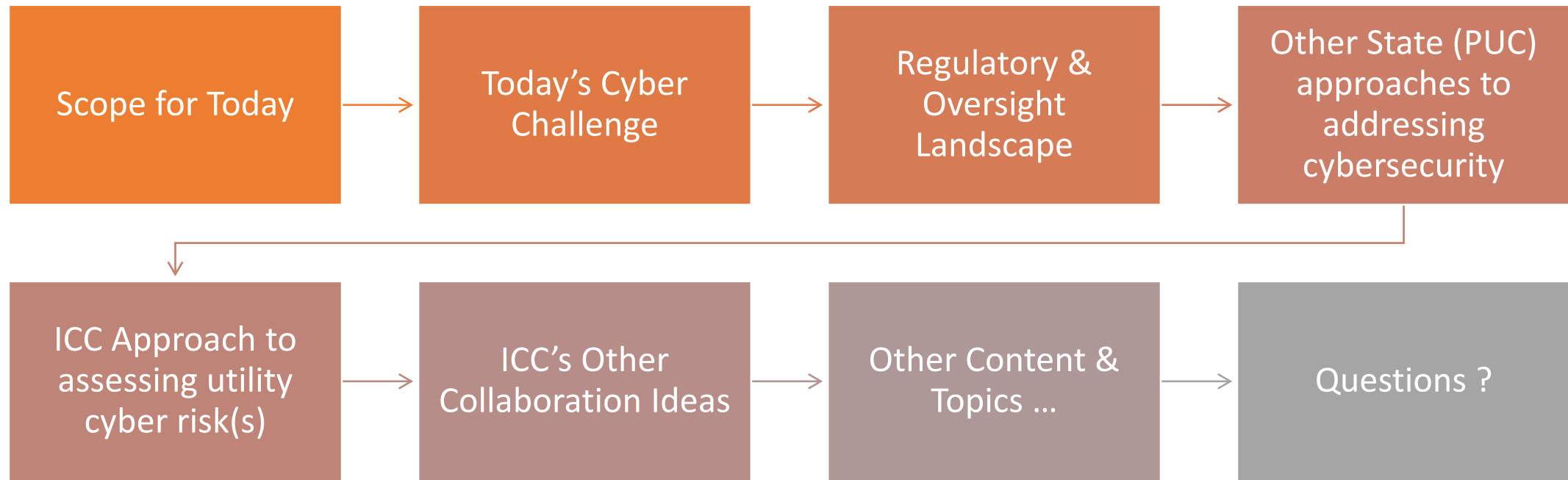


Today's Roadmap



Disclaimer

The views and opinions expressed herein strictly represent those of the presenter at this moment, and may not necessarily agree with positions of ICC Commissioners or Commission Staff. The presenter reserve the right to change those views and opinions as new information becomes available.

Nothing in this presentation should be interpreted as legal advice. You should accept legal advice only from a licensed legal professional with whom you have an attorney-client relationship. You should contact such a lawyer who may assist you in any matters to which you desire legal advice.

The views and opinions expressed herein strictly represent those of the presenters at this moment, and may not necessarily agree with positions of ICC Commissioners or Commission Staff. The presenters reserve the right to change those views and opinions as new information becomes available.

Nothing in this presentation should be interpreted as legal advice. You should accept legal advice only from a licensed legal professional with whom you have an attorney-client relationship. You should contact such a lawyer who may assist you in any matters to which you desire legal advice.

Increasing complex
information rich
environment



Defining Risk & Risk Management

Risk: A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and may be avoided through preemptive action.

<http://www.businessdictionary.com/definition/risk.html>

Risk Management: Identification, analysis, assessment, control, and avoidance, minimization, or elimination of unacceptable risks.

An organization may use risk assumption, risk avoidance, risk retention, risk transfer, or any other strategy (or combination of strategies) in proper management of future events.

<http://www.businessdictionary.com/definition/risk-management.html>

Defining Cybersecurity

Cybersecurity is the concept of protecting information and technology systems from attacks, damages or unauthorized access.



Cybersecurity encompasses solutions against all sorts of breaches and hacking, including internal misuse, corporate espionage, ransomware, crypto-mining and denial of service attacks.

Due Care: Putting reasonable measures in place to protect assets or data.

Due Diligence: Ensuring that security measures remain sufficient to protect that assets or data.

Cybersecurity is only part of a holistic security risk and resilience effort that is required to protect people, assets, and operations.



Approaches to Address Risk

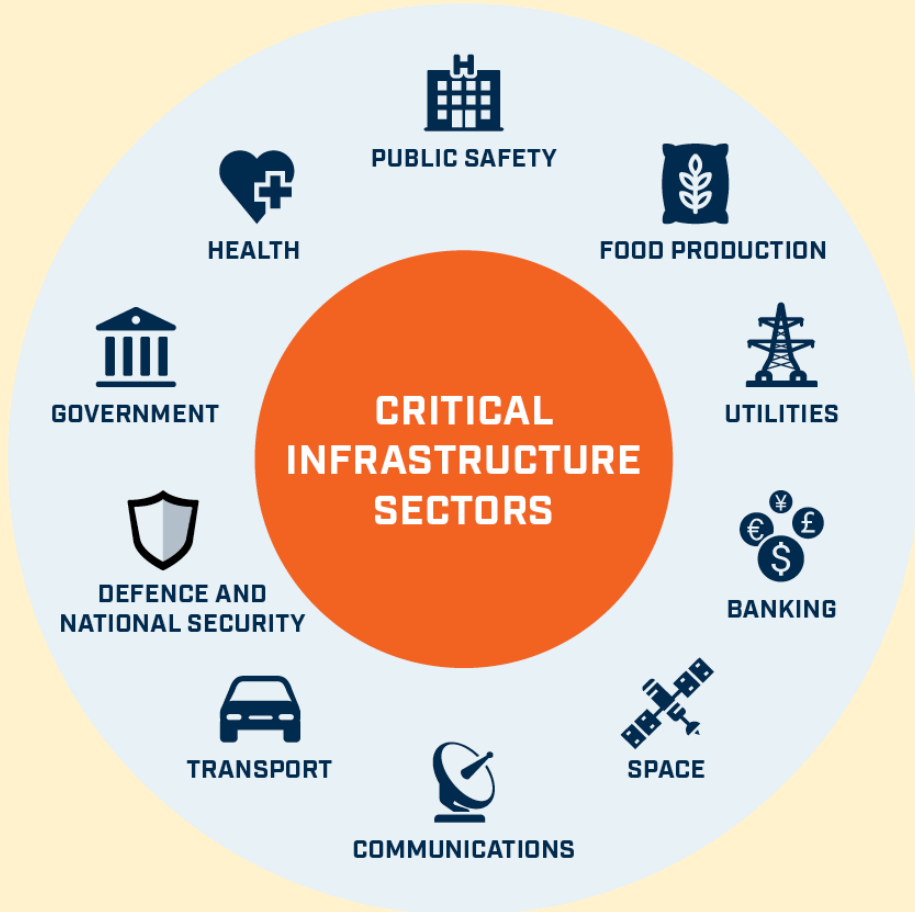
Compliance Based, Risk Based or a Combination?



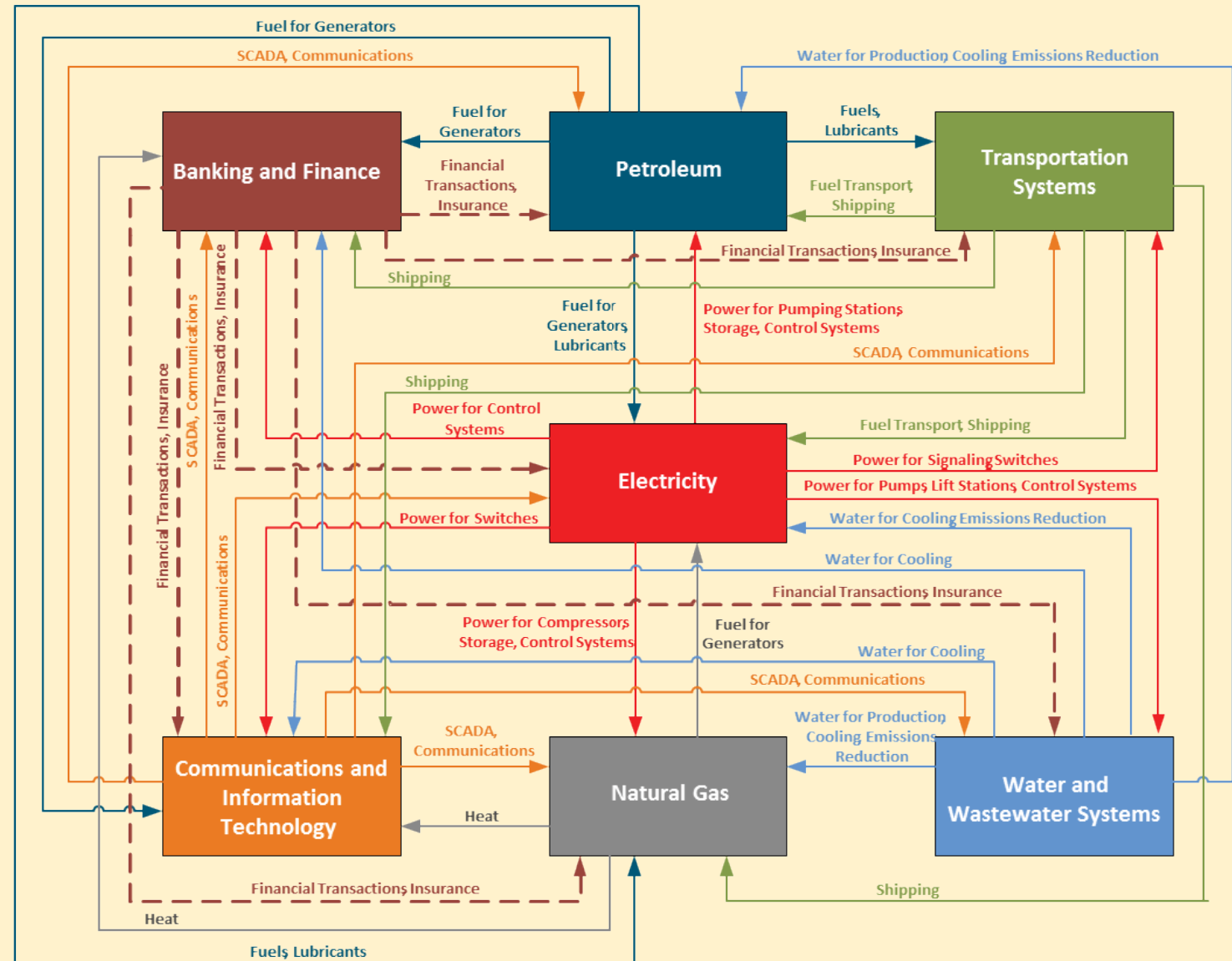
		PROBABILITY (Expected Frequency)				
		FREQUENT	LIKELY	OCCASIONAL	SELDOM	UNLIKELY
SEVERITY (Expected Consequence)		A	B	C	D	E
CATASTOPHIC	I	EH	EH	H	H	M
CRITICAL	II	EH	H	H	M	L
MODERATE	III	H	M	M	L	L
NEGLECTIBLE	IV	M	L	L	L	L

LEGEND: EH = extremely high risk, H = high risk, M = medium/moderate risk, L = low risk

