NextGrid
Illinois

WELCOME TO MEETING #3 – PEOPLE / PROCESS

WORKING GROUP 3 (RELIABILITY, RESILIENCY, AND CYBER SECURITY)

AGENDA

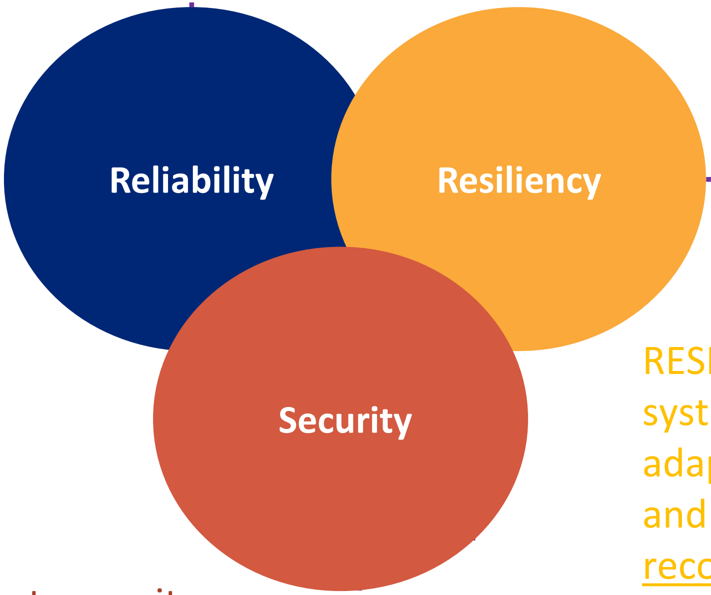
Time	Agenda Item	Presenter
9:00AM – 9:10AM (10 minutes)	**Meeting #2 Recap, Other Updates**	WG3 Co-Leads
9:10AM – 10:10AM (60 minutes)	**People / Process Presentations**	NERC EPRI Ameren
10:10AM – 11:00 AM (50 minutes)	**People Discussion**	WG Members, WG Co-Leads
11:00AM – 11:05AM (5 minutes)	**BREAK**	
11:05AM – 11:55 AM (50 minutes)	**Process Discussion**	WG Members, WG Co-Leads
11:55AM – 12:00PM (5 minutes)	**Questions?** **Process Discussion Items to Carryover to Next Meeting?** **Next Steps & Call for Presenters**	WG Co-Leads

WORKING GROUP RECAP, AND OTHER UPDATES

CO-LEADS:
MANIMARAN GOVINDARASU
DOMINIC SAEBELER

RELIABILITY, RESILIENCY, AND CYBER SECURITY

RELIABILITY: “ability of the system or its components to withstand instability, uncontrolled events, cascading failures, or unanticipated loss of system components”



RESILIENCY: “ability of a system or its components to adapt to changing conditions and withstand and rapidly recover from disruptions”

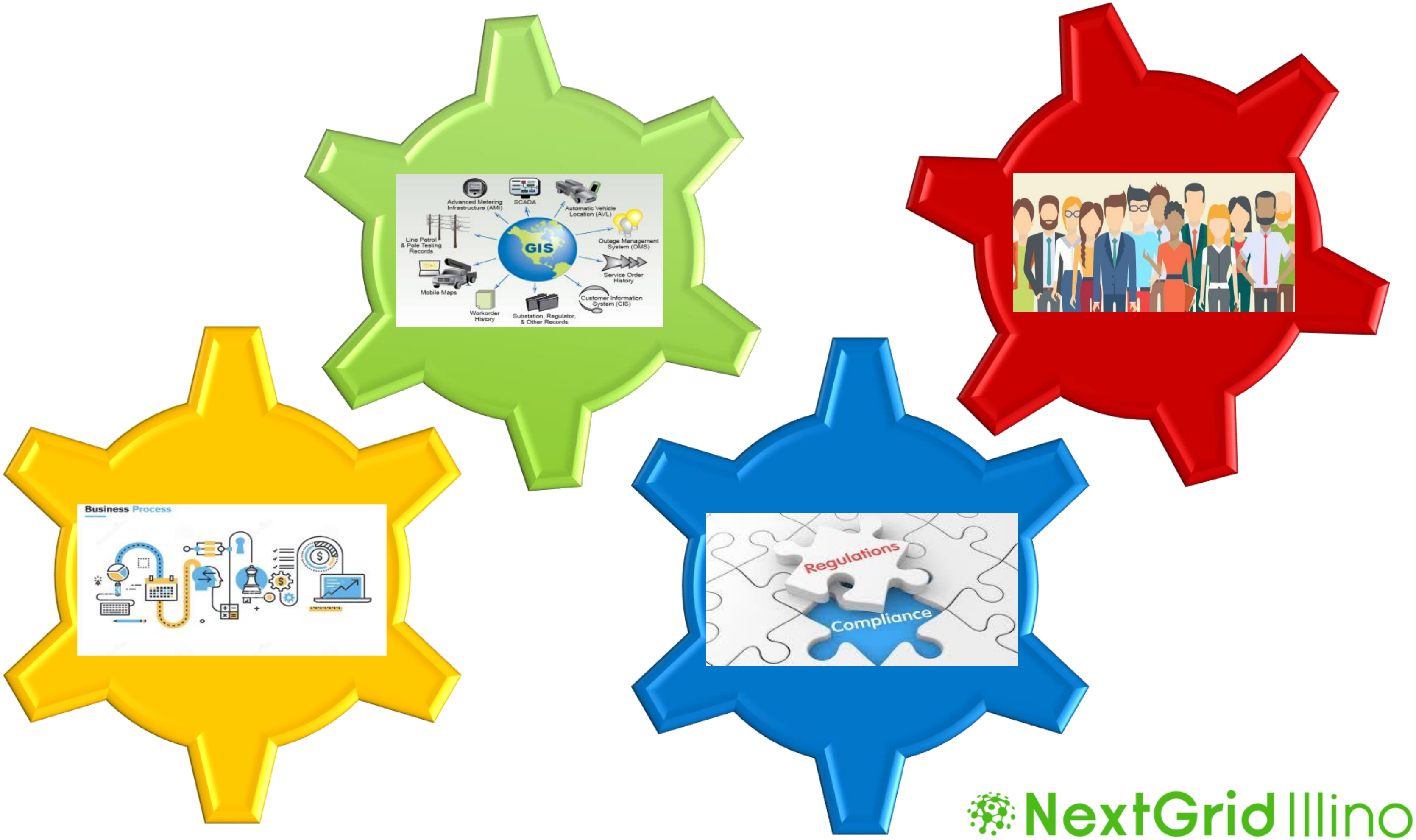
SECURITY: “ability of a system or its components to withstand attacks (including physical and cyber incidents) on its integrity and operations”

Definitions from DOE Quadrennial Energy Review: Second Installment: Chapter IV)

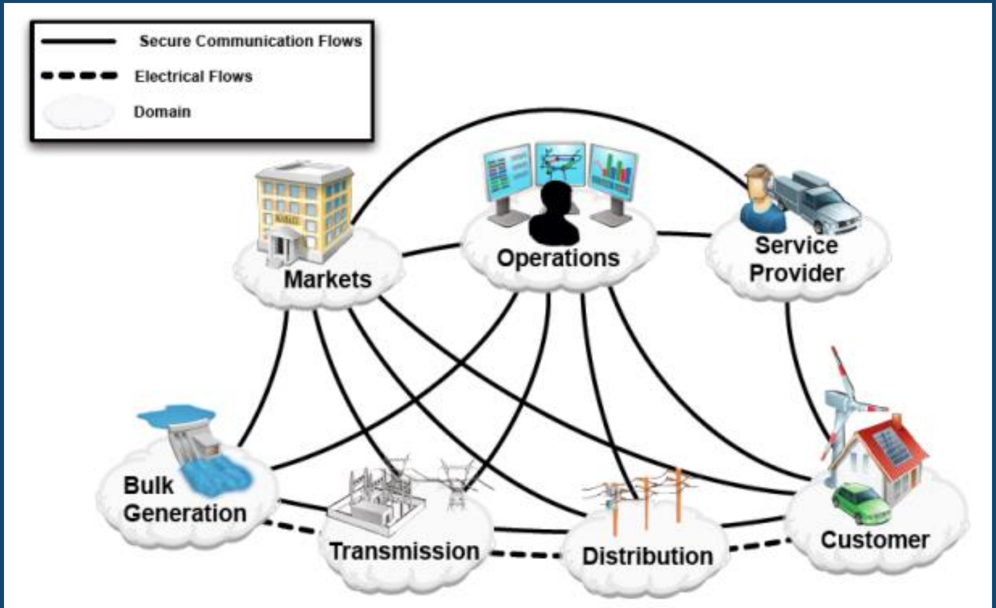
NextGrid Illinois

PROPOSED APPROACH

TECHNOLOGY, PEOPLE, PROCESS, AND REGULATION


Advanced Metering Infrastructure (AMI)
SCADA
Automatic Vehicle Location (AVL)
Line Patrol & Pole Testing Records
GIS
Outage Management System (OMS)
Service Order History
Mobile Maps
Workorder History
Substation, Regulator, & Other Records
Customer Information System (CIS)
Business Process
Regulations
Compliance

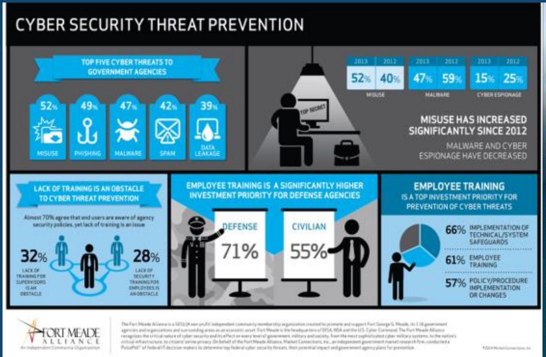
SMART GRID: A CYBER-PHYSICAL SYSTEM



Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, Reliability Standards, February 2012

TECHNOLOGY

NextGrid Illinois



CYBER SECURITY THREAT PREVENTION

TOP FIVE CYBER THREATS TO GOVERNMENT AGENCIES

52%	49%	47%	42%	39%
MISUSE	PHISHING	MALWARE	SPAM	DATA LEAKAGE

	MISUSE		MALWARE		CYBER ESPIONAGE	
	2013	2012	2013	2012	2013	2012
	52%	40%	47%	59%	15%	25%

TOP SECRET

MISUSE HAS INCREASED SIGNIFICANTLY SINCE 2012

MALWARE AND CYBER ESPIONAGE HAVE DECREASED

LACK OF TRAINING IS AN OBSTACLE TO CYBER THREAT PREVENTION

Almost 70% agree that end users are aware of agency security policies, yet lack of training is an issue

