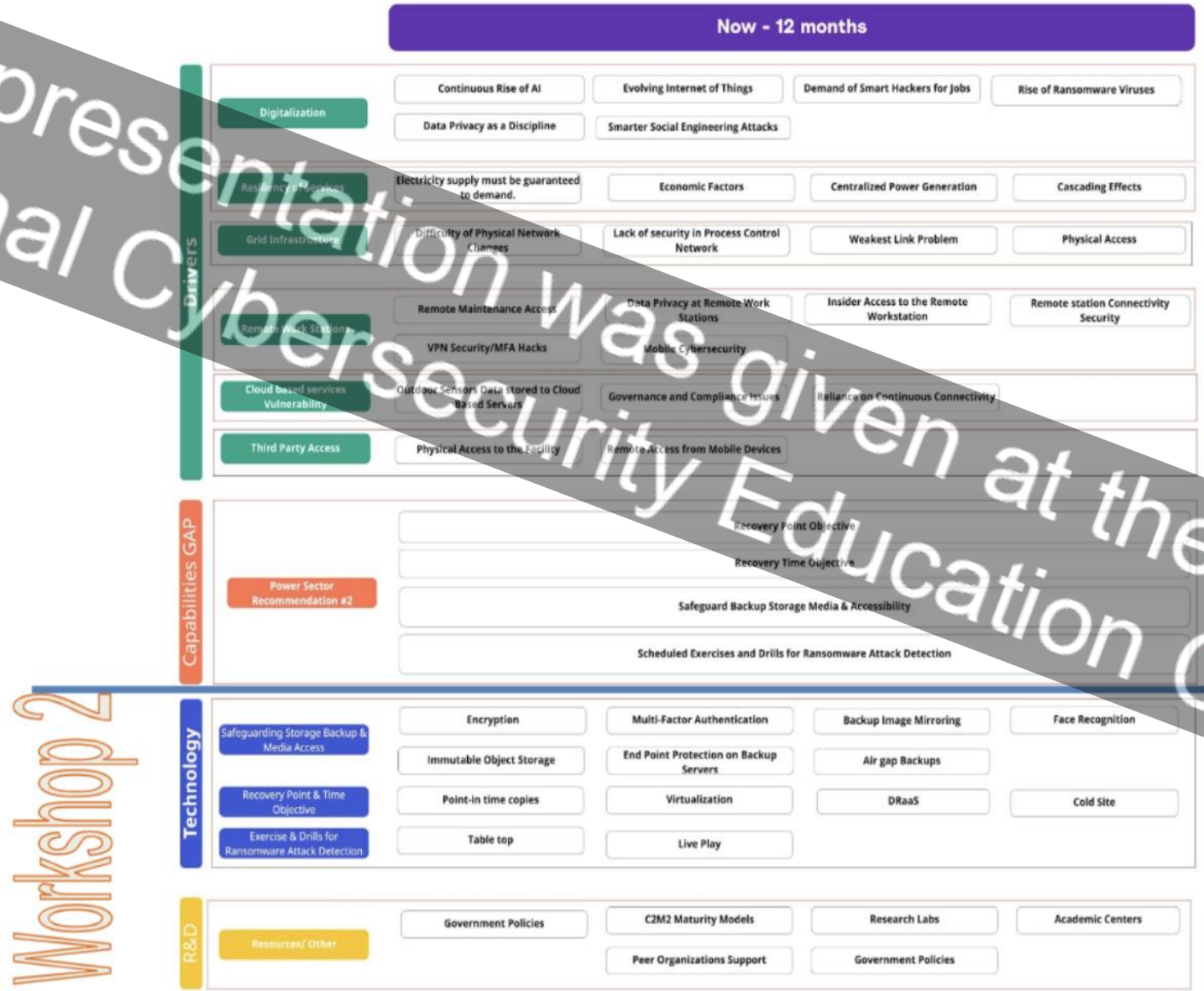
What research needs to be pursued to develop technological solutions?