The Interrelationships of Risk

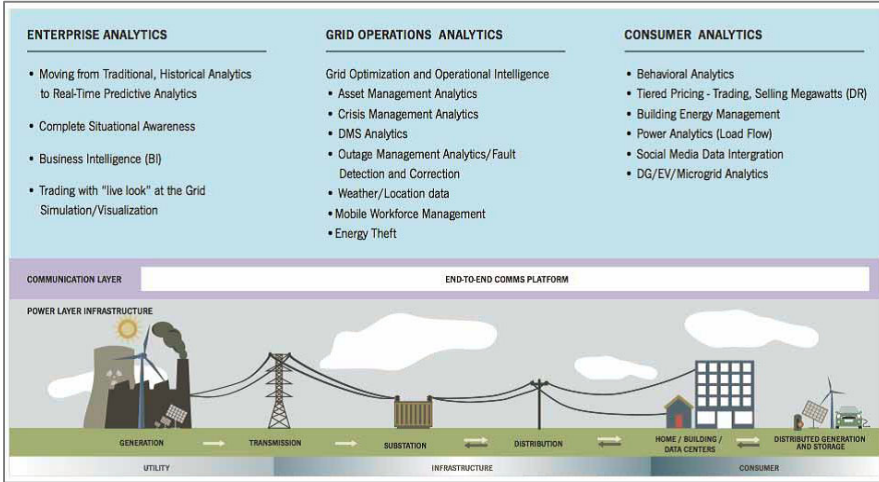


<https://www.huntsmansecurity.com/industries/critical-infrastructure/>



<https://www.hsaj.org/articles/14091>

Many Sources & Issues to Address



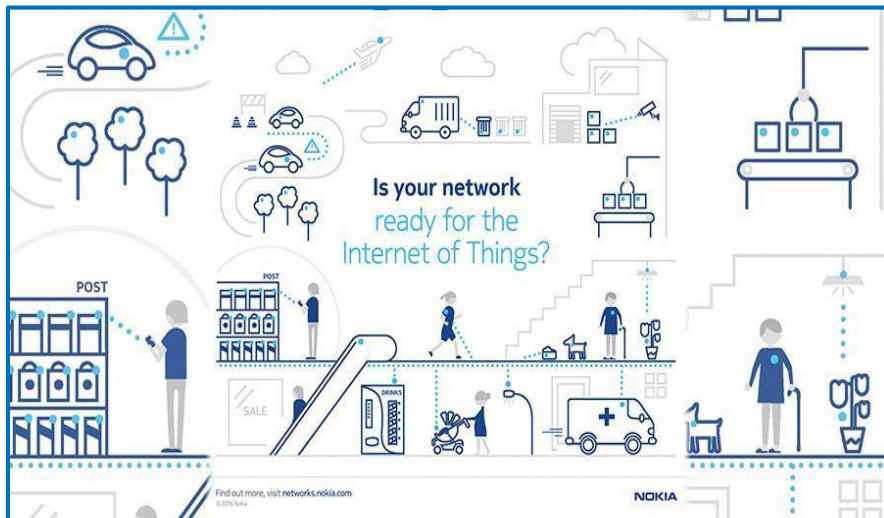
<https://www.einfochips.com/blog/shaping-up-analytics-for-the-smarter-grid/>



<https://telecom.economictimes.indiatimes.com/news/iot-initiatives-should-translate-into-business-models-across-sectors-telecom-secretary/64465285>



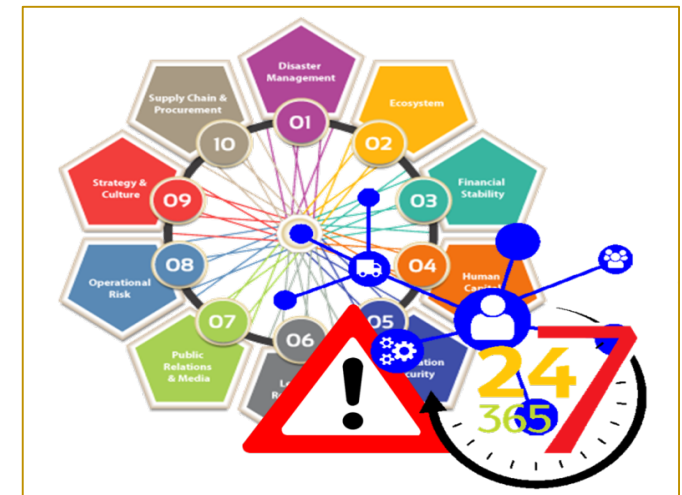
<https://castris.com/ransomware-cruda-realidad-internet-vs-bigdata-cloud-marketing-humo/>



<http://www.telecomreview.com/index.php/articles/telecom-vendors/1605-nokia-eases-iot-market-entry-for-mobile-operators>



<https://automation.isa.org/integrated-security-strategy-protect-industrial-assets/>



<https://www.enterrasolutions.com/blog/resiliency-and-supply-chain-risk-management/>

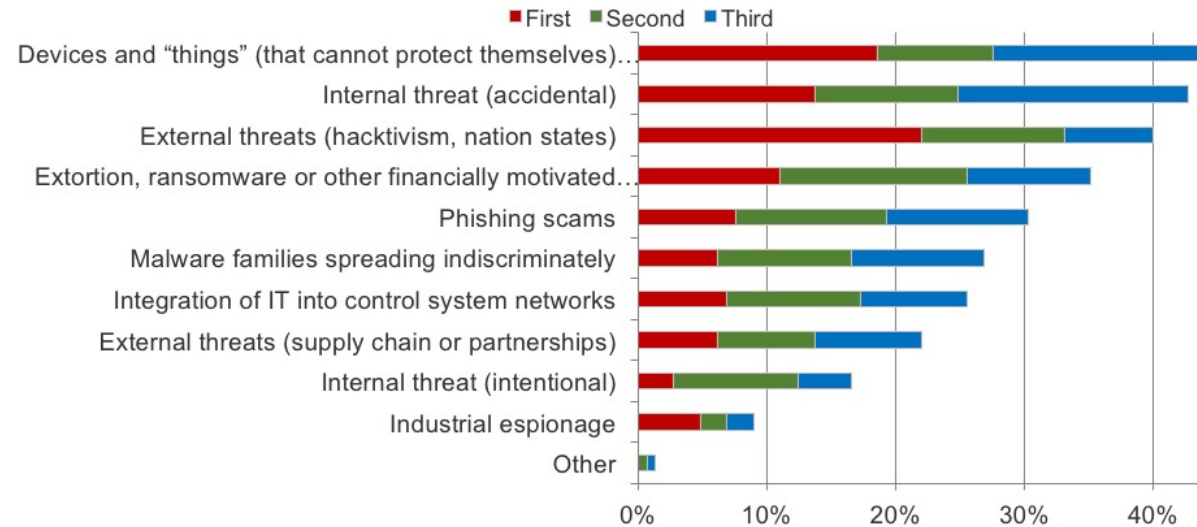
Threat Vectors

SANS
Analyst Program



THREAT VECTORS

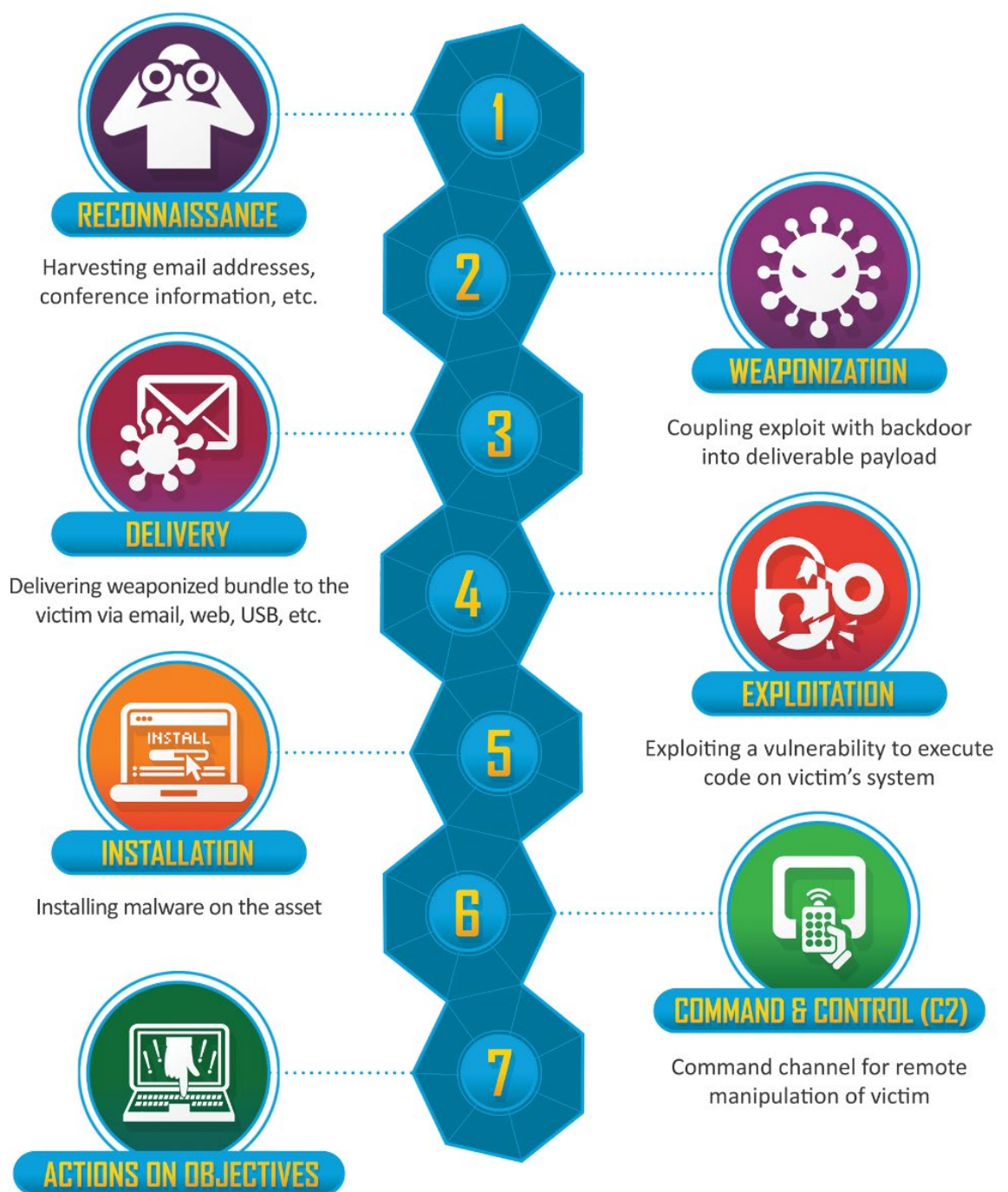
What are the top three threat vectors you are most concerned with? Rank the top three, with "First" being the threat of highest concern.



SANS

from the most trusted name in information security

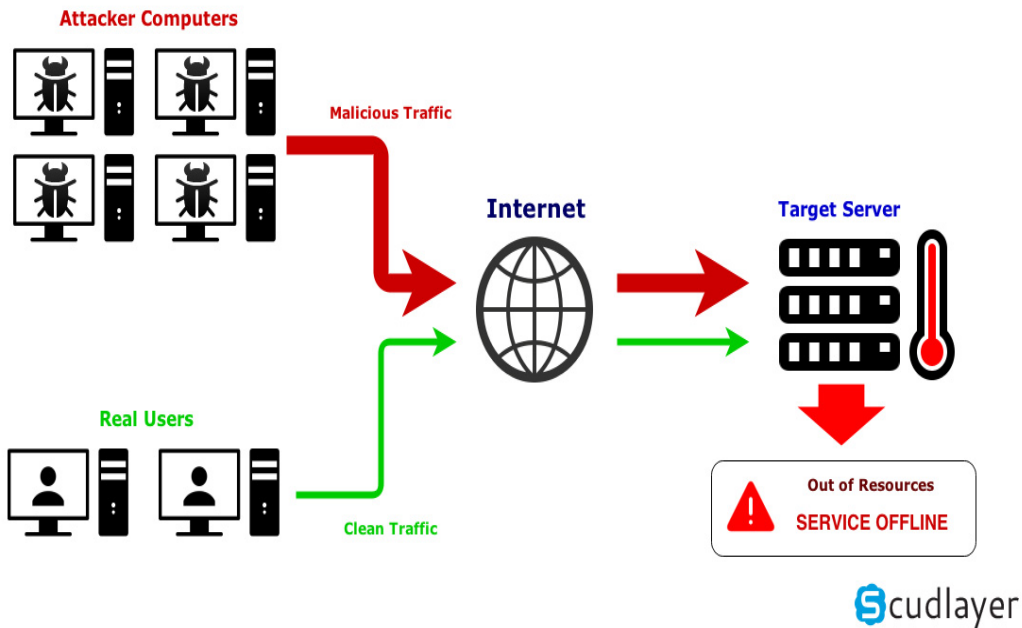
- A **cyber kill chain** is a collection of processes and steps related to the use of cyberattacks on systems. Some describe the cyber kill chain as representing the “stages” of a cyberattack and how they move to the next step. In general, the cyber kill chain is a step-by-step description of how a attack progresses toward its objective.