32% LACK OF TRAINING FOR SUPERVISORS IS AN OBSTACLE

28% LACK OF SECURITY TRAINING FOR EMPLOYEES IS AN OBSTACLE

EMPLOYEE TRAINING IS A SIGNIFICANTLY HIGHER INVESTMENT PRIORITY FOR DEFENSE AGENCIES

DEFENSE 71%

CIVILIAN 55%

EMPLOYEE TRAINING IS A TOP INVESTMENT PRIORITY FOR PREVENTION OF CYBER THREATS

66% IMPLEMENTATION OF TECHNICAL/SYSTEM SAFEGUARDS

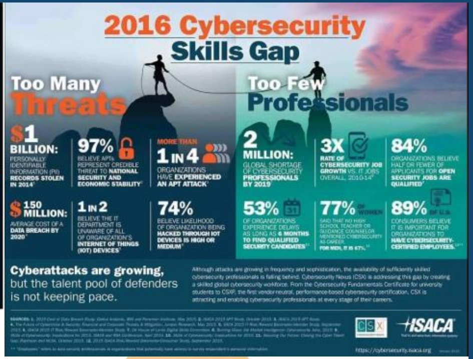
61% EMPLOYEE TRAINING

57% POLICY/PROCEDURE IMPLEMENTATION OR CHANGES

FORT MEADE ALLIANCE
An Independent Community Organization

The Fort Meade Alliance is a 501(c)4 non-profit independent community membership organization created to promote and support Fort George G. Meade, its 116 government agencies and organizations and surrounding areas as an economic asset. Fort Meade is the headquarters of DISA, NSA and the U.S. Cyber Command. The Fort Meade Alliance recognizes the critical nature of cyber security and its effect on every level of government, military and society. From the most sophisticated cyber military systems, to the nation's critical infrastructure, to citizens' online privacy. On behalf of the Fort Meade Alliance, Market Connections, Inc., an independent government market research firm, conducted a PulsePoll of federal IT decision-makers to determine top federal cyber security threats, their potential impact and government agency plans for prevention.

©2014 Market Connections, Inc.



2016 Cybersecurity Skills Gap

Too Many Threats

$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) RECORDS STOLEN IN 2014[1]

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO NATIONAL SECURITY AND ECONOMIC STABILITY[2]

MORE THAN 1 IN 4 ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK[3]

$150 MILLION: AVERAGE COST OF A DATA BREACH BY 2020[4]

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S INTERNET OF THINGS (IOT) DEVICES[5]

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM[6]

Too Few Professionals

2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY PROFESSIONALS BY 2019[7]

3X RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14[8]

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR OPEN SECURITY JOBS ARE QUALIFIED[9]

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS 6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES[10]

77% OF WOMEN SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. FOR MEN, IT IS 67%.[11]

89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.[12]**

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

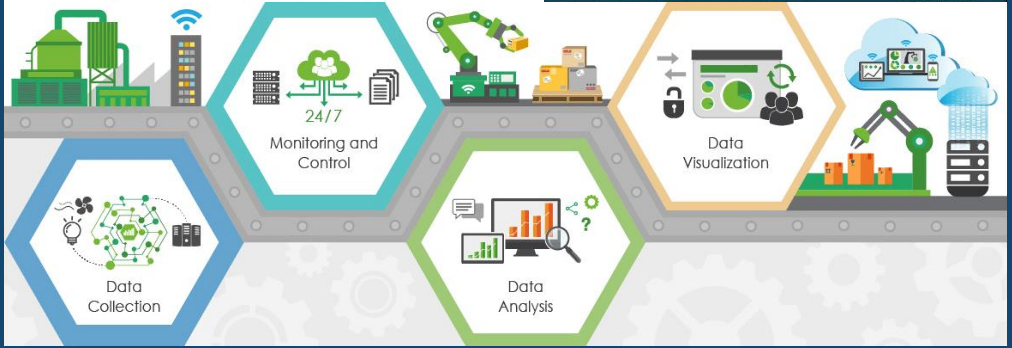
Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

SOURCES: [illegible]

** "Employees" refers to [illegible]

CSX ISACA

https://cybersecurity.isaca.org



PEOPLE

NextGrid Illinois

PROCESS

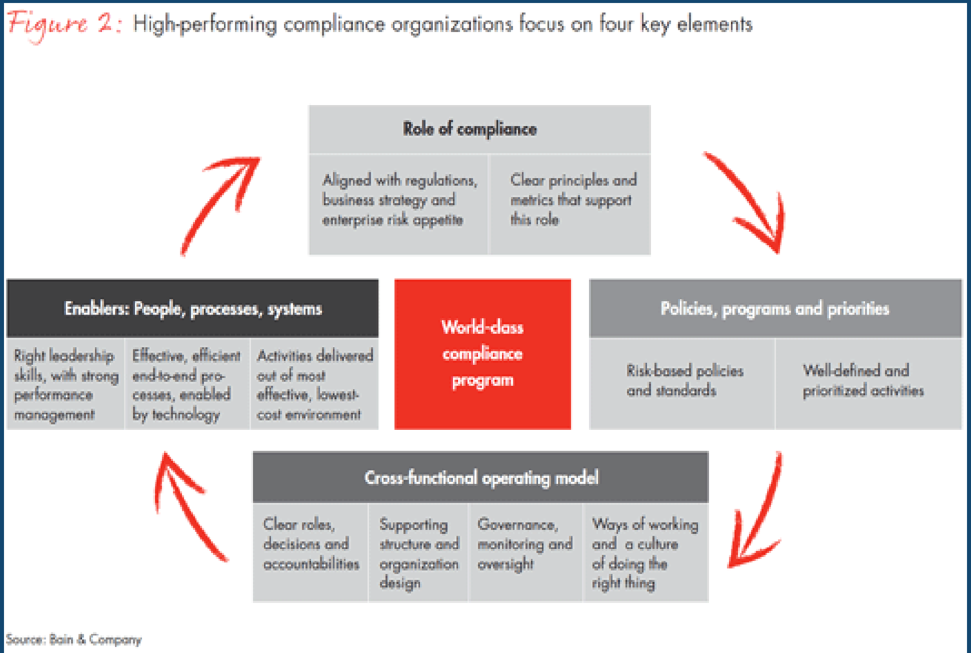


Figure 2: High-performing compliance organizations focus on four key elements

World-class compliance program

Role of compliance

- Aligned with regulations, business strategy and enterprise risk appetite
- Clear principles and metrics that support this role

Policies, programs and priorities

- Risk-based policies and standards
- Well-defined and prioritized activities

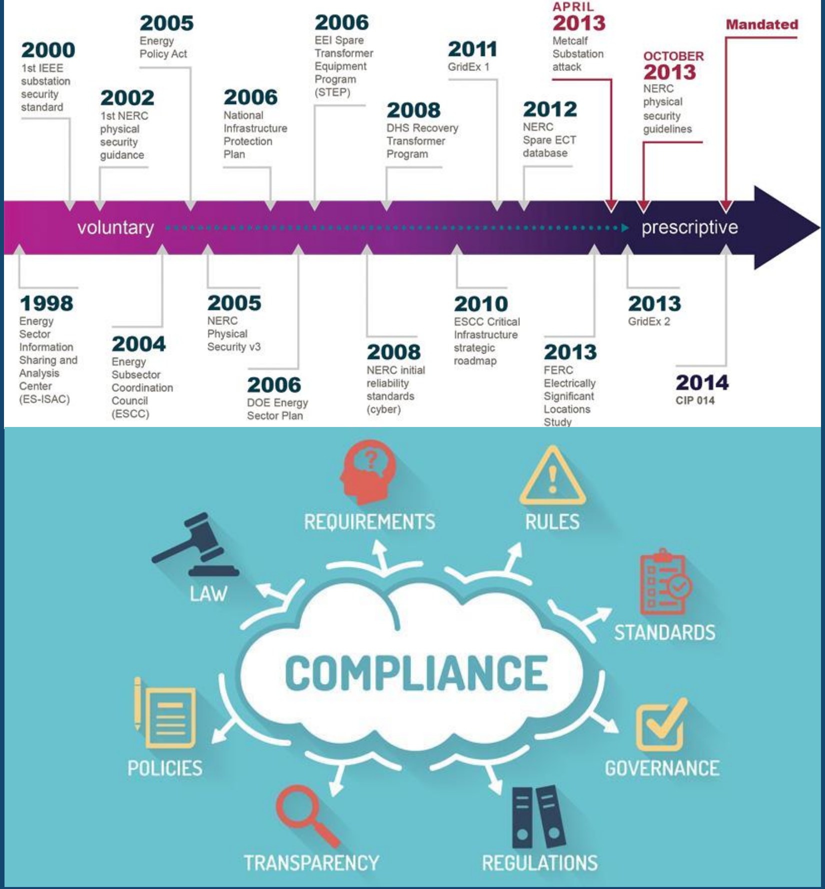
Cross-functional operating model

- Clear roles, decisions and accountabilities
- Supporting structure and organization design
- Governance, monitoring and oversight
- Ways of working and a culture of doing the right thing

Enablers: People, processes, systems

- Right leadership skills, with strong performance management
- Effective, efficient end-to-end processes, enabled by technology
- Activities delivered out of most effective, lowest-cost environment

Source: Bain & Company



2000 1st IEEE substation security standard

2005 Energy Policy Act

2002 1st NERC physical security guidance

2006 National Infrastructure Protection Plan

2006 EEI Spare Transformer Equipment Program (STEP)

2008 DHS Recovery Transformer Program

2011 GridEx 1

2012 NERC Spare ECT database

APRIL 2013 Metcalf Substation attack

OCTOBER 2013 NERC physical security guidelines

Mandated

voluntary → prescriptive

1998 Energy Sector Information Sharing and Analysis Center (ES-ISAC)

2004 Energy Subsector Coordination Council (ESCC)

2005 NERC Physical Security v3

2006 DOE Energy Sector Plan

2008 NERC initial reliability standards (cyber)

2010 ESCC Critical Infrastructure strategic roadmap

2013 FERC Electrically Significant Locations Study

2013 GridEx 2

2014 CIP 014

REGULATION & COMPLIANCE

NextGrid Illinois

TOPICS MATRICES

Challenges	Opportunities	Solutions	Education	Potential Action Items
Technology				
" " "	" " "	" " "	" " "	" " "
" " "	" " "	" " "	" " "	" " "
People				
" " "	" " "	" " "	" " "	" " "
" " "	" " "	" " "	" " "	" " "
Process				
" " "	" " "	" " "	" " "	" " "
" " "	" " "	" " "	" " "	" " "
Regulations & Compliance				
" " "	" " "	" " "	" " "	" " "
" " "	" " "	" " "	" " "	" " "