Driver | Capability Gap | Commercially Available Technology | Commercially Unavailable Technology | Existing R&D Program or Project | R&D Program Requirement

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

PNW Electric System: Ransomware Technology Roadmap

Functions and Category: **Identify**



Workshop 2

Workshop 1

Roadmap Area :

III. DETECT (5/7)

Technology Roadmap
PNW Power Grid-Ransomware

Connection between Drivers and Cap. Gaps Groups

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Drivers

Collaboration and Communication to Prevent Attacks

- D1 Ransomware impact classifications. Not all ransomware incidents are deliberate "attacks" often they are discovering targets as they go. I feel the public should be more informed as to whether the ransomware incidents are due to targeted attacks or poor network setups or maintenance practices.
- D10 Area/Clarity Mgmt.
- D12 Cybersecurity Collaboration and Sharing to understand emerging and current ransomware attack vectors.
- D18 Sharing Key Indicators of Compromise to mitigate and remediate vulnerabilities to our Critical Infrastructure.
- D26 Separation of IT and OT in grid organizations
- D27 Multi-agency and cross sector information sharing of Indicators of Compromise will help to build a resilient cybersecurity methodology.
- D31 We need significant investment in Artificial Intelligence (AI) to detect phishing and smishing attacks that open the door to the penetration of Operational Technology (OT) systems.

Grid Infrastructure and Network Systems

- D1 Ransomware impact classifications. Not all ransomware incidents are deliberate "attacks" often they are discovering targets as they go. I feel the public should be more informed as to whether the ransomware incidents are due to targeted attacks or poor network setups or maintenance practices.
- D3 Efficient Disaster Recovery and Business Continuity planning: "Everyone" has been hacked... PNI, Whitehouse, IRS, even CIA. The game should shift to recovery with a healthy defense. Even the strongest defense tech has proven to be exploitable
- D5 OT and control systems need tightly controlled network segmentation to ensure any form of proliferation is limited. Business systems need this same level of segmentation but often do not have it.
- D16 Physical security of geographically diverse utilities
- D20 Limit exposure/access of systems to their intended scope as much as possible.
- D29 Constraints in updating software and systems in a timely manner
- D31 We need significant investment in Artificial Intelligence (AI) to detect phishing and smishing attacks that open the door to the penetration of Operational Technology (OT) systems.

Planning and Resiliency

- D3 Efficient Disaster Recovery and Business Continuity planning: "Everyone" has been hacked... PNI, Whitehouse, IRS, even CIA. The game should shift to recovery with a healthy defense. Even the strongest defense tech has proven to be exploitable
- D4 Business Continuity planning should include "manual mode" which has been proven to keep the lights on. Ukraine (Black Energy, Ukraine)
- D8 Business Continuity Planning
- D17 Board and officer-level sponsorship and interest/prioritization
- D23 Having playbooks already defined for known threats and checklists, documentation, for all assets and procedures as defined for various cyber incidents.
- DX "Standardized digital models Asset and configuration management Supply chain management Resiliency building blocks (From EPRI Roadmap 2030 Under Identify)"

Capability Gaps

Detection Processes

- CG7 "Implementation of Planning efforts is critical. Planning Equipment Training Exercise There are several tools and resources available to assist." D4, D8, D20, D18 DE.DP-2
- CG10 Most OT networks and the ICS on the network are poorly documented. This presents a challenge for [1] teams to determine who should have access to what, [2] identifying appropriate/authorized system to system connections, [3] conclusive evaluations of the OT network, if you can't scan it safely and it is poorly documented this can be a serious challenge. DE.DP-1, DE.DP-3
- CG16 Detection systems that can understand the interconnection and interdependencies between IT, OT and electrical grid networks. D26 DE.DP-2
- CG2 "Develop relationship with Oregon TITAN Fusion Center. Ensure information sharing and direct link on security and threat related information." D3 ID.RA-2
- CG21 Fortune 500 companies must [illegible] DE.DP-1
- CG11 OT network traffic can be difficult to monitor [illegible] DE.DP-2,3
- CG19 Event/Log aggregation is not often shared across capacity management, IT operations, and cybersecurity. The log "plumbing" can become extremely ad-hoc. DE.AE-3 DE.DP-2,3,4
- CG3 "Comprehensive Continuity of Operation Plan. Development of a plan to address the consequences of the incident and how to clarify critical tasks and steps. The plan should also follow national COOP standards and clearly identify chain of command and focused playbook steps." 4, 8, 2023 ID.AM, ID.BE DE.DP-4, 5
- CG24 IT detection products are destructive to OT and non-functional. OT detection products (Dragos, Nerve, Claroty, Nozomi, etc.) are not excellent in multiple types of environments (Gen/Trans/Dist/Cloud) DE.AE-1, DE.CM-1 DE.CM-8, DE.DP-5
- CG17 Cyber Log and event requirements are almost never included in designs and are always understood after the fact. DE.DP-5
- CG8 Connect with county Emergency Management partners to develop a strong approach to planning, training, and exercise approach. Key is local participation in the access resources as local as possible and find ways to enhance relationships and awareness throughout to maximize preparedness. D18 ID.BE-2, DE.DP-4