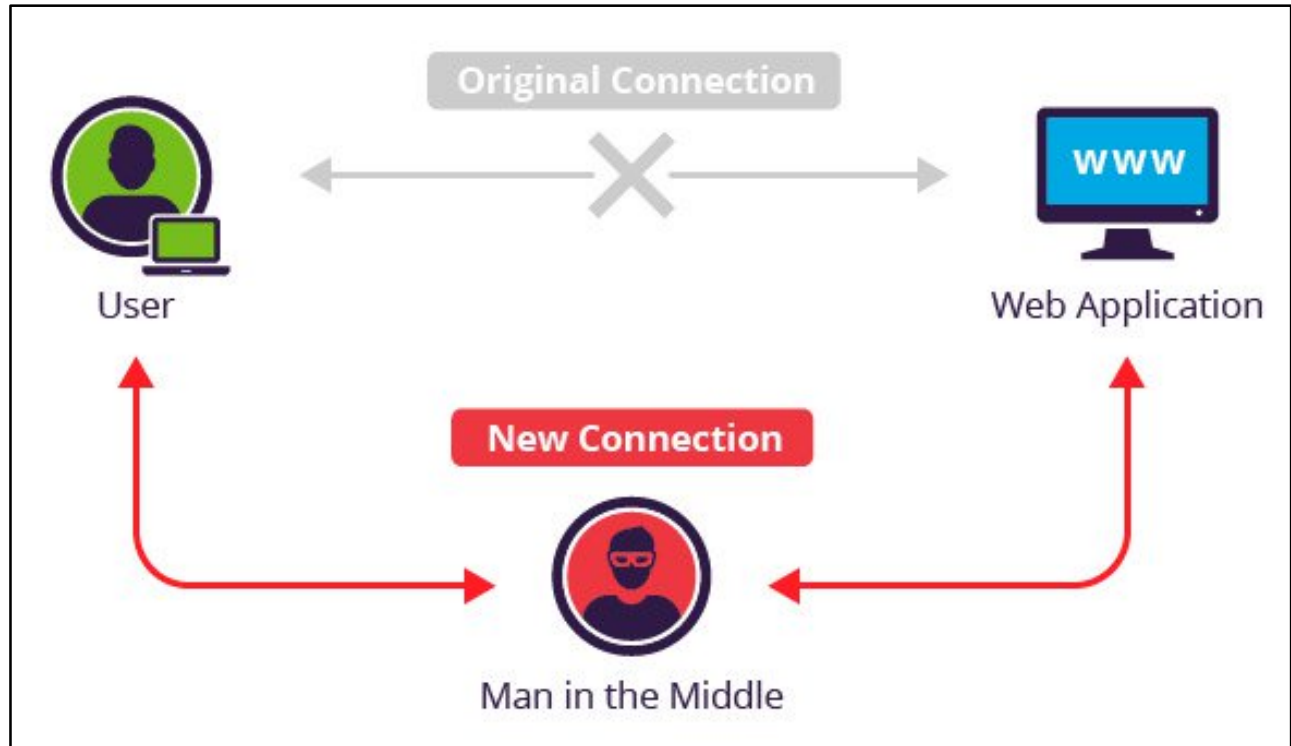
Communications Company Cyber Attack Challenges

Distributed Network Attacks are often referred to as **Distributed Denial of Service (DDoS) attacks**. This type of attack takes advantage of the specific capacity limits that apply to any network resources – such as the infrastructure that enables a company’s website. The DDoS attack will send multiple requests to the attacked web resource – with the aim of exceeding the website’s capacity to handle multiple requests... and prevent the website from functioning correctly.

Operation of a DDoS attack



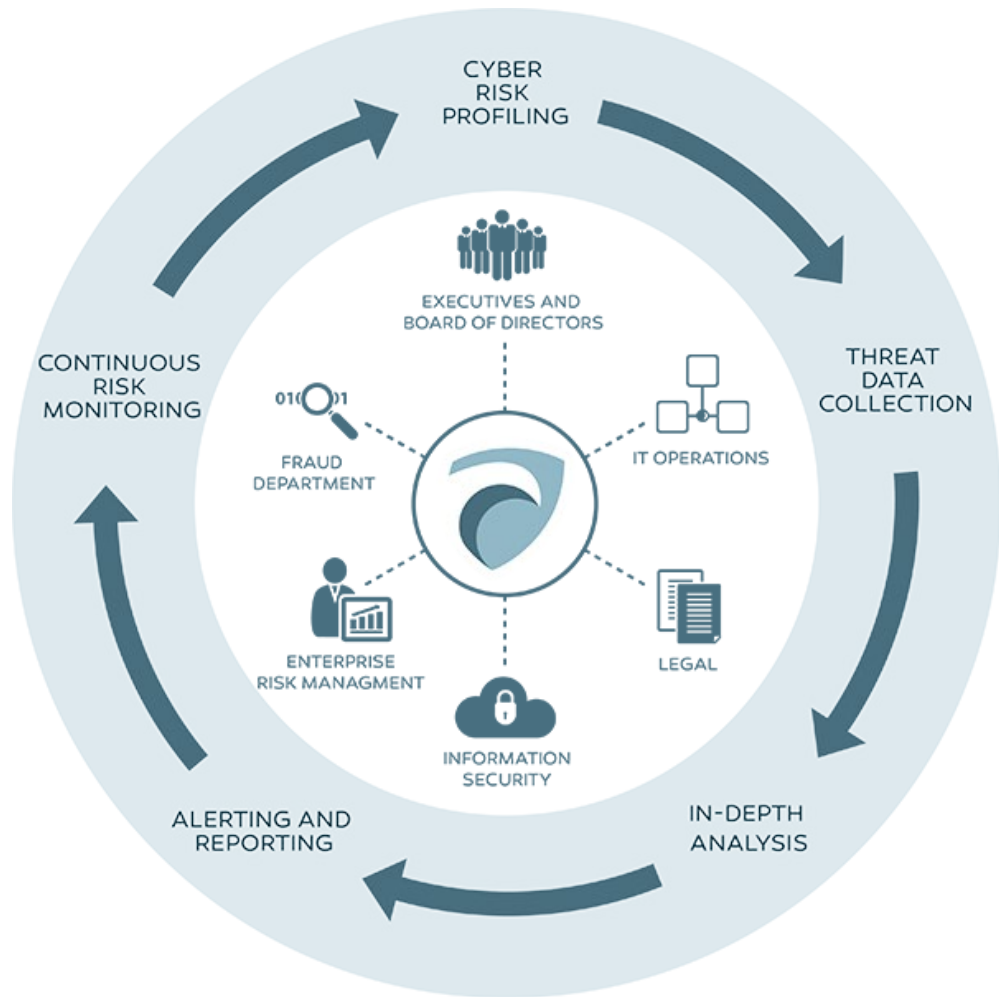
A **Man in the Middle (MitM)** attack occurs when a hacker inserts itself between the communications of a client and a server. Session hijacking is a common MitM attack - In this type of attack, an attacker hijacks a session between a trusted client and network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client.



<https://medium.com/@kapil.sharma91812/understanding-ddos-attack-15dd2cbce2a>

<https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>

Threat Intelligence



ANALYTICS

115+ MILLION
node graph-based analytics engine

340 MILLION
correlation relationships defined

OVER 600 TERABYTES
of analytics storage

212 PETABYTES
sensor traffic analyzed each month

45 BILLION URLS
analyzed each month

DATA SOURCES

Incident Response
Over 100,000 incident response hours/year
Hundreds of subject matter experts
across 16 countries

SENSORS
11 million sensors around the world
deployed across 60 countries
24x7x365 visibility through 6 worldwide SOCs

THREAT ANALYTICS
Billions of events processed each day

INTELLIGENCE

DETECTION
Identify threats that other solutions miss
7 million attacks detected each month
Discovered 19 out of 36 zero days

PROACTIVE
Stay a step ahead of the attacker by
understanding motivations and techniques
delivered across 40 technology partners
40+ targeted industry profiles

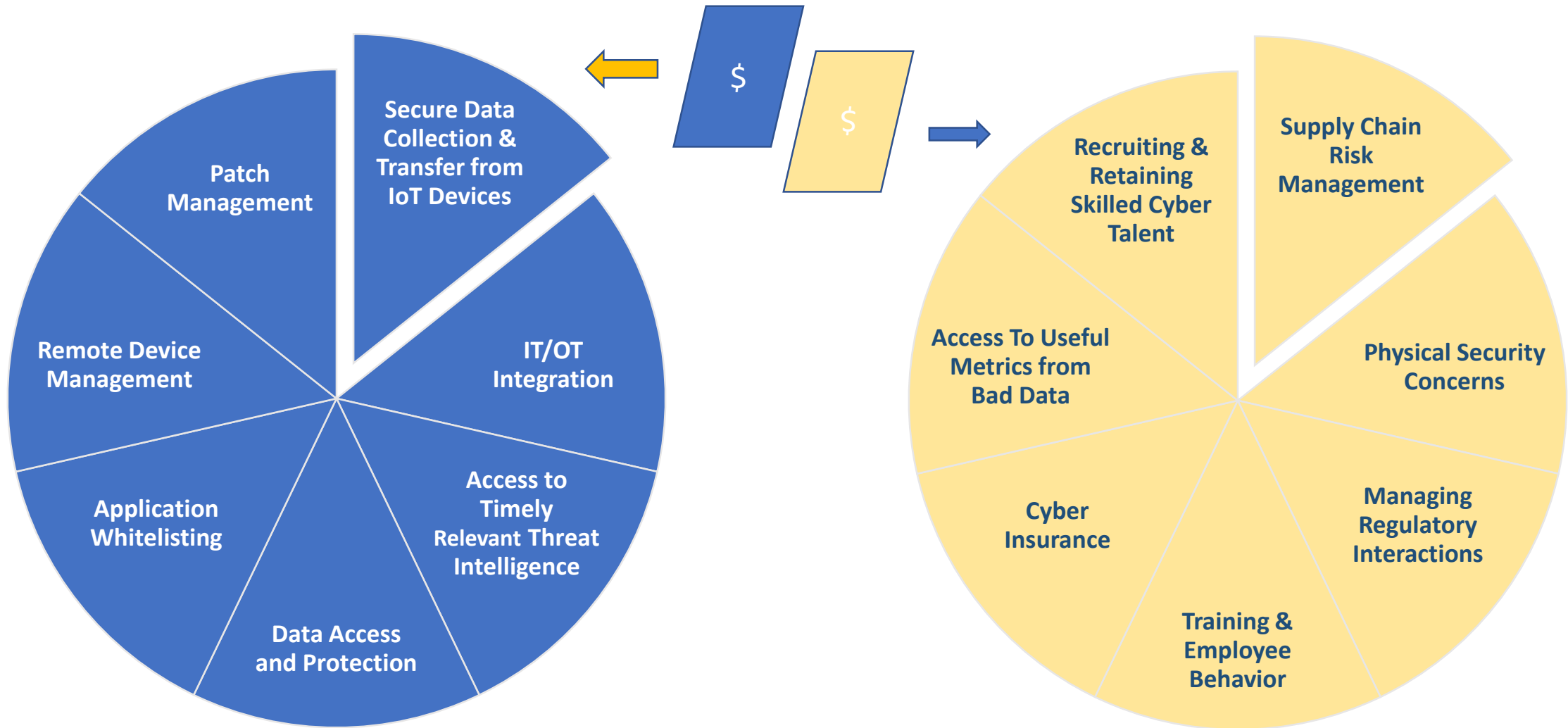
RESPONSE
Answer key questions and prioritize threats
based on attacker context
30+ advanced threat actors tracked
300+ advanced malware families tracked
10+ nation-state threat sponsor profiles

Who owns cyber defense ?



<https://www.oliverwyman.com/content/marsh/americas/us/en/campaigns/cyber-campaign.html>

Business Cyber Challenges





Regulatory &
Oversight
Landscape

PUCs - ICC & Cyber Risk



COMMISSIONS - U.S. state utilities commissions [URC, PUC or PSC] are typically governing bodies created to regulate the rates and services of public utilities operating in their respective jurisdictions (typically a state). They balance many factors including setting manageable rates, attracting investment and upgrade potential, reliability, resiliency and security of utilities.

ILLINOIS - In 2017, The Illinois Commerce Commission Created the Office of Cybersecurity and Risk Management to focus additional attention on the emerging risks posed by cyber threats to critical infrastructure in the electric, gas, water and telecommunications industries that operate and provide essential services to consumers and businesses within Illinois.