NextGrid Illinois

PEOPLE / PROCESS PRESENTATIONS

E-ISAC

Electricity Information Sharing and Analysis Center

BILL LAWRENCE

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Electricity Information Sharing and Analysis Center

Bill Lawrence, Director of the E-ISAC
NextGrid Webinar
May 11, 2018

RESILIENCY | RELIABILITY | SECURITY

Agenda

- E-ISAC mission and vision
- E-ISAC products and services
- NextGrid process priority topics
  - Metrics (#3)
  - Harmonizing frameworks (#5)
  - Exercising (evaluation and testing) (#6)
- E-ISAC points of contact

Mission

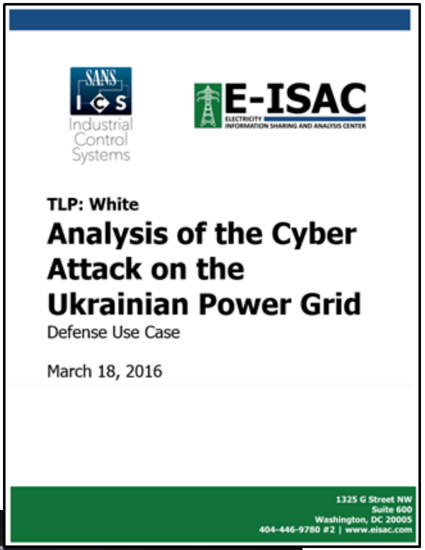
The E-ISAC reduces cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration

Vision

To be a world class, trusted source for the quality analysis and rapid sharing of electricity industry security information

E-ISAC Products and Services

- Products
  - Subject matter experts for NERC Alerts
  - Incident (cyber and physical) bulletins
  - Weekly, monthly, and annual summary reports
  - Issue-specific reports
- Programs and Services
  - Monthly briefing series, first Tuesday of the month
  - Grid Security Conference (GridSecCon)
  - Grid Exercise (GridEx)
  - Cyber Risk Information Sharing Program (CRISP)
  - Industry Augmentation Program (IAP)
- Tools
  - E-ISAC portal (www.eisac.com)
  - Critical Broadcast Program (CBP) notifications
  - Cyber Automated Information Sharing System (CAISS)



SANS ICS Industrial Control Systems

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

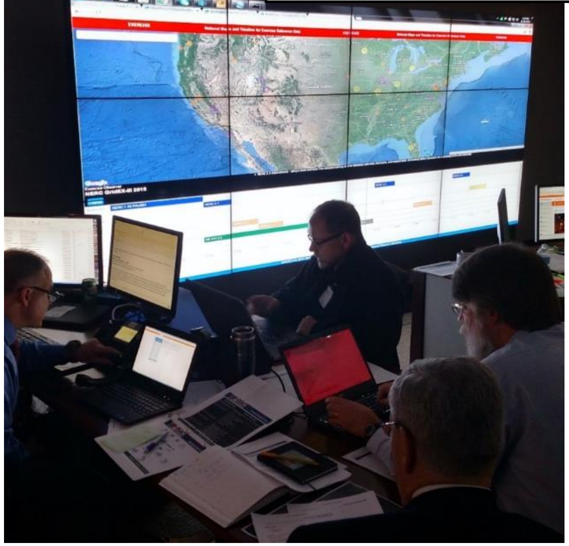
TLP: White

Analysis of the Cyber Attack on the Ukrainian Power Grid

Defense Use Case

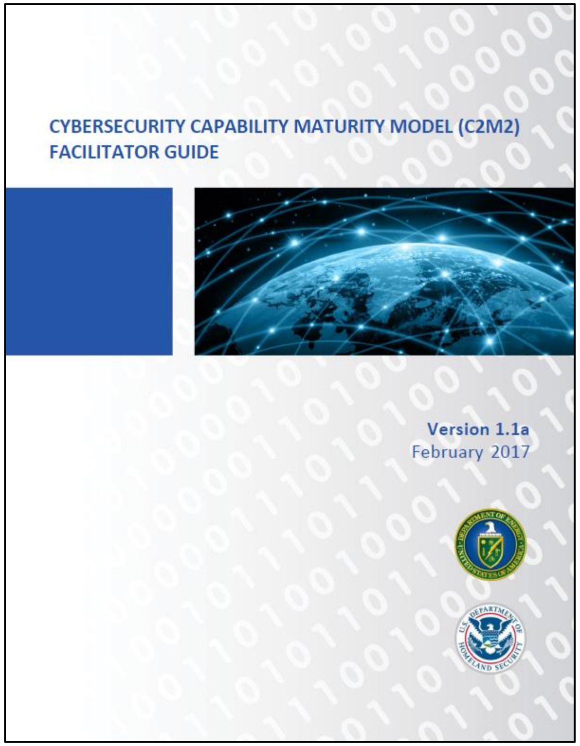
March 18, 2016

1325 G Street NW
Suite 600
Washington, DC 20005
404-446-9780 #2 | www.eisac.com



Metrics

- *3. Address need for metrics to quantify effectiveness of interventions*
  - Electricity Sector Cybersecurity Capability Maturity Model (ES-C2M2)



CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)
FACILITATOR GUIDE

Version 1.1a
February 2017

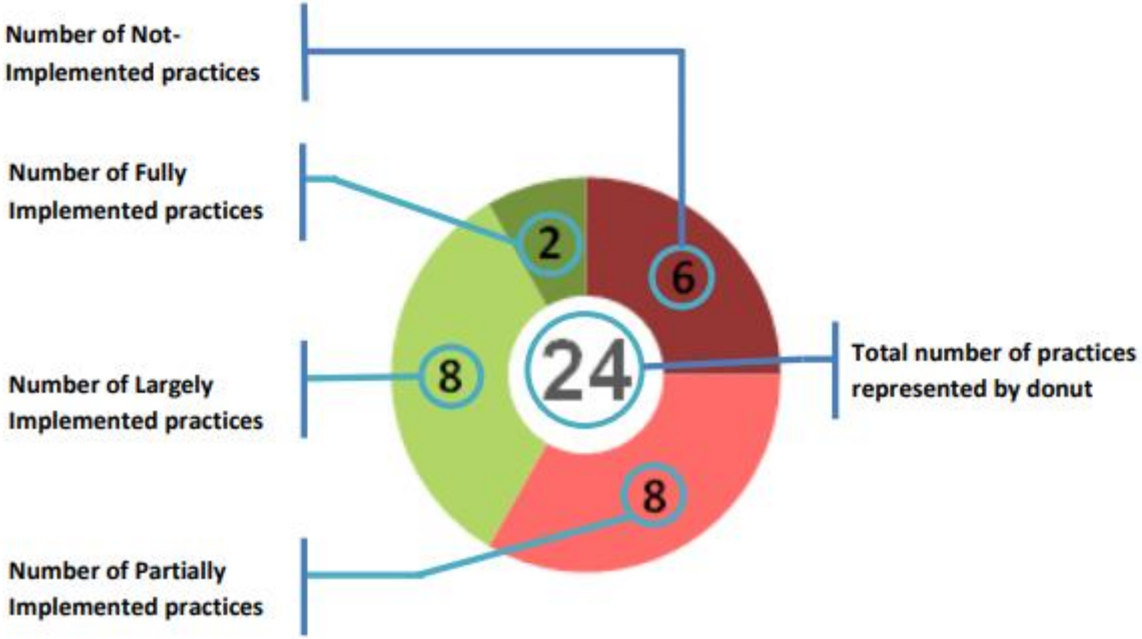


Figure 2: Graphical Representation of Single Donut

Metrics (continued)

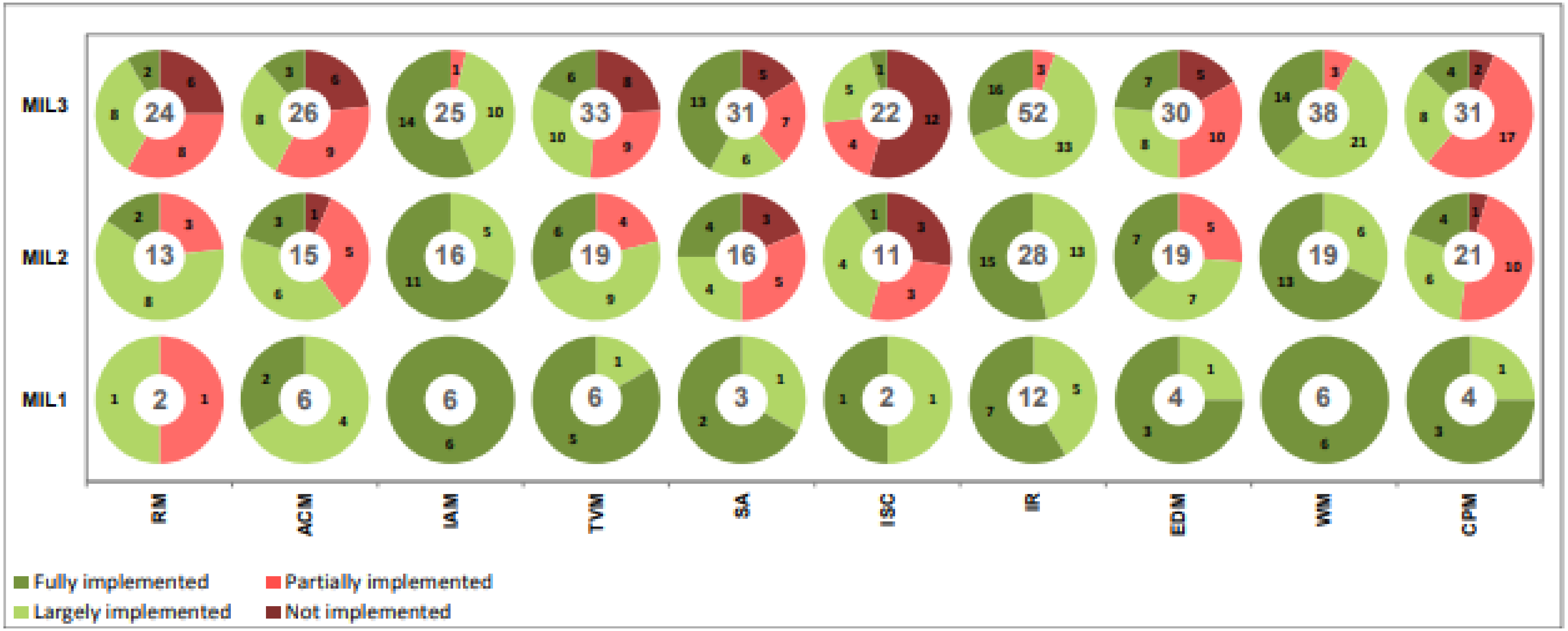
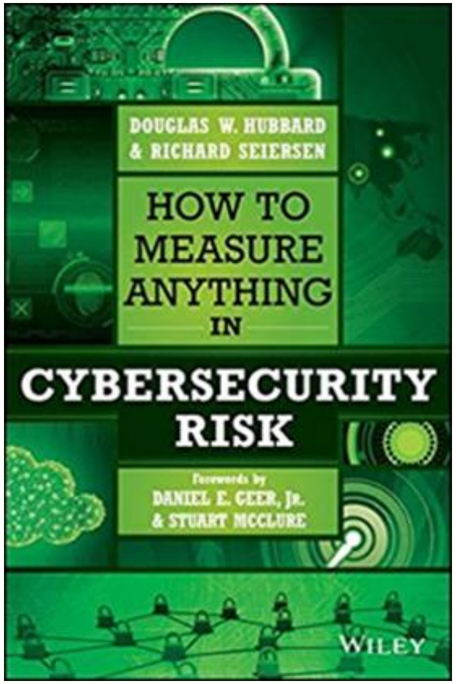