Driver	Capability Gap
Commercially Available Technology	Commercially Unavailable Technology
Existing R&D Program or Project	R&D Program Requirement

Connection between Drivers, Cap. Gaps Groups – Techn. Charac., and R&D Programs

Drivers

Remote Workstation Requirements

D2 Zero trust policies applied to appropriate zones within the Purdue Model, TCP/IP enables lateral movement whereas ZTNA does not allow. Ransomware thrives in environments that allow it to "worm" through the networks and devices attached.

D3 Efficient Disaster Recovery and Business Continuity planning: "Everyone" has been hacked…FBI, Whitehouse, IRS, even CEH. The game should shift to recovery with a healthy defense. Even the strongest defense tech has proven to be exploitable

D29 Need for remote access in operations (e.g., support)

D30 MFA and sometimes even individual access accountability is hard in utility systems (Note: this may have changed in the recent years)

D22 Understanding vendor access and using appropriate trust levels. Also, insure that all technology is being updated as required. Have sandbox to test updates before implementing them live on the system.

Capability Gaps

Recovery Planning

CG1 Restoration of some equipment/software requires 3rd party or OEM Specialists. ICS systems can also consist of legacy equipment and the restoration can be cumbersome/delayed due to lack of documentation or available expertise. RC.RP-1

CG2 Impacts of Ransomware attacks can vary due to complexity of "how" it is commonly designed prior to its deployment. Meaning sometimes there can be pre-payload actions that could be disruptive but not directly correlated to the setup of an attack/infection. This may complicate restoration efforts if not identified in mitigation/forensic efforts. RC.RP-1

Improvements

CG6 Sunsetting legacy infrastructure, identifying owners and transition plans to the cloud or secure service RC.IM-1,2

CG13 "Document lesson learned!Share results of the ransomware attack and remediation and mitigation efforts. Enforce the use of industry best practices including in the regulated Critical Infrastructure sectors." RC.IM-1

CG5 Share Indicators of Compromise (IOC) and remediation or mitigation steps with threat intelligence sources. This will reduce the impact of ransomware and strengthen the resilience of our Critical Infrastructure. 19 RC.IM-1, RC.CO-3

CG7 Real IR and remediation plans with active or frequent drills/exercises. Executive dashboard reporting with leadership accountability RC.IM-1

CG10 Modular OT equipment to facilitate quick recovery RC.IM-1

Technology Characteristics

T1 Split Byte for archive data. Eliminates ability for Ransomware Actor to impact the data. An 8-bit word is split to 8 different disks. https://splitbyte.com/ There is redundancy across the disks, so that even if one disk is damaged, the others can fill in the dataset. CG2, CG15

T2 Squirrel Compliance Solutions allows for lockdown of access nodes to prevent ransomware ingress. (RESPOND) https://www.squirrelcompliancysolutions.com/

T3 Design of OT devices such that they are easy to recover from failures. Example: isolated functionality in multi-functional devices where each functionality can be independently recovered. Context: asset owners typically have back-up of master configurations. CG13

T4 A process rather than technology. Document hard to recover devices and make preventive or recover plans for those devices. CG1, CG16, CG7

T5 Technology to automatically remove unneeded software in OT devices - reduce bloat. Some vendors do this by design but bloat creeps up when using third-party libraries. Example: no point having a full web-server implementation when only a portion of the functionality is used. Vendors having access to automated code auditing and reduction technologies can help. ONR funded a large program that developed tools and technologies for reducing code and functionality bloat. Technology may be available from that program. CG12

R&D Programs

RD1 MSP Version of Squirrel Compliance code T2

ML research and AI research are under way. Natural Language Processing (NLP) would be a new investigation.

RD2 Fast Recovery of OT Devices T3

There is research in embedded systems space looking at hardware assisted isolation and protection of critical functions. Fast restart based recovery has also been explored.