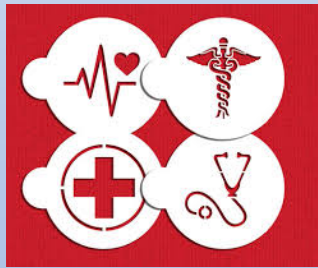
POLICIES - PUCs from states across the country are in various stages of actively assessing, directing, supporting and promoting economically appropriate measures be taken by utilities to ensure the reliability, resiliency and security of critical infrastructure in the electric, gas, water and telecommunications industries. These efforts should be consistent, adaptive and directed toward addressing the persistent and ongoing cyber threats to their operations and secure information.

**Many Factors
in Play within
a Public Utility
Commission**

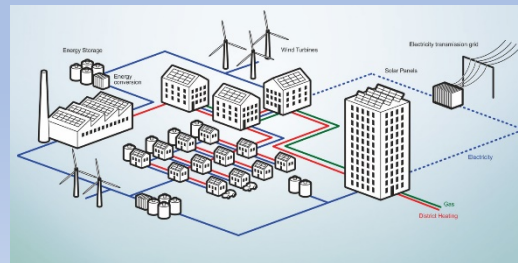
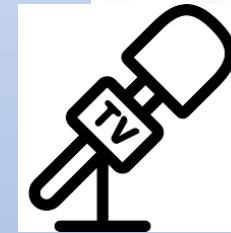


Complex Event Response Coordination

Event Response Planning - who is in charge of coordination during a crisis?



- Governmental entities
- Utilities
- First Responders (police, fire, national guard, etc.)
- Humanitarian Groups
- Businesses
- Military
- Medical
- Press, Social Media, etc.

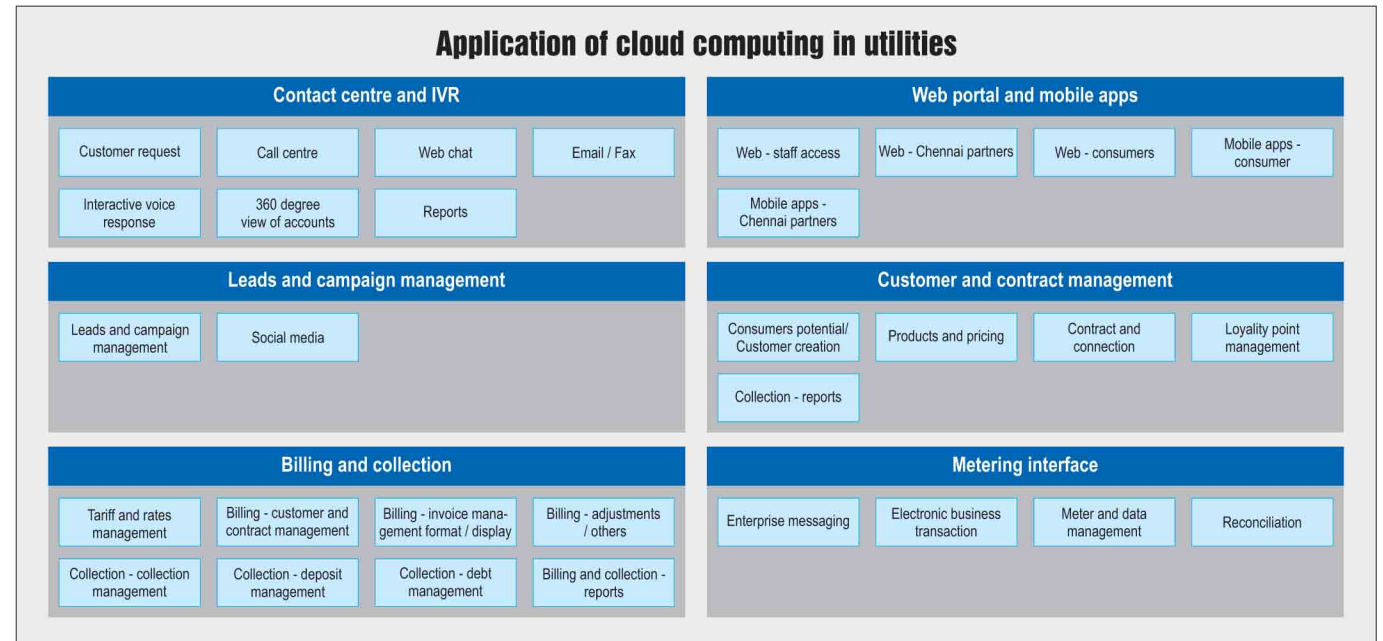


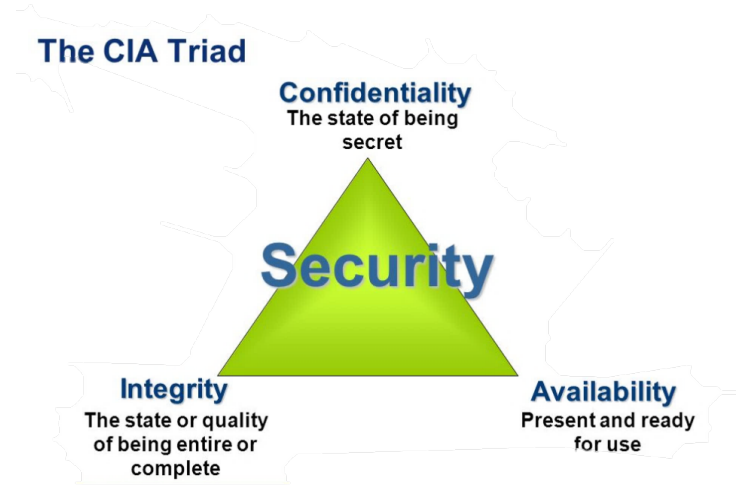
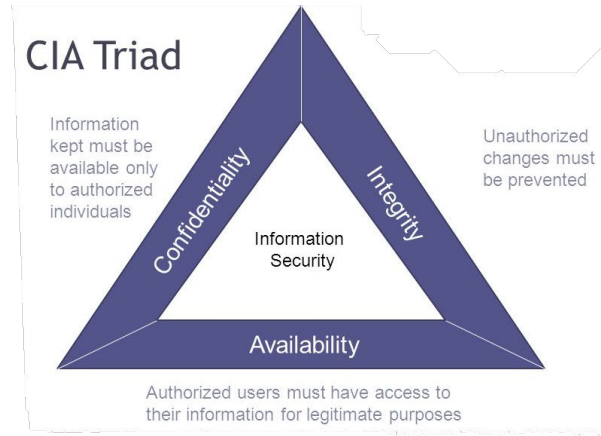
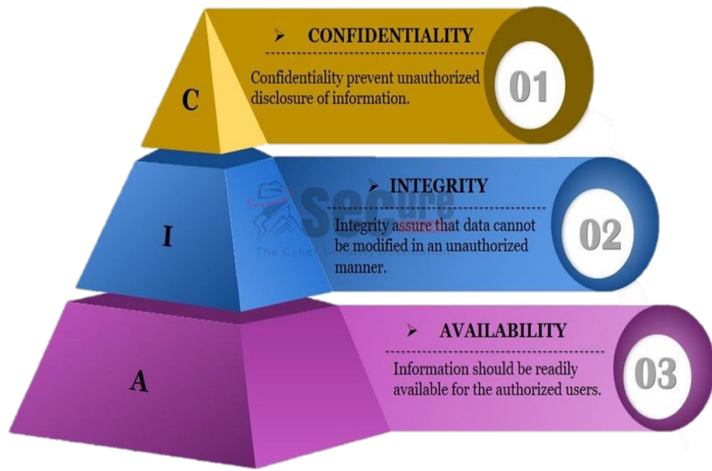
Cloud Computing Investment Decisions

NERC CIP v5 & v6 Impact OT Cloud Computing Decisions – Some Entities

NERC CIP v5 & v6 Impact OT Cloud Computing Decisions – Some Entities

NERC CIP v5 & v6 Impact OT Cloud Computing Decisions – Some Entities





Securing and Using Data

Assessment of Capabilities



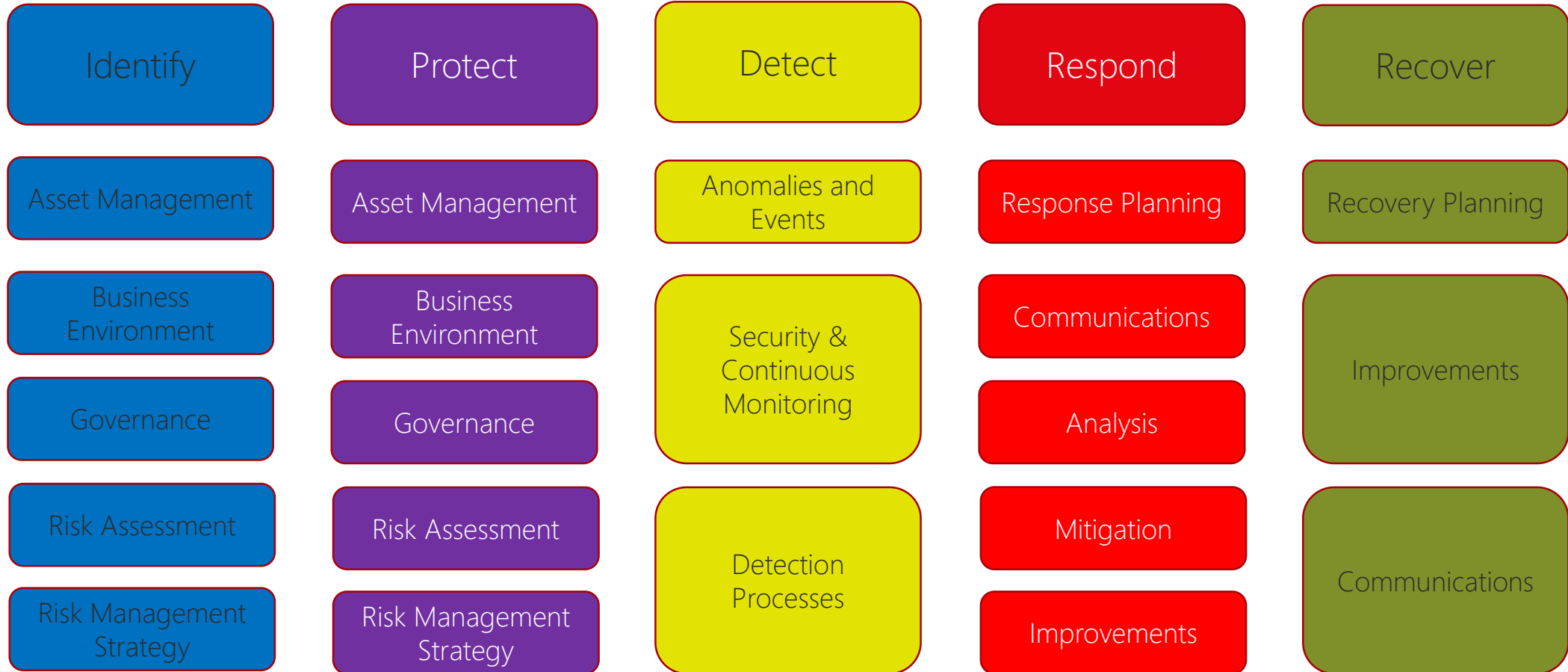
Assessment of Capabilities

Asking Good Questions

- Payload v. Threat Vector Emphasis – where do you fall
- Do you know everything that is connected to your network?
- How are you managing credentials?
- What is your employee risk knowledge focus?
- Are you adopting and implementing frameworks

Best Practice Adoption

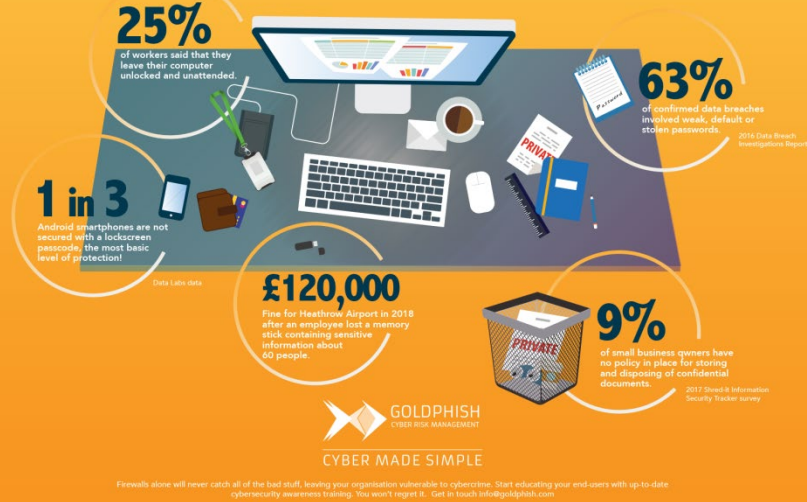
NIST Cybersecurity Framework (CSF)