Figure 3: Domains Graphical Summary of the C2M2 Survey

Metrics (continued)

- We:
  - Can learn from other domains
  - Have more data than we think
  - Need less data than we think
  - Can make better security and investment decisions using quantitative, probabilistic methods



DOUGLAS W. HUBBARD & RICHARD SEIERSEN

HOW TO MEASURE ANYTHING IN CYBERSECURITY RISK

Forewords by DANIEL E. GEER, Jr. & STUART MCCLURE

WILEY

Harmonizing frameworks

- *5. Harmonizing framework adoption for: information sharing, incident response management, and contingency planning/analysis criteria*
- E-ISAC
  - Portal with dedicated user communities www.eisac.com
    - Voluntary information sharing and required reporting
  - Cyber Automated Information Sharing System (CAISS)
  - Cyber Risk Information Sharing Program (CRISP)
  - Cross-sector and federal government partners
- Other opportunities
  - DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
  - National Guard
  - FBI field offices
  - DHS Protective Security Advisors

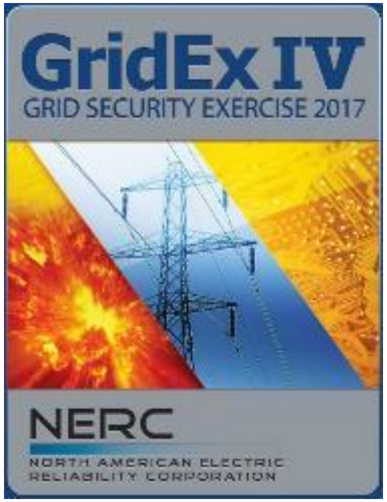
Exercising (evaluation and testing)

- *6. Prioritizing effective, regular, and consistent evaluation and testing of core capabilities*
  - Department of Energy's regional exercise initiatives
  - National Exercise Program (NLE, Cyber Storm, etc.)
  - NERC's biennial GridEx IV

GridEx Mission Statement

GridEx is an unclassified public/private exercise
designed to simulate a coordinated cyber/physical attack
with operational impacts
on electric and other critical infrastructures
across North America
to improve security, resiliency and reliability

GridEx IV Objectives



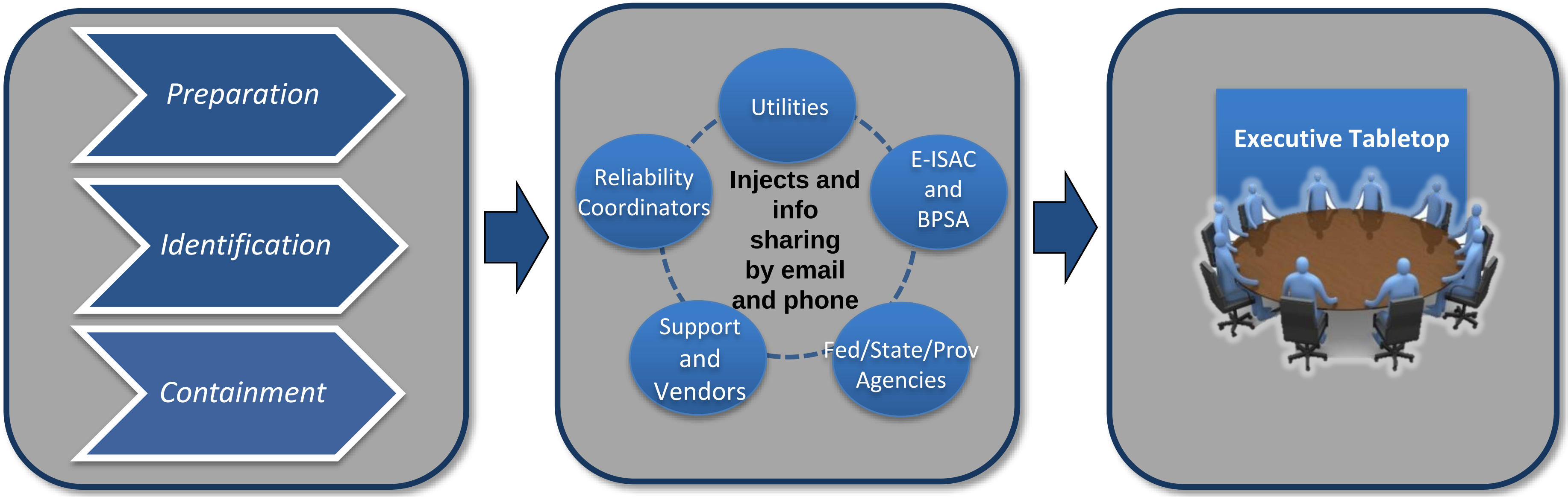
- Exercise incident response plans
- Expand local and regional response
- Engage critical interdependencies
- Improve communication
- Gather lessons learned
- Engage senior leadership

Exercise Components

Move 0 Pre-Exercise

Distributed Play (2 days)

Executive Tabletop (1/2 day)