RD3 Software/Functionality Debloating for OT devices T3

ONR funded a large program called Total Platform Cyber Protection (TPCP) that investigated and developed automated debloating technologies

RD4 Litigation has prevented research advancement. T1

Driver

Capability Gap

Commercially Available Technology

Commercially Unavailable Technology

Existing R&D Program or Project

R&D Program Requirement

Item ID — Description — Connection to other level item(s)

Agent-Based Decision Making Model (ABDM) For Oregon Stakeholders

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Agent-Based Stakeholder Bargaining for Decision Making

Portland State
Hatfield School of Government

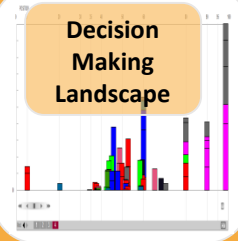
Framing

Definition of Problem

Structuring of Issues

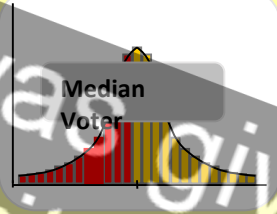
Issue

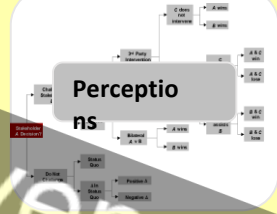
Issue n
Issue 2
Issue 1
Data Collection
Continuum
Stakeholders
Influence
Position
Importance
Decision Making Landscape

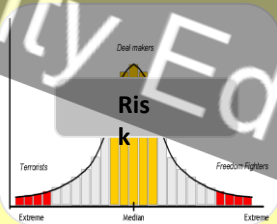


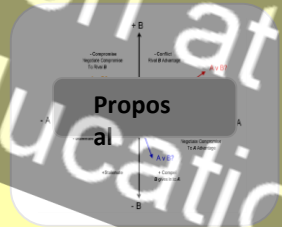
Analysis

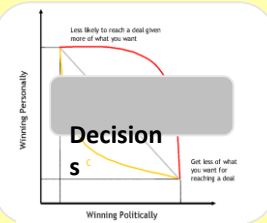
Model Algorithms

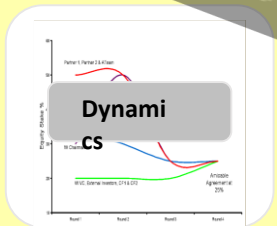






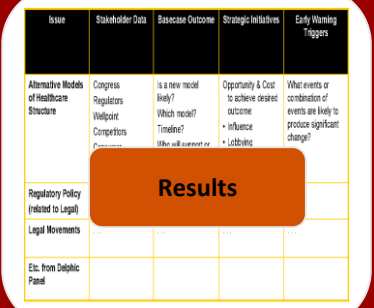






Output

Results



Issue Outcomes

Paths

Consensus

Action Plan

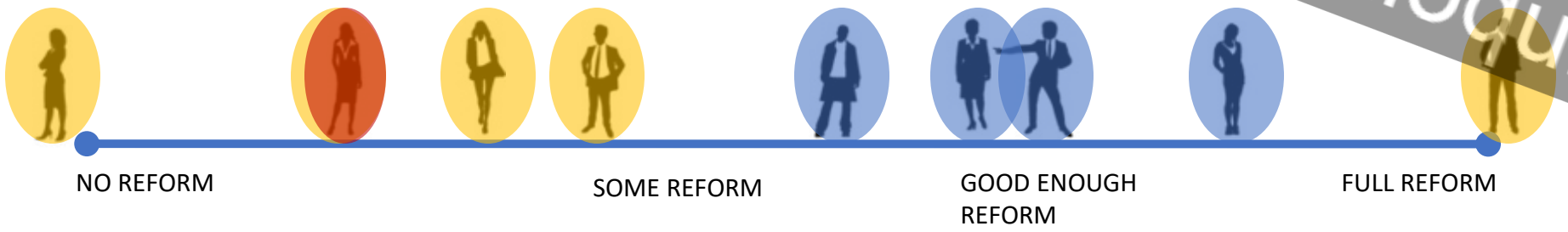
Portland State
Hatfield School of Government

Key Questions for Date Collection

1. Who are the **stakeholders** relevant to the issue?
2. What **positions** do they adopt?
3. What is their potential to **influence** the outcome?
4. How **salient** is the issue to them?

How: Drilling Down into Stakeholder Dynamics

- *Who is expected to change position?*
- *In response to whom?*
- *What is the predicted outcome and what degree of consensus obtains?*
- *What are the potential obstacles to achieving the desired level of reform?*



Oregon Stakeholders

- Two years of a face-to-face discussion with representatives of high-tech companies, PG&E, BPA, NW Natural, Umatilla Electric Cooperative, Avangrid, FBI, CISA, State of Oregon CIO, CISO, Technology Association of Oregon, Nike, PSU, University of Oregon, Oregon State University, Mt. Hood Community College, Portland Community College, Chemeketa Community College, Oregon Institute of Technology, elected representatives and senators in the Oregon Legislature, League of Oregon Cities, Association of Oregon Counties, Special Districts Association of Oregon, and K12 School Districts Association.