Human Error(s)

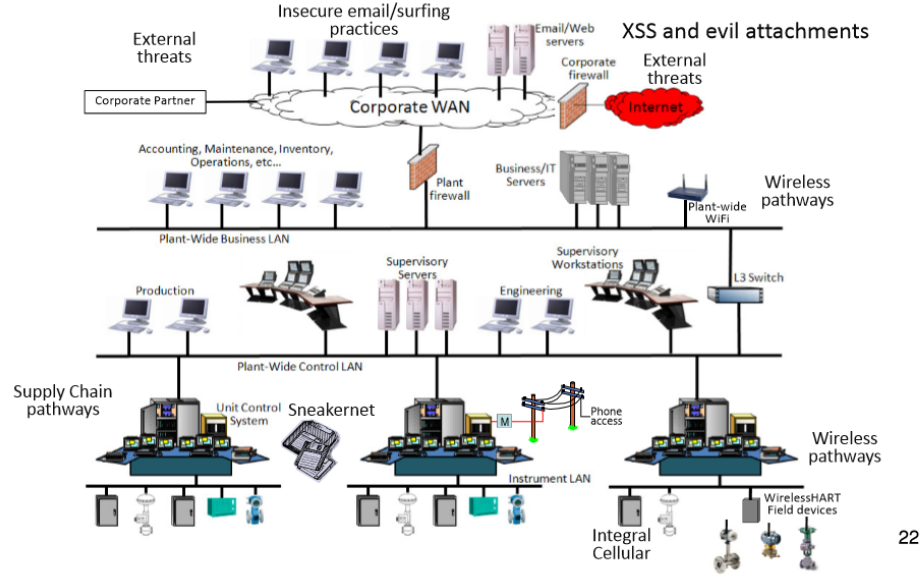
CYBER RISKS FROM EMPLOYEE BAD HABITS

A company's commitment to data security must start with formal, and visible, security policies and procedures. A cluttered workplace can lead to information breaches caused by human error.



<https://goldphish.com/clear-desk-clear-screen-reduces-cyber-risk/>

Potential Points of Attack



22

<https://formaspace.com/articles/it-computers/manufacturing-facility-cyber-attacks/>



<https://www.isdecisions.com/blog/it-security/insider-threats-banking-financial-institutions/>

ARE YOUR EMPLOYEES EDUCATED ABOUT CYBER-RISKS?

Require Security Training for All Employees

Human error plays one of the biggest roles in security breaches today. Nine in 10 companies now require this training to assess or improve security knowledge among their employees.

CIO INSIGHT

<https://www.cioinsight.com/security/slideshows/are-your-employees-educated-about-cyber-risks.html>

SOCIAL ENGINEERING

PROTECT YOUR ORGANIZATION FROM TARGETED SCAMS

1% OF EMPLOYEES ARE RESPONSIBLE FOR **75%** OF ENTERPRISE SECURITY RISK

WHAT IS SOCIAL ENGINEERING?

Social engineering refers to the practice of using non-technical methods to trick people into doing something they wouldn't normally do otherwise. Threat actors form relationships with targeted victims to get access to information or personal details that can be used to breach corporate networks, facilities, or accounts.

HOW IT WORKS

Prior to launching an attack, threat actors research details about targeted victims via publicly available information from the web and social media, or gather information on them from previous breaches, often purchased on the Dark Web.

Attackers use this information to construct highly convincing, customized messages (text, email, social media messages) that appear to be from a "trusted" source, such as a family member, friend, or colleague. These messages require some type of action on the victim's part, whether it is to open an attachment, fill out a form, click a link, or pass over money.

Example: You receive an email from someone who appears to be your uncle who says he is traveling abroad and lost his credit card. It is an emergency and he needs you to wire him money NOW. He sends you a link for the money transfer. Because you think your uncle is in trouble, you don't research the situation and send him the money. You find out the hard way you're out \$1,000.

Example: The Head of Human Resources receives an email with what appears to be a legitimate resume. However, it is laced with malicious code. Upon opening the attachment, her computer is infected, and the threat actor who sent the email now has access to her company's network.

35% OF EMPLOYEES HAVE CLICKED A LINK FROM AN UNKNOWN SENDER

3 MINUTES **60 PEOPLE** IN JUST THREE MINUTES, 60 PEOPLE CAN FALL VICTIM TO CYBERCRIME

55% ON AVERAGE, MORE THAN HALF OF A COMPANY'S PERSONNEL (WHICH SECURITY) HAVEN'T RECEIVED SECURITY AWARENESS TRAINING

MAJOR BREACHES ATTRIBUTED TO SOCIAL ENGINEERING

2011, RSA
Two groups of low-to-mid-level employees received spear phishing emails containing a malicious attachment. Once opened, it installed a backdoor into the corporate network, giving the attackers access to RSA's data.

\$66 MILLION

2013-2015, CARBANAK HEIST
The Carbanak Criminal Group sent spear phishing emails to employees at banks, IT payment systems, and financial institutions. Once opened, the emails infected the victims' computers with cybercriminals control of their computer and ultimately access to the networks of the victims' organizations.

UP TO \$1 BILLION

RECOMMENDATIONS

AWARENESS TRAINING
Awareness training should be mandatory for all employees. It should be refreshed regularly to keep employees up-to-date on the latest threats and best practices for avoiding them.

TRUST YOUR GUT
If you receive a message that seems suspicious, don't click on any links or attachments. If you're unsure, ask your IT department for help.

WATCH WHAT YOU POST
Be mindful of what you post on social media. Threat actors can use this information to build a profile of you and your organization.

WATCH ATTACHMENTS
Be cautious of attachments from unknown senders. If you receive an attachment from a contact, verify the sender's identity before opening it.

STAY STRONG
Do not be intimidated by a message. Report it to your IT department. If you receive a message that seems suspicious, do not click on any links or attachments.

Cyveillance
www.cyveillance.com

<https://www.lookingglasscyber.com/blog/threat-intelligence-insights/how-to-not-be-a-victim-of-social-engineering/>

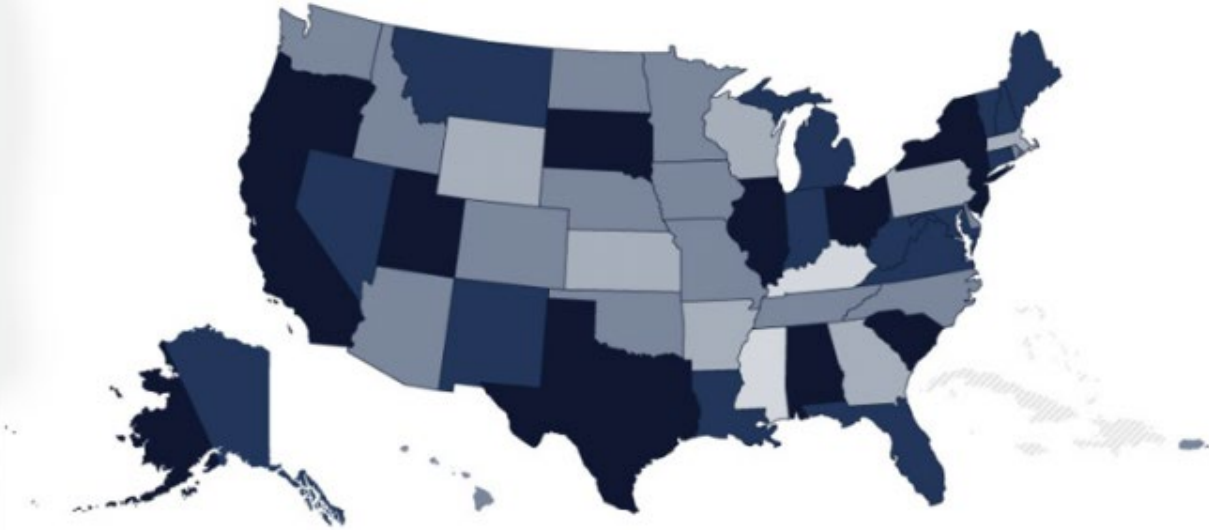
Reporting Requirements under 220 ILCS 5/4-101

The Commission shall require all public utilities to establish a security policy that includes on-site safeguards to restrict physical or electronic access to critical infrastructure and computerized control and data systems. The Commission shall maintain a record of and each regulated entity shall provide to the Commission an annual affidavit signed by a representative of the regulated entity that states:

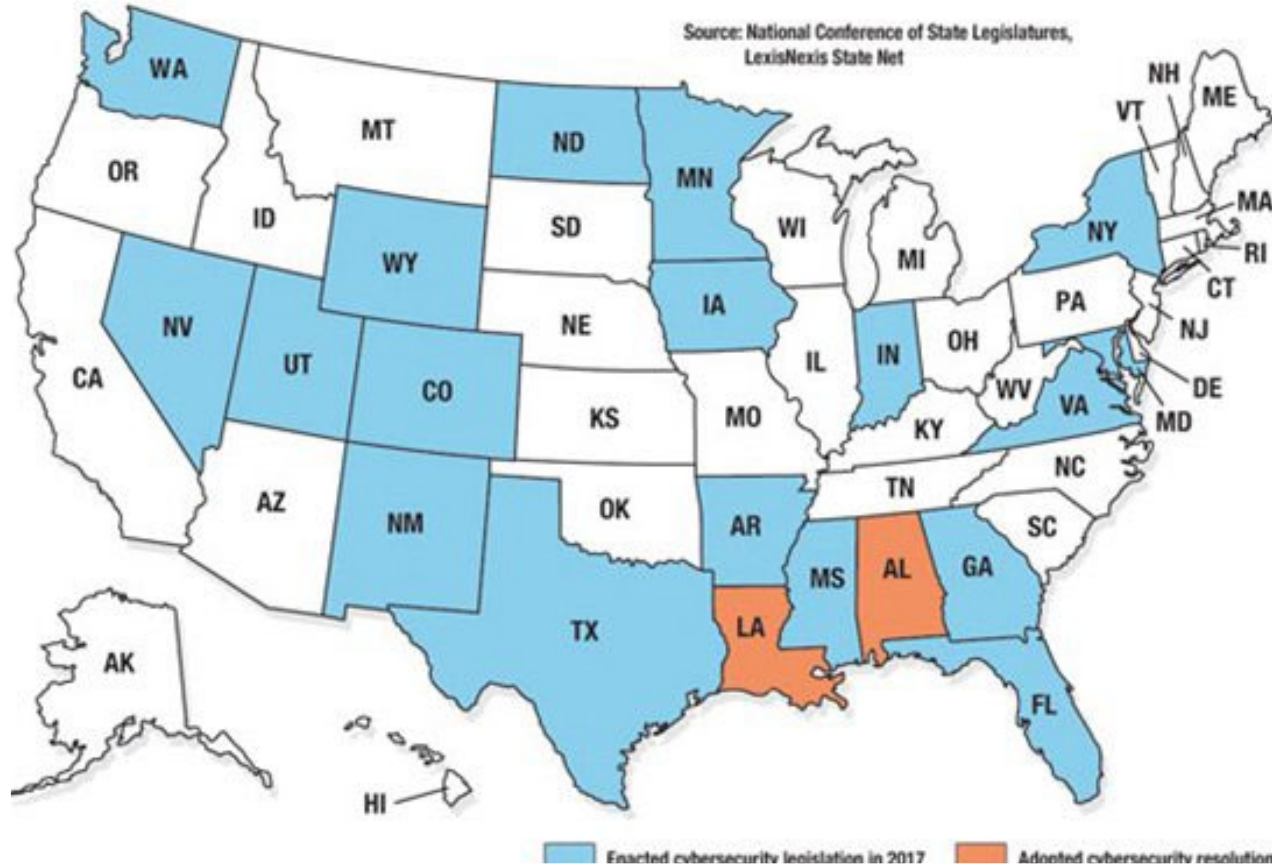
- (1) that the entity has a security policy in place;
- (2) that the entity has conducted at least one practice exercise based on the security policy within the 12 months immediately preceding the date of the affidavit; and
- (3) with respect to any entity that is an electric public utility, that the entity follows, at a minimum, the most current security standards set forth by the North American Electric Reliability Council.