Preparation

Identification

Containment

Utilities

E-ISAC and BPSA

Fed/State/Prov Agencies

Support and Vendors

Reliability Coordinators

Injects and info sharing by email and phone

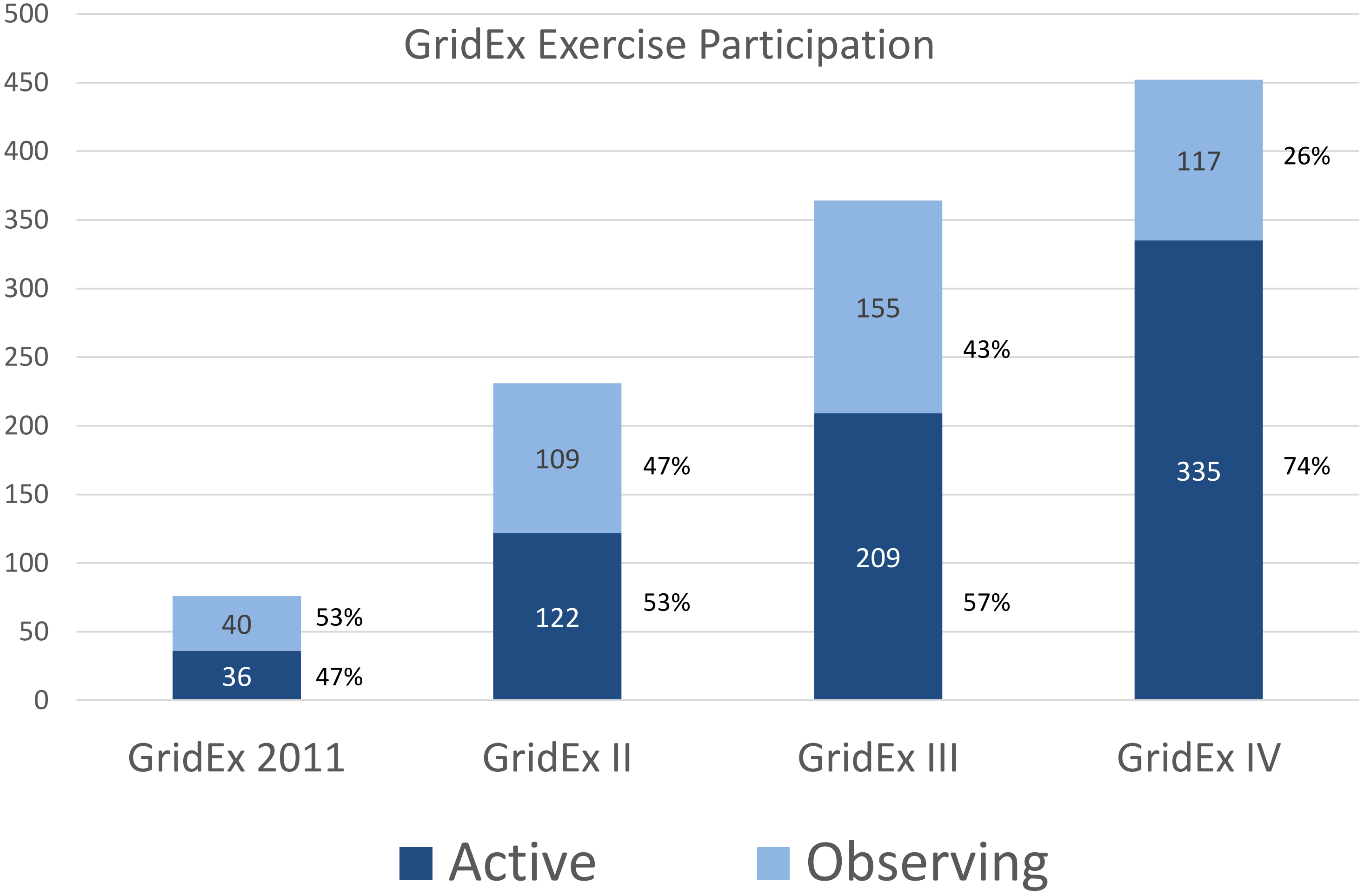
Executive Tabletop

Operators may participate in Cyber Intrusion detection activities

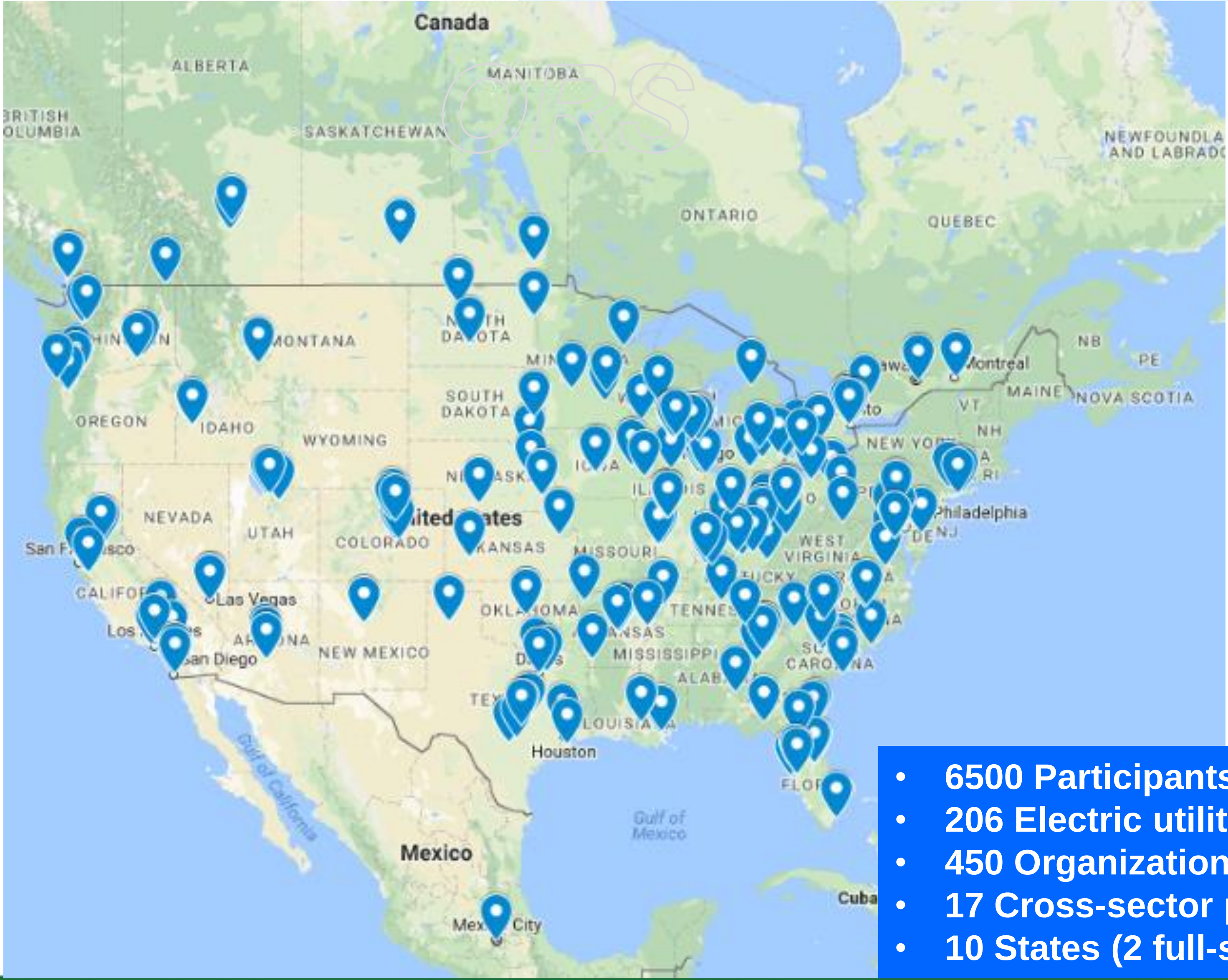
Players across the stakeholder landscape will participate from their local geographies

Facilitated discussion engages senior decision makers in reviewing distributed play and exploring policy triggers

GridEx Participation



GridEx IV: Who Participated?



- 6500 Participants
- 206 Electric utilities
- 450 Organizations
- 17 Cross-sector partners
- 10 States (2 full-scale)

More information

- GridEx V is November 13-14, 2019
- GridSecCon 2018 in Las Vegas, NV, October 15-19
- E-ISAC points of contact
  - events@eisac.com
  - memberservices@eisac.com
  - operations@eisac.com

Questions and Answers

GALEN RASCHE

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

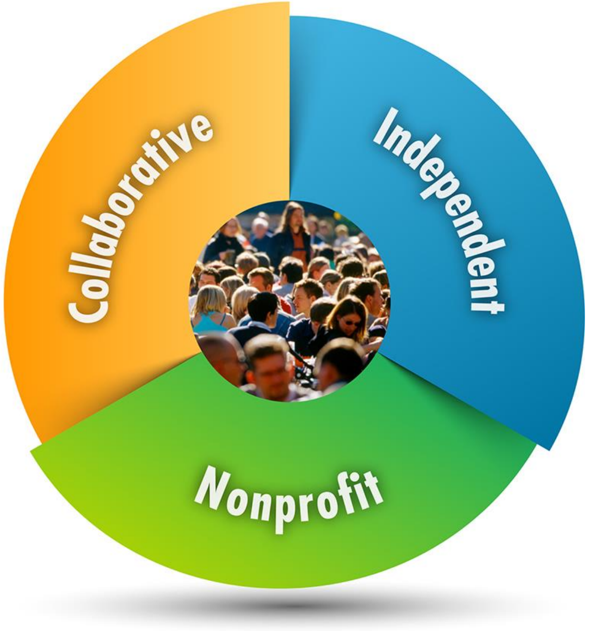
Illinois NextGrid: Utility of the Future Study

WG3: Reliability, Resiliency, and Cyber Security

Galen Rasche
Sr. Program Manager,
Cyber Security
grasche@epri.com

May 11, 2018

About the Electric Power Research Institute



Independent

Objective, scientifically based results address reliability, efficiency, affordability, health, safety, and the environment

Nonprofit

Chartered to serve the public benefit

Collaborative

Bring together scientists, engineers, academic researchers, and industry experts

Industry Trends Impacting Cyber Security Risk

Generation, Transmission & Distribution

- Real-time situational awareness
- Dynamic supply / demand balancing with DER (DERMS)
- Mobile workforce
- Increased automation and communications

Customer

- Self generation (Solar PV, Storage,..)
- Electric vehicles
- IoT devices

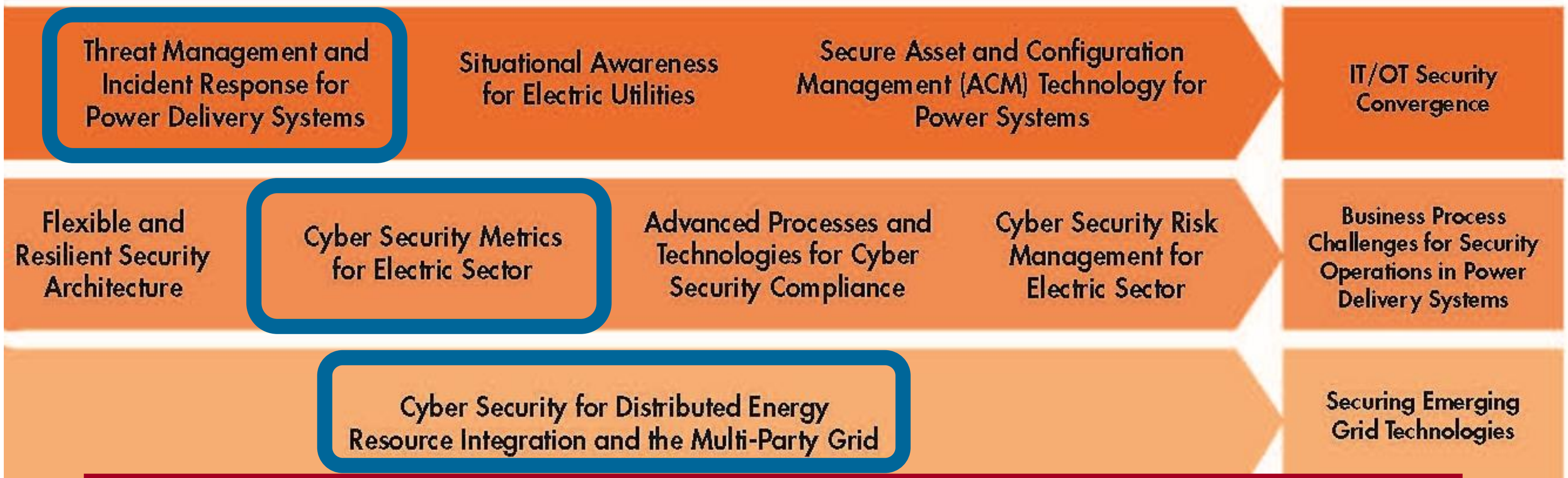
Third Parties

- DER and DR aggregators

National Security/Resiliency Mindset

- Malicious attack or natural catastrophe

Information, Communication and Cyber Security Roadmap



Threat Management and Incident Response for Power Delivery Systems

Situational Awareness for Electric Utilities

Secure Asset and Configuration Management (ACM) Technology for Power Systems

IT/OT Security Convergence

Flexible and Resilient Security Architecture

Cyber Security Metrics for Electric Sector

Advanced Processes and Technologies for Cyber Security Compliance

Cyber Security Risk Management for Electric Sector

Business Process Challenges for Security Operations in Power Delivery Systems

Cyber Security for Distributed Energy Resource Integration and the Multi-Party Grid

Securing Emerging Grid Technologies

EPRI's Cyber Security Program R&D for Industry…

- ***Mitigate risks*** to legacy and next-generation grid systems
- ***Improve security*** with advanced network and threat management technology and practices
- ***Effectively evaluate*** security program processes
- ***Learn*** how peer utilities address their security challenges
- ***Leverage*** *EPRI's* industry expertise, sector knowledge, and Cyber Security Research Lab to provide value ranging from thought leadership to hands-on demonstrations

IT/OT Security Convergence

Incident Response

- Integrated Security Operations Center
- IDS/IPS
- Forensics
- Security Data Analytics

Situational Awareness

- Developing near-real-time knowledge of a dynamic operating environment
- Common Operating Picture

Threat Management

- OT threat intelligence use cases, methodologies, and tools

Asset and Configuration Management

- Technologies to improve device identification and configuration management

Threat Detection – PG&E Metcalf Substation Shooting

Telecom, Cyber Security

Physical Security

Control Center

12:58 & 1:07 a.m. AT&T fiber-optic telecommunications cables were cut and Internet Service Provider network cables cut near Metcalf substation

1:31 a.m. Surveillance camera at substation recorded a streak of light followed by muzzle flash of rifles and sparks from bullets hitting the fence.