Bargaining Issues: A Major Initiative

Oregon Cybersecurity Center of Excellence						
stakeholders	veto	Power	issue1	salience	issue2	salience
State Legislature	Y	80	60	90	30	95
Governor	Y	100	60	90	30	95
PSU	N	10	60	95	100	90
OSU	N	10	60	95	100	90
UO	N	10	60	95	100	90
Private Sector TAO	N	10	60	95	60	85
PGE	N	10	60	85	60	85
Pacific Energy	N	10	60	80	60	85
Community Colleges	N	5	100	95	100	90
Other universities	N	5	100	95	100	90
LOC	N	10	60	85	60	85
AOC	N	10	100	85	60	85
ASD	N	5	100	85	60	85
CISO	N	10	60	85	30	90
ISSUE 1: Establish a Cybersecurity Center of Excellence						
0	no OCCoE					
30	Small scope (only limited to three universities)					
60	Three universities plus others over time					
100	Full scale participation of all universities and community colleges now					
ISSUE 2: Funding						
0	no funding					
30	One time limited funding					
60	One time full funding					
100	Fund in perpetuity					

RESULTS FROM OREGON:

- STAKEHOLDERS COMMITTED TO COLLABORATION ON THE CHALLENGES – NOT JUST IN POWER CRITICAL INFRASTRUCTURE.

- **HB 2049:** STATE OF OREGON ESTABLISHES THE OREGON CYBERSECURITY CENTER OF EXCELLENCE.
  - PSU's Cybersecurity & Cyber Defense Policy Center is identified as the administrative home.

  - PSU Receives an NSF Innovative Engine Phase I Grant for two-years to establish a coalition of industry-university-government partnership for the future SmartGrid.

Oregon CCoE Mission Areas (Complementing State CIO Efforts)

Network & Systems Security and Resiliency

Oregon State University

Systems Security & Privacy, Cyber Operations

Portland State

Public Policy & National Security, Technology Roadmap,

Cloud Security

OREGON CYBERSECURITY CENTER of EXCELLENCE

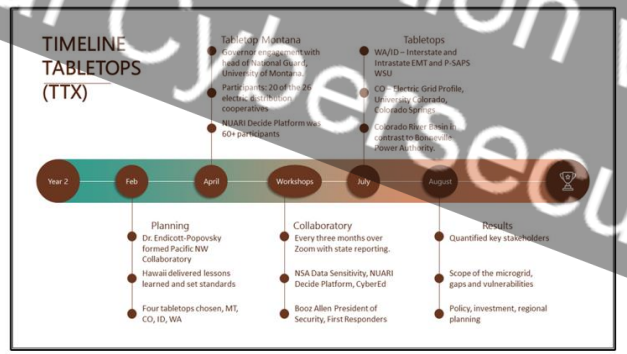
Community Engagement, Workforce Development,

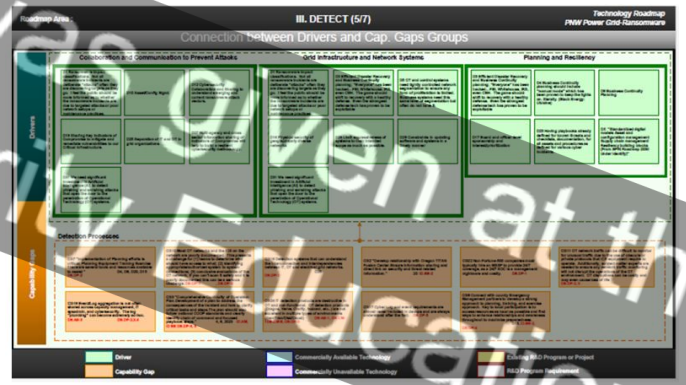
Security Services & Cutting Edge Research

Portland State
Hatfield School of Government

Conclusions

- Identified key consultants to focus and lead efforts
- Evaluated protection capability through **Tabletops**





- Detected capabilities through **Technology Roadmaps**
- Analyze stakeholders' ability to respond

Thank You for Listening

This presentation was given at the 2023 National Cybersecurity Education Colloquium