Other State
(PUC)
approaches to
addressing
cybersecurity



←		Stricter laws	Less strict laws	→	
5	Alabama	5	Texas	4	Michigan
5	California	5	Utah	4	Montana
5	Illinois	4-5	Alaska	4	Nevada
5	New Jersey	4	Connecticut	4	New Hampshire
5	New York	4	Florida	4	New Mexico
5	Ohio	4	Indiana	4	Vermont
5	Oregon	4	Louisiana	4	Virginia
5	South Carolina	4	Maine	4	West Virginia
5	South Dakota	4	Maryland	3	Arizona
				3	Colorado
				3	Delaware
				3	Hawaii
				3	Idaho
				3	Iowa
				3	Minnesota
				3	Missouri
				3	Nebraska
				3	North Carolina
				3	North Dakota
				3	Oklahoma
				3	Rhode Island
				3	Tennessee
				3	Washington
				3	Guam
				3	Puerto Rico
				2	Arkansas
				2	Kansas
				2	Massachusetts
				2	Pennsylvania
				2	Wisconsin
				2	Wyoming
				2	Washington, I
				2	U.S. Virgin Isl
				1	Kentucky
				1	Mississippi

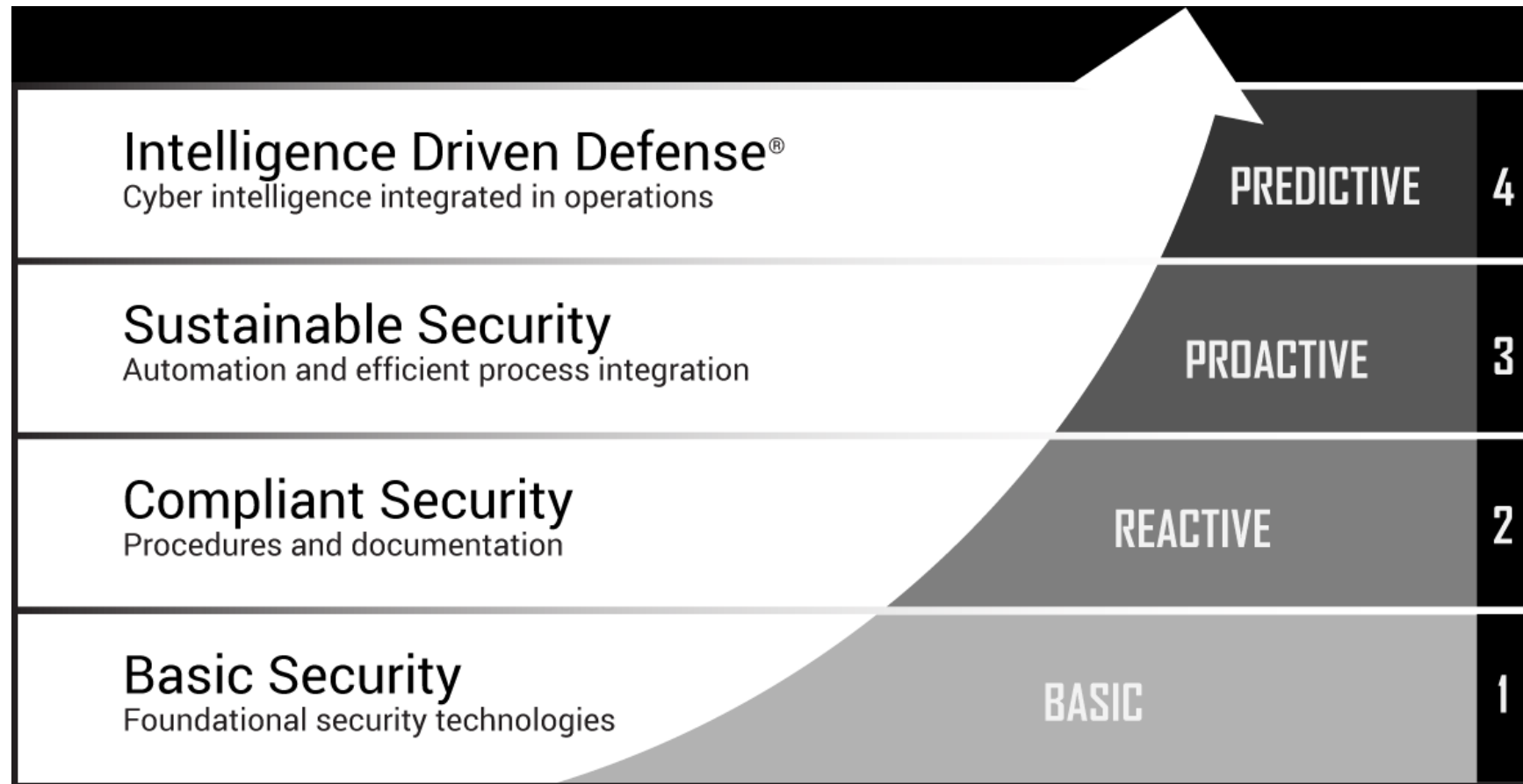


Varying Levels of Engagement Among the States

Data Protection and Breach Notification Focus

Cybersecurity Approaches Among PUCs

- Cybersecurity risk has become an issue of concern for PUCs
- PUCs are approaching the subject in different manners
 - Some Leading
 - Some Watching
 - Some Waiting
- Federal and States have overlapping and separate responsibilities, and all are working to figure out the approach



(In no particular order)
Florida, Texas, Michigan,
New Jersey, Kansas,
Illinois

Subset of Other States' Approaches

Florida

- Since 2014, the Florida Public Service Commission (FPSC) Office of Auditing and Performance Analysis has conducted periodic reviews of the physical and cyber security measures of several investor owned utilities in Florida.

http://www.floridapsc.com/Files/PDF/Publications/Reports/General/Electricgas/Cyber_Physical_Security.pdf#search=security



Review of Cyber and Physical Security Protection of Utility Substations and Control Centers

APRIL 2018

BY AUTHORITY OF
The Florida Public Service Commission
Office of Auditing and Performance Analysis

Michigan

In March 2018: The Michigan Legislature passed a law exempting cybersecurity and vulnerability information from its Freedom of Information Act

<https://www.usnews.com/news/best-states/michigan/articles/2018-03-06/legislature-oks-exempting-cybersecurity-info-from-foia>

In December 2018:

- Michigan Public Service Commission (PSC) approved revisions to its rules on Electrical Technical Standards requiring IOUs and Coops to provide annual and incident reporting to the PSC;
- The Michigan PSC also completed an Issue Brief addressing their actions on cybersecurity;

New Jersey

In 2016, New Jersey issued the Board of Public Utilities (BPU) Cybersecurity Order mandating utilities comply with its comprehensive utility cybersecurity program requirements

- Cybersecurity risk management (identify, analyze, control, monitor);
- Maintain situational awareness, incident reporting, response and recovery;
- Security awareness training;
- Utilities have to submit certification letters certifying compliance with the order and associated program requirements

Kansas

- Kansas Intelligence Fusion Center (KIFC)
 - Fully funded by state government, participation is free but by invitation only
- Operates at Top Secret (TS) classification level
- Protection of critical infrastructure and proprietary information
 - Exemptions in Kansas Sunshine Laws
 - State analysts are siloed from sensitive information, avoiding the creation of state records in the first place
 - Information cannot form the basis for regulatory enforcement



ICC's Approach to Cybersecurity

Strategy

Active assessment and interpretation of approaches;

Gaining a thorough understanding of current risks, mitigation and resiliency;

Sharing perspectives across sectors while prioritizing and incenting active sharing and collaborative behavior; and

Support and promote use of effective & economically prudent tactics that protect critical utility infrastructure

Understand, Inform and Balance Legislative Interactions and Increased Regulation



Prepare, Prepare, Prepare ... and then Prepare More

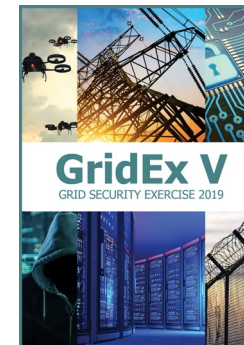


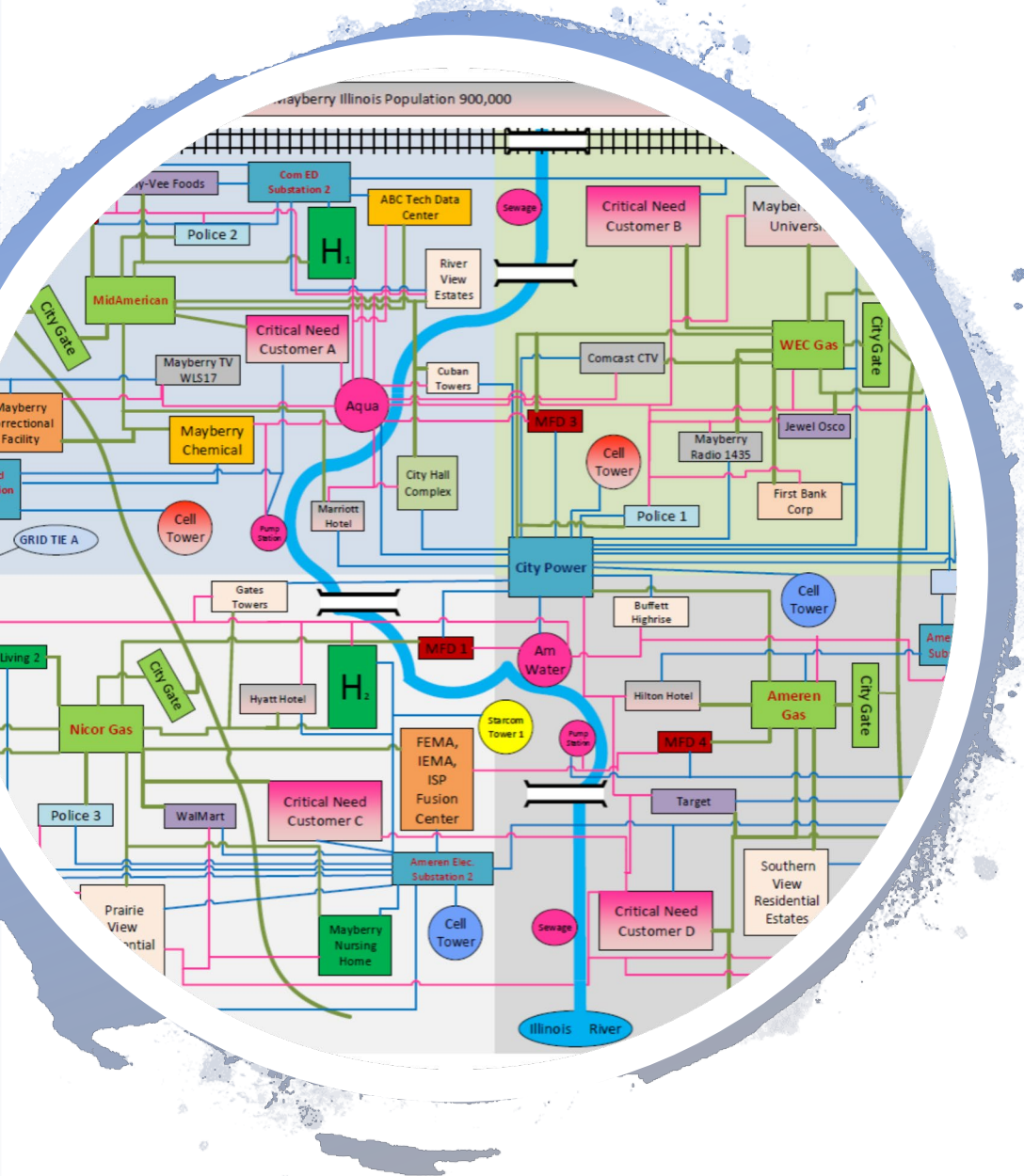
- There is no good excuse for not actively preparing for cyber attack responses
- In some states - preparation is a statutory requirement
 - Illinois requires utilities to have security plan & test it at least once a year
- Practicing, Drilling and Communicating are vital to an organizations ability to function effectively during a real event
- Table Top Exercises are a great way to bring various internal (and external) teams together to work through simulated situations that reveal weaknesses, answer questions and drive activities that strengthen and promote improved processes



ICC C&RM
Communication
& Cyber
Exercises
(2017 & 2018)