1:37 a.m. PG&E received an alarm from motion sensors at the substation, possibly from bullets grazing the fence.

1:41 a.m. Sheriff's department received a 911 call about gunfire.

1:45 a.m. The transformers, riddled with bullet holes leaked 52,000 gallons of oil, overheated, PG&E's control center received equipment-failure alarm.

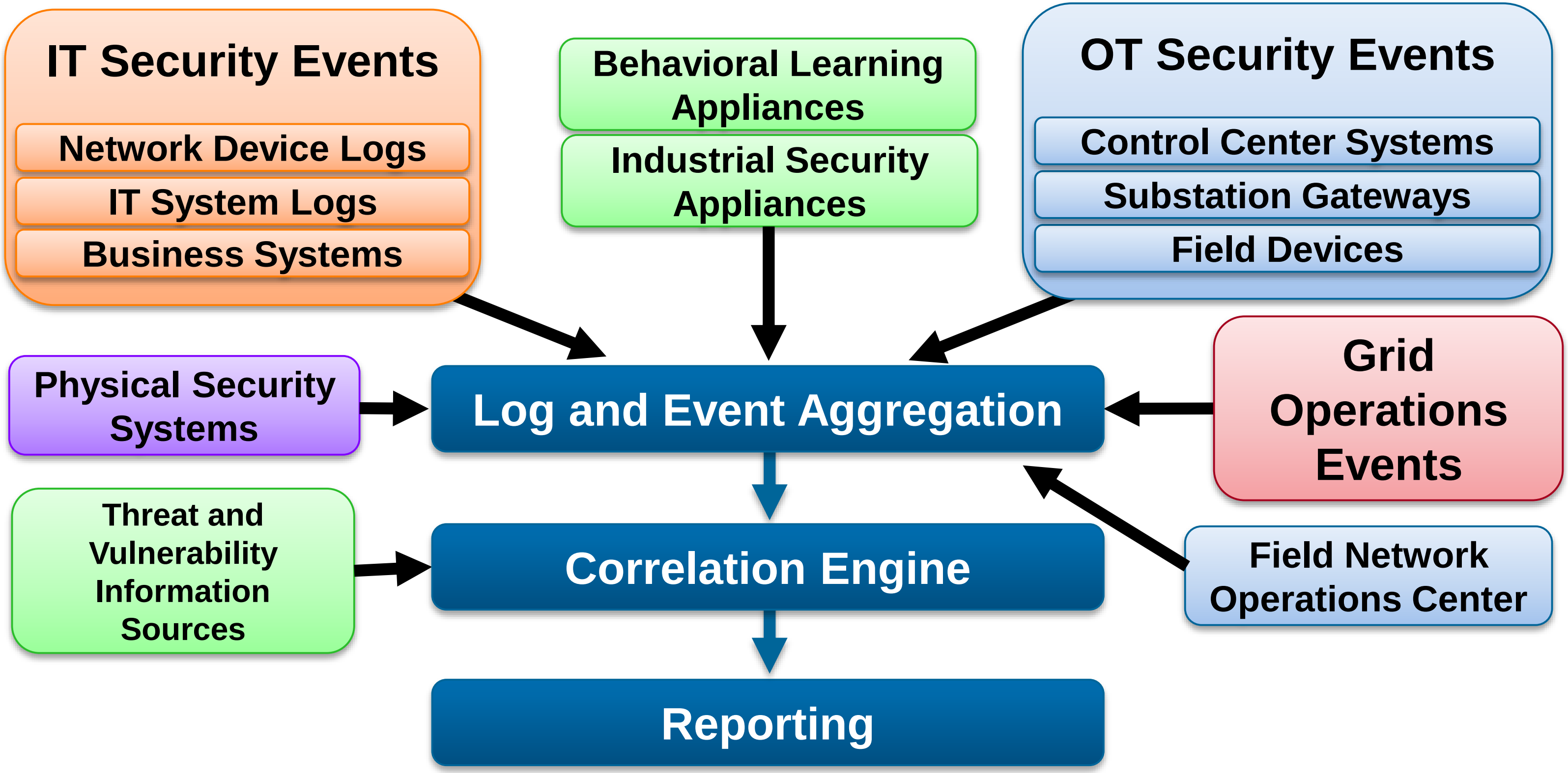
1:51 a.m. Police officers arrived, but found everything quiet. Unable to get past the locked fence and seeing nothing suspicious, they left.

3:15 a.m. A PG&E worker arrived to survey the damage

* https://en.wikipedia.org/wiki/Metcalf_sniper_attack

How quickly can utilities correlate these events with Siloed Monitoring and Analysis?

Integrated Security Operations Center (ISOC)



IT Security Events

Network Device Logs

IT System Logs

Business Systems

Behavioral Learning Appliances

Industrial Security Appliances

OT Security Events

Control Center Systems

Substation Gateways

Field Devices

Physical Security Systems

Log and Event Aggregation

Grid Operations Events

Threat and Vulnerability Information Sources

Correlation Engine

Field Network Operations Center

Reporting

Security Information and Event Management (SIEM)

What Are Security Metrics?

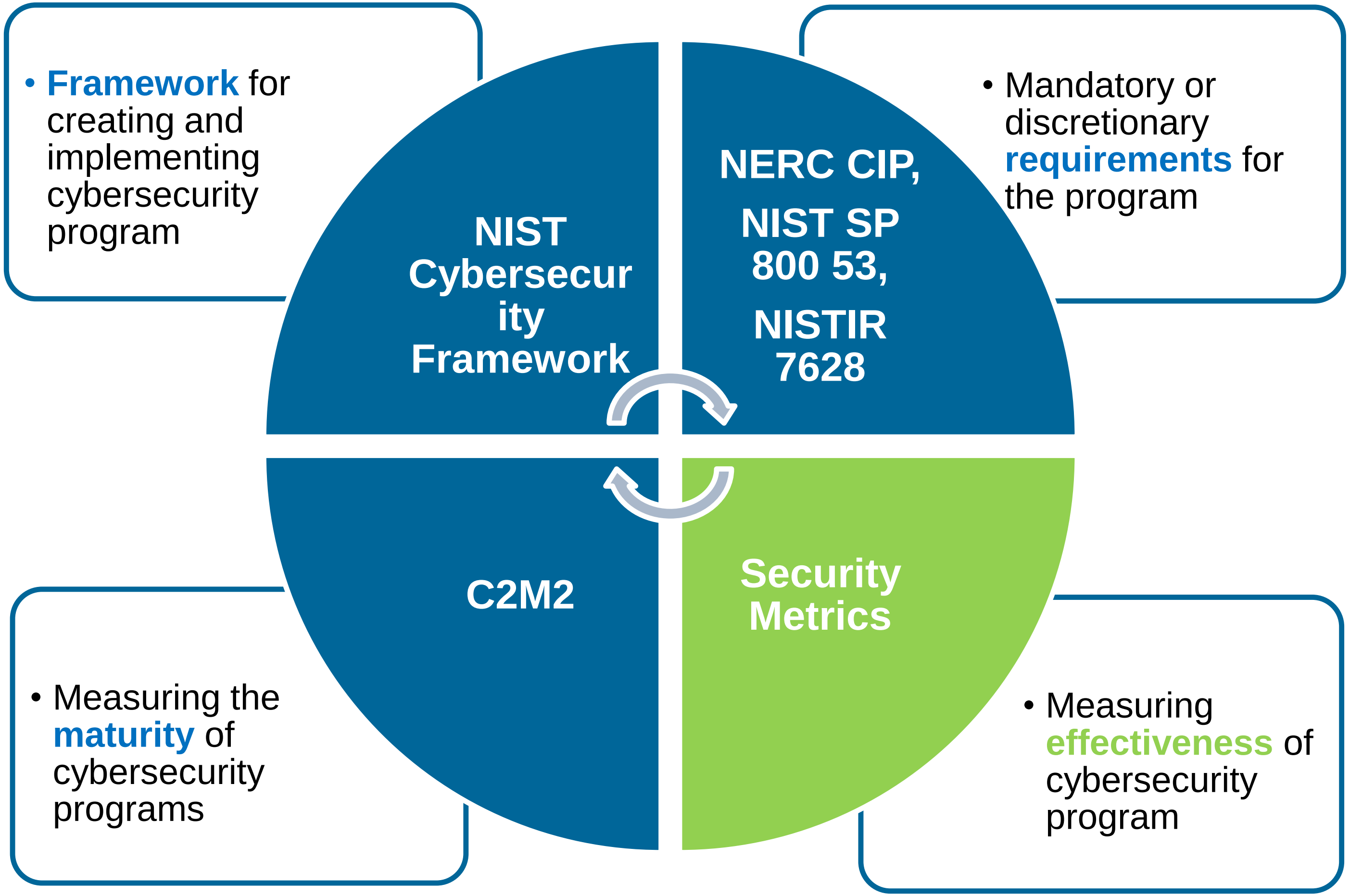
Numbers

representing

the **EFFECTIVENESS** of

security controls

Security Metrics – Where does it fit?



- **Framework** for creating and implementing cybersecurity program

NIST Cybersecurity Framework

- Mandatory or discretionary **requirements** for the program

NERC CIP,

NIST SP 800 53,

NISTIR 7628

C2M2

- Measuring the **maturity** of cybersecurity programs

Security Metrics

- Measuring **effectiveness** of cybersecurity program

Why Do We Need Security Metrics?

Security Team

- To find out what works and what does not work
- To communicate security posture, threats, and risks
- To demonstrate value of their work

IT/OT Management

- Make sound decisions on security technology, resource allocation, etc.
- To trend the effectiveness of security controls over time
- Make recommendations to senior management on security priorities

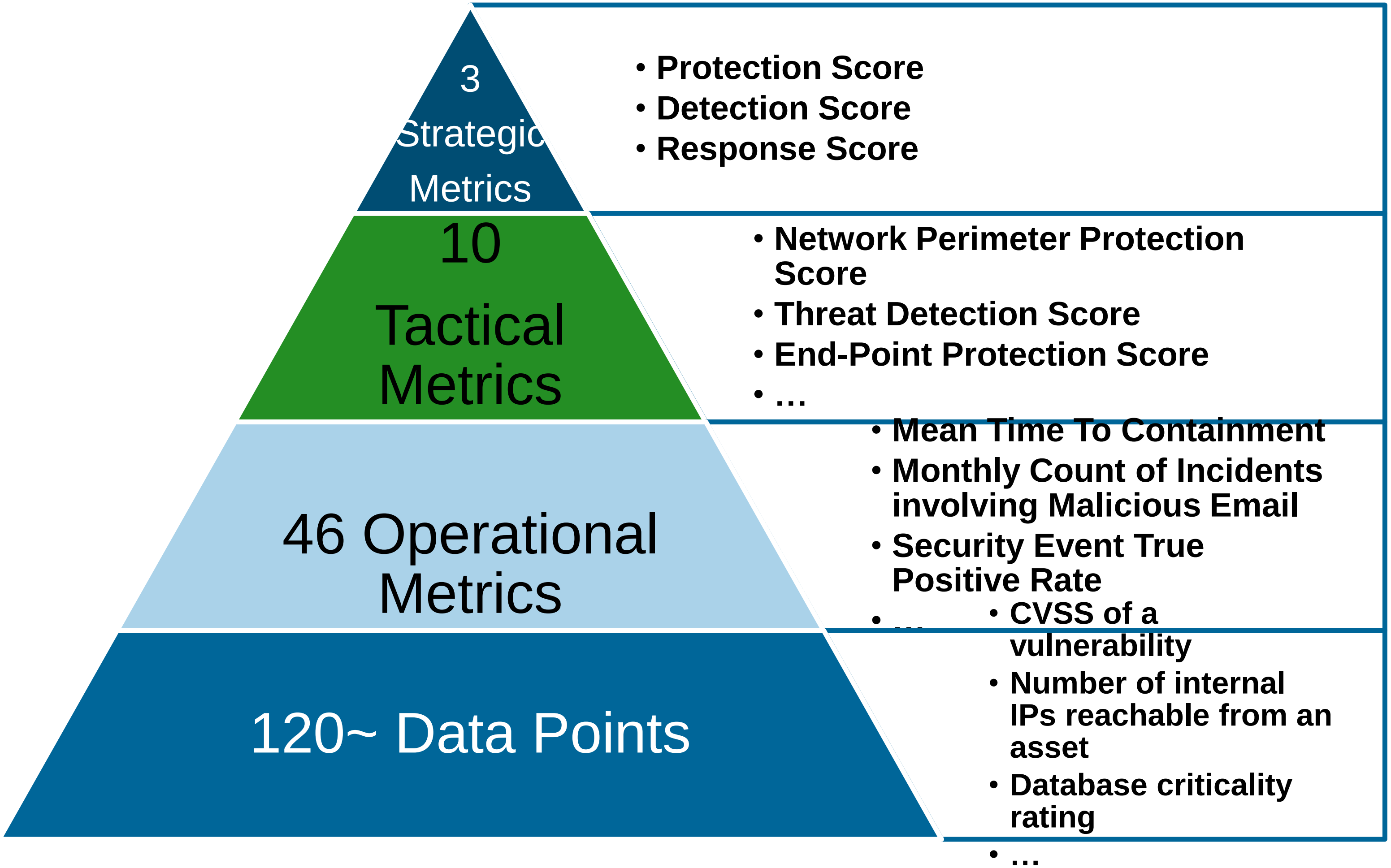
Senior Management / The Board

- Assess the cyber security risk
- Make strategic decisions on cyber security risk management

Stakeholders

- "Is our data secure?"
- "Is our power grid secure?"

Recap: EPRI’s Security Metrics



3 Strategic Metrics

- Protection Score
- Detection Score
- Response Score

10 Tactical Metrics

- Network Perimeter Protection Score
- Threat Detection Score
- End-Point Protection Score
- …

46 Operational Metrics

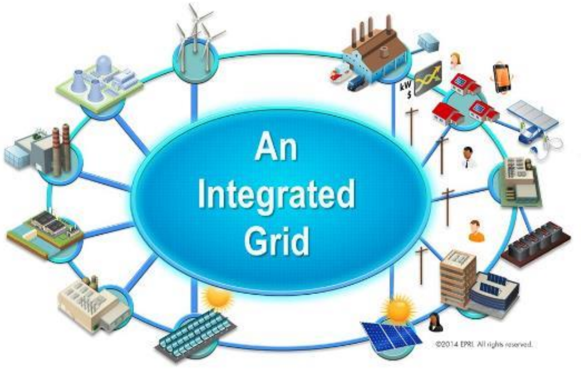
- Mean Time To Containment
- Monthly Count of Incidents involving Malicious Email
- Security Event True Positive Rate
- …

120~ Data Points

- CVSS of a vulnerability
- Number of internal IPs reachable from an asset
- Database criticality rating
- …

Cyber Security Challenges for the Multi-Party Grid

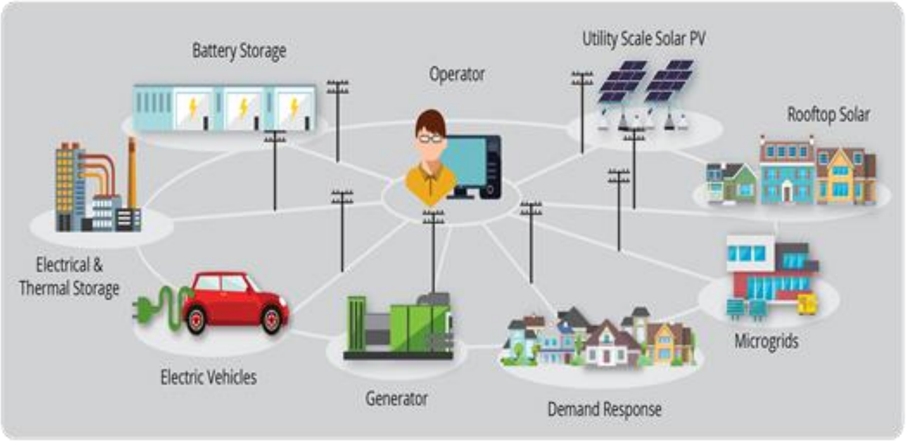
- Generation and storage assets may not be owned or operated by the utility
- Energy generation/consumption can be controlled by an aggregator
- Technology and business services are performed by third parties
- Operating increasingly complex, interconnected systems
- Dynamic governance relationships



How should the industry address these challenges?

The Path Forward

- Multi-Party Grid Risk Model
- Framework for Collaborative Security Management
- Cyber Security Guidelines for DER Integration
- Light-weight Encryption
- Simple Certificate or Cryptographic Key Management Scheme
- Cloud Security for Cyber-Physical Systems



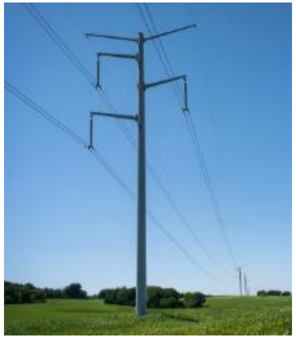
Together…Shaping the Future of Electricity

ERIC HERR

Ameren
ILLINOIS

The Human Factor: Challenges and Opportunities

NextGrid WG3 | 05.11.2018



Eric Herr | Director Cybersecurity Operations

Ameren
FOCUSED ENERGY. For life.

Institutionalizing Cybersecurity

Current State

- Mandatory training
- Simulations
- Functional scorecards
- Awareness campaigns

Opportunities

- Gamification - make training fun
- Incentivize secure behaviors
- Include cybersecurity curriculum in all degree programs
- Partner with the trades to develop competencies in apprenticeship programs

Developing a Security Mindset

Current State

- Organizational boundaries exist between IT and OT
- Heavy reliance on network segmentation for security
- Different security technologies in IT and OT operated by different teams
- Situational awareness gaps

Opportunities

- Integrate IT/OT operations
- Reduce technical debt
- Align roles and responsibility by competency
- Develop the hunting discipline
- Career rotations within government and industry agencies

Threat Intelligence and Adversary Behavior

Current State

- Labor intensive process
- Heavy focus on static indicators of compromise
- Little orchestration of threat data across technology
- Lack of security clearance prohibits access to timely threat intelligence data

Opportunities

- Threat and vulnerability is primed for automation and RPA use cases
- Analysts focus on adversary tradecraft, not static indicators
- Lobby to reduce dwell time on clearances
- Expand programs such as DOE CRISP and others to all utilities

Educating the Customer

Current State

- Little direct communication to customers regarding security of IoT devices
- Consumer IoT device configurations are not secure out of the box and updates can be complicated

Opportunities

- As an industry, we should educate consumers on risks associated with IoT devices
- Include cybersecurity curriculum in primary and secondary education
- Evolve the cybersecurity awareness campaign at the state level

Building a Cybersecurity Workforce

Opportunities

- Develop recruiting pipelines into universities and military
- Encourage and support a diverse cybersecurity workforce
- Support and participate with innovation hubs, hackathons, summer camps and other mentoring opportunities at all levels of education
- Create an exciting, dynamic workspace
- Incentivize professional growth
- Broaden adoption of cybersecurity scholarships
- Support apprenticeships as entry to cybersecurity careers

DISCUSSION FORMAT

Purpose: Describe challenge, identify opportunities, suggest solutions, and propose action items.