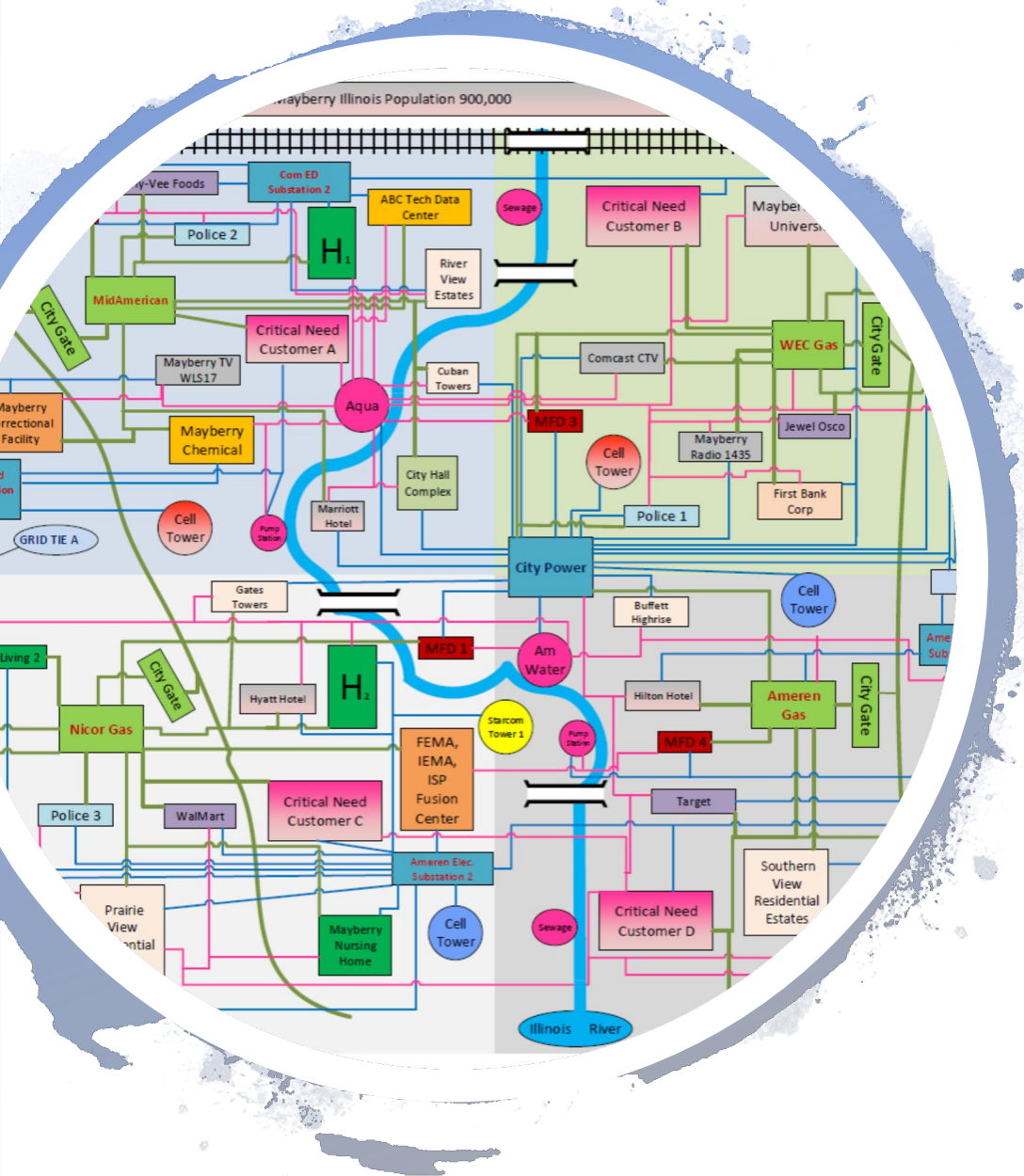
Exercises and Events





Cyber & Communications Joint Exercise 2017

- Investor-Owned Utilities
 - Electric
 - Gas
 - Water
- Microcosm of Illinois
 - Service territories
 - Seams
- Cross-sector and Cross-entity
- A lot of information in a short amount of time
- Lots of difficult questions provided backdrop to learn and test plans



Cyber & Communications Joint Exercise 2017

- Critical customers in each quadrant
 - Healthcare
 - First Responders
 - Campuses
 - Educational
 - Tech
 - Commercial
 - Industrial
- Combined Weather and Cyber Events
- Uncertainty
- Telecom Outage – Can't use your phone during response
- Low-temps and Fuel Shortage

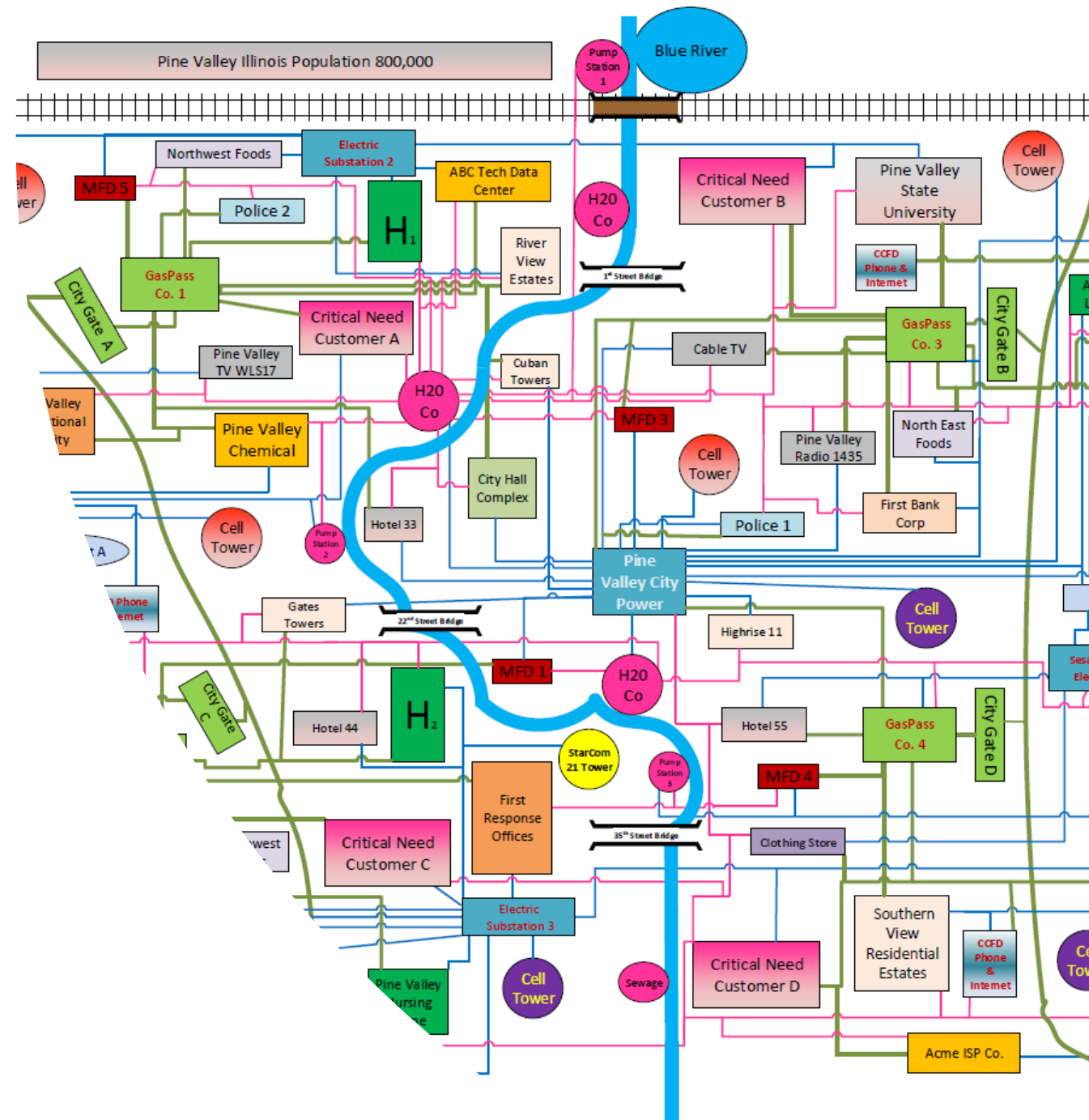
Spin-off Group from 2017 Communications Exercise

- Utility Communications Coordination Group
 - Corporate communications personnel from each participating utility
 - Continue discussions, maintain relationships, in preparation for disruptive events affecting multiple utilities
 - Best practices sharing, discussing lessons learned from other sectors
 - E.g. Starbucks, Uber, Netflix high profile PR incidents



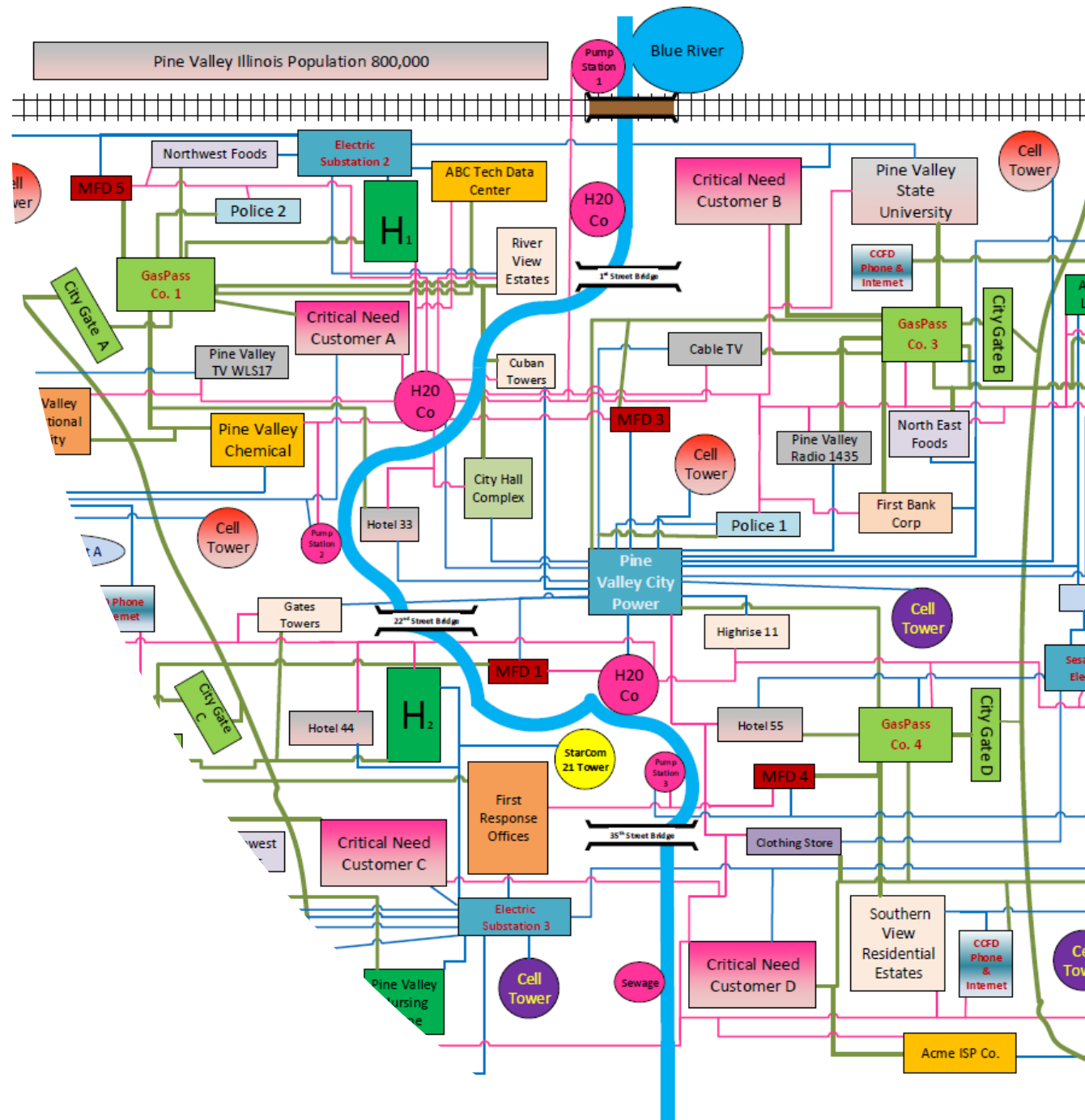
Cyber & Communication Exercise 2018

- IOUs + Telecom
- Functional area breakouts
 - Crisis Management
 - Corporate Communications
 - Cyber
 - Legal and Regulatory
 - Operations
 - Telecom
- Cross-Sector Learning
- Mock Press Conference