Participant Feedback: <u>Let us know if this discussion format is not optimal</u>

WebEx Protocol:

- Raise hand or send chat message to let host know you have a comment or question
- Host will notify who has the floor and who is on deck

WORKING GROUP

PEOPLE DISCUSSION

PEOPLE OVERVIEW

Challenges	Opportunities	Solutions	Education	Potential Action Items
1. Ensuring a collaborative and consistent approach towards achieving a higher level of cyber and physical security	Building resiliency throughout ecosystem; growing employee skillset	Capability measurement: a. Baseline and advanced capabilities b. Drivers' license type certification	Achieving a baseline level of cyber and physical security competency among all personnel	*[input sought, if any]*
2. Improve mindset and institutional culture to optimize problem solving capabilities and avoid the "failure of imagination"	Growing security subject matter expertise, aging workforce/turnover	Avoid sensory data overload through use of tools like machine learning, data visualization	" " "	" " "
3. Streamlining data sharing, security clearance, access to necessary intelligence while balancing the need to protect critical infrastructure information	Expedite security clearances (which currently take 18+ months to process) and real-time intel sharing.	Expedite credible and accurate threat intel sharing through: (1) improvement of government declassification of information and (2) improvement of processes for sharing of information	" " "	" " "
4. Fully understanding adversary behavior: tactics, capabilities, tools, strategies, growing sophistication, identity of the adversaries; including insider threats	" " "	" " "	" " "	" " "
5. Fully understanding stakeholder expectations	Engaging all customers in addressing security challenges, community buy-in.	Defining customer role in ensuring security; understanding true customer reliability expectations and cost sensitivity, including among different customer types (e.g. residential, business, CI)	" " "	" " "
6. Overcoming inadequate cybersecurity workforce	Moving to 24/7 cybersecurity workforce	Attracting/retaining talent; Automation, AI, to support and enhance human capital; marketing breadth of opportunities; fully utilizing existing programs such as hackathons	Multidisciplinary approach required, educational pipeline insufficient bandwidth; university level education, short courses, summer schools	Communicating an inspirational vision (e.g. how to get people excited about internship at utility v. Apple or NASA)

PEOPLE #1 – 2

Challenges	Opportunities	Solutions	Education	Potential Action Items
1. Ensuring a collaborative and consistent approach towards achieving a higher level of cyber and physical security	Building resiliency throughout ecosystem; growing employee skillset	Capability measurement: a. Baseline and advanced capabilities b. Drivers' license type certification	Achieving a baseline level of cyber and physical security competency among all personnel	*[input sought, if any]*
2. Improve mindset and institutional culture to optimize problem solving capabilities and avoid the "failure of imagination"	Growing security subject matter expertise, aging workforce/turnover	Avoid sensory data overload through use of tools like machine learning, data visualization	" " "	" " "

PEOPLE #3 – 4

Challenges	Opportunities	Solutions	Education	Potential Action Items
3. Streamlining data sharing, security clearance, access to necessary intelligence while balancing the need to protect critical infrastructure information	Expedite security clearances (which currently take 18+ months to process) and real-time intel sharing.	Expedite credible and accurate threat intel sharing through: (1) improvement of government declassification of information and (2) improvement of processes for sharing of information	" " "	" " "
4. Fully understanding adversary behavior: tactics, capabilities, tools, strategies, growing sophistication, identity of the adversaries; including insider threats	" " "	" " "	" " "	" " "

PEOPLE #5 – 6

Challenges	Opportunities	Solutions	Education	Potential Action Items
5. Fully understanding stakeholder expectations	Engaging all customers in addressing security challenges, community buy-in.	Defining customer role in ensuring security; understanding true customer reliability expectations and cost sensitivity, including among different customer types (e.g. residential, business, CI)	" " "	" " "
6. Overcoming inadequate cybersecurity workforce	Moving to 24/7 cybersecurity workforce	Attracting/retaining talent; Automation, AI, to support and enhance human capital; marketing breadth of opportunities; fully utilizing existing programs such as hackathons	Multidisciplinary approach required, educational pipeline insufficient bandwidth; university level education, short courses, summer schools	Communicating an inspirational vision (e.g. how to get people excited about internship at utility v. Apple or NASA)

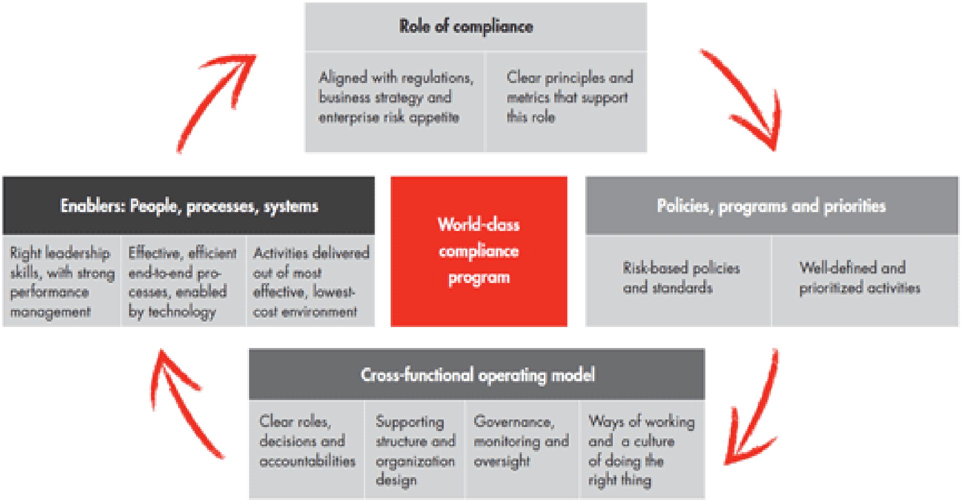
BREAK

5 MINUTES

WORKING GROUP
PROCESS DISCUSSION

PROCESS

Figure 2: High-performing compliance organizations focus on four key elements



Role of compliance

- Aligned with regulations, business strategy and enterprise risk appetite
- Clear principles and metrics that support this role

Policies, programs and priorities

- Risk-based policies and standards
- Well-defined and prioritized activities

Cross-functional operating model

- Clear roles, decisions and accountabilities
- Supporting structure and organization design
- Governance, monitoring and oversight
- Ways of working and a culture of doing the right thing

Enablers: People, processes, systems

- Right leadership skills, with strong performance management
- Effective, efficient end-to-end processes, enabled by technology
- Activities delivered out of most effective, lowest-cost environment

World-class compliance program

Source: Bain & Company

NextGrid Illinois

PROCESS OVERVIEW

Challenges	Opportunities	Solutions	Education	Potential Action Items
1. Encouraging industry to gravitate toward adoption of a standardized set of approaches to increase operational efficiency	Trend towards adopting business practices even when not required because they make sense and are effective (e.g. NERC CIP, NIST, C2M2). Maturing risk management programs. DOE cybersecurity risk management process (RMP).	Formalize processes to certify people in best-practice use when interacting with OT and IT	*[input sought, if any]*	*[input sought, if any]*
2. Effectively measuring vendor capabilities, practices, and competencies when introducing their products into grid operations (including multiple tiers in the supply chain)	Securing supply chain and ensuring vendors incorporate and integrate security protection capabilities	Building resiliency throughout ecosystem; Supply chain security: Cloud, 3rd Party, and Consumer-grade Products	" " "	" " "
3. Address need for metrics to quantify effectiveness of interventions	Adoption of risk assessment and capability maturity models. Third-party assessment and continuous improvement.	Establish metrics for reliability, resiliency, and cybersecurity	" " "	" " "
4. Promoting an integrated return on investment strategy that includes physical and cyber security management (workforce, technology, process)	Ensuring security planning is incorporated in strategic planning and business processes; Potential valuation of resilience attributes in transmission planning	Incorporating change management into overall project plans	" " "	" " "
5. Harmonizing framework adoption for: information sharing, incident response management, and contingency planning/analysis criteria	Promote increased cross-utility information sharing with regard to threat identification and incident response, complimentary to role of ISACs. Define need for information. Recognizing differing needs and goals.	Increased public private partnerships to facilitate information and best practices sharing. Enhancing operations across RTO seams (processes and tools); Responsive congestion management across RTO seams. Integrating emerging technologies to improve process.	" " "	" " "
6. Prioritizing effective, regular, and consistent evaluation and testing of core capabilities	Testing and exercising crisis and incident management capabilities across multiple jurisdictions	Exercise response capabilities through local, regional, and national coordinated exercises (CSIRT, GridEx, etc.)	" " "	Continued development of ESCC Cyber Mutual Assistance program to coordinate between utilities in the event of an attack

PROCESS #1 – 2

Challenges	Opportunities	Solutions	Education	Potential Action Items
1. Encouraging industry to gravitate toward adoption of a standardized set of approaches to increase operational efficiency	Trend towards adopting business practices even when not required because they make sense and are effective (e.g. NERC CIP, NIST, C2M2). Maturing risk management programs. DOE cybersecurity risk management process (RMP).	Formalize processes to certify people in best-practice use when interacting with OT and IT	*[input sought, if any]*	*[input sought, if any]*
2. Effectively measuring vendor capabilities, practices, and competencies when introducing their products into grid operations (including multiple tiers in the supply chain)	Securing supply chain and ensuring vendors incorporate and integrate security protection capabilities	Building resiliency throughout ecosystem; Supply chain security: Cloud, 3rd Party, and Consumer-grade Products	*" " "*	*" " "*

PROCESS #3 – 4

Challenges	Opportunities	Solutions	Education	Potential Action Items
3. Address need for metrics to quantify effectiveness of interventions	Adoption of risk assessment and capability maturity models. Third-party assessment and continuous improvement.	Establish metrics for reliability, resiliency, and cybersecurity	" " "	" " "
4. Promoting an integrated return on investment strategy that includes physical and cyber security management (workforce, technology, process)	Ensuring security planning is incorporated in strategic planning and business processes; Potential valuation of resilience attributes in transmission planning	Incorporating change management into overall project plans	" " "	" " "

NextGrid Illinois

PROCESS #5 – 6

Challenges	Opportunities	Solutions	Education	Potential Action Items
5. Harmonizing framework adoption for: information sharing, incident sharing, incident response management, and contingency planning/analysis criteria	Promote increased cross-utility information sharing with regard to threat identification and incident response, complimentary to role of ISACs. Define need for information. Recognizing differing needs and goals.	Increased public private partnerships to facilitate information and best practices sharing. Enhancing operations across RTO seams (processes and tools); Responsive congestion management across RTO seams. Integrating emerging technologies to improve process.	" " "	" " "
6. Prioritizing effective, regular, and consistent evaluation and testing of core capabilities	Testing and exercising crisis and incident management capabilities across multiple jurisdictions	Exercise response capabilities through local, regional, and national coordinated exercises (CSIRT, GridEx, etc.)	" " "	Continued development of ESCC Cyber Mutual Assistance program to coordinate between utilities in the event of an attack

NEXT
STEPS

NEXT STEPS

1. Whitepaper Sample and Template (WG Co-Leads and WG Members)
2. Submit content to Google Drive (WG Members and WG Co-Leads)
3. Review Priority Matrix and Remaining Topics Matrix (WG Members)
4. Distribute Regulatory & Compliance Matrices (WG Co-Leads)
5. Review and comment on notes from this session (WG Members)
6. Review and research topics for next session (WG Members)

FUTURE MEETINGS

FUTURE MEETINGS

Meeting #4 : **May 22, 2018 (WebEx 9AM-12PM)**

- **Regulatory and Compliance** (*and Any Carried Over Process Topics*)

NextGrid Public Policy Meeting: June 14, 2018

- Chicago 1PM-3:30PM
- Public participation and presentations from all Working Group Leads
- Optional 10AM-12Noon in-person WG3 meeting

Meeting #5 : June 25, 2018 (WebEx 12PM-3:30PM)

- WG Report Discussion (WebEx)

Final Chapter Due : **June 29, 2018**

NextGrid Illinois

THANK YOU