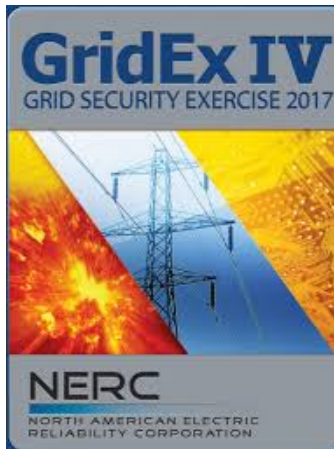
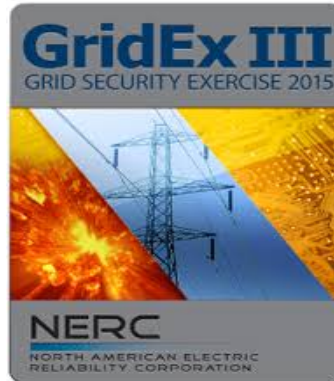
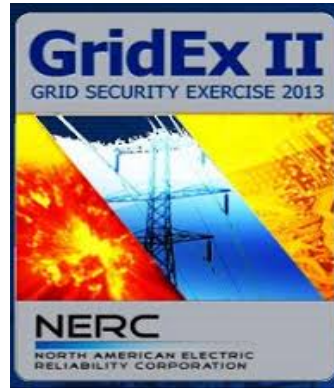
Cyber & Communication Exercise 2018

- Combined Weather, Physical, Cyber
- Changes in Response to 2017 Feedback
 - Less Information Overall
 - No Real-Time Injects
 - More Information in Advance
 - More Chances for Collaboration
 - More Autonomy Over Service Territory and Customers
 - Mock Press Conference



External Exercises

Participation



GridEx V

GRID SECURITY EXERCISE 2019



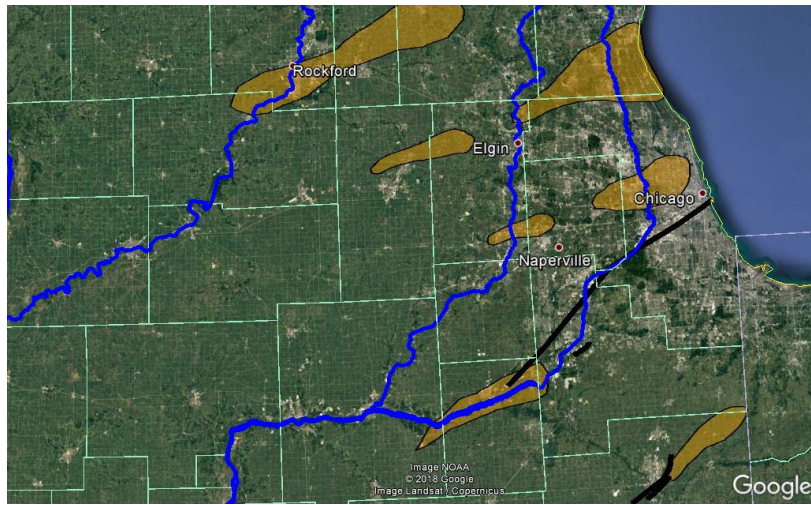
Operation Power Play 2019

Illinois Statewide Exercise

OPERATION POWER PLAY

2017

Illinois Statewide Exercise

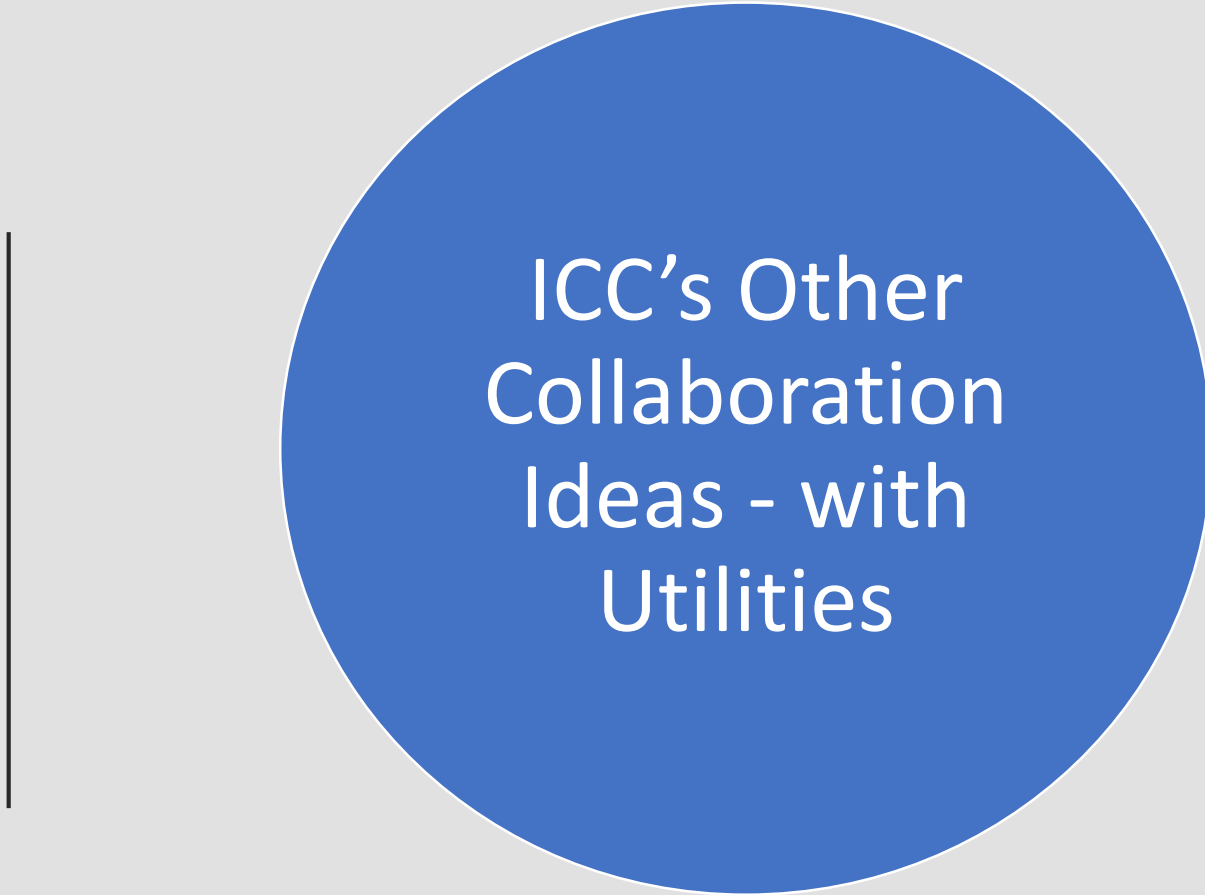


Supporting Agencies Participating:

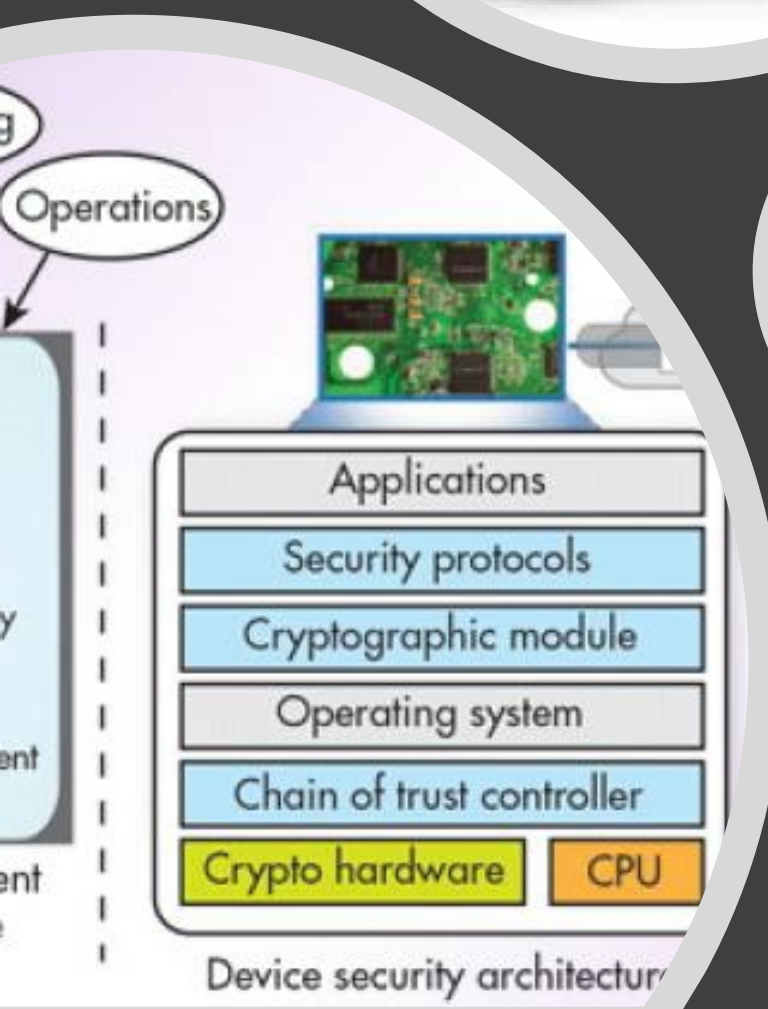
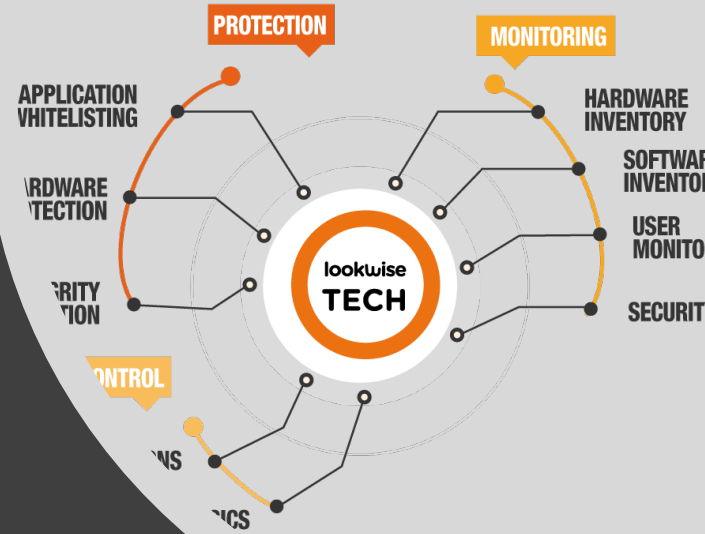
AQUA, **CPIC**, **ChicagoFIRST**, **US Army Corps of Engineers**, **IL Civil Air Patrol**, **NATIONAL WEATHER SERVICE**
Exelon, **Exelon Generation**, **SWAT**, **IPWMAN**, **CyrusOne**, **ILLINOIS AMERICAN WATER**
Frontier COMMUNICATIONS, **Pepco Holdings**, **IMERT**, **verizon**, **RUSH**
cta, **Illinois Department of Transportation**, **CME Group**, **westMONROE**, **KIRKLAND & ELLIS LLP**
AMTRAK, **PEOPLES GAS**, **NORTH SHORE GAS**, **Nicor Gas**, **pace**, **bp**
comcast, **BMO Harris**, **at&t**, **Metra**, **Southern Company**
motorola, **Business Services**, **FEDERAL BUREAU OF INVESTIGATION**, **FEDERAL RESERVE SYSTEM**, **at&t**, **Metra**, **AURORA**
Walgreens, **GSA**, **FEDERAL BUREAU OF INVESTIGATION**, **FEDERAL RESERVE SYSTEM**, **CHICAGO MIDWAY INTERNATIONAL AIRPORT**, **AURORA**
PRECISION RESTORATIONS, **ILEAS**, **O'HARE INTERNATIONAL AIRPORT**, **ILLINOIS NATIONAL GUARD**, **UIC**, **American Red Cross**
JPMorganChase, **Harbor Funds**, **PECO**, **BNSF RAILWAY**
WAL*MART, **THE UNIVERSITY OF CHICAGO**
Sprint, **American Water Works Association**, **IllinoisSection**, **FHLB Chicago**, **Illinois Petroleum Marketers Association**, **Illinois Association of C-Stores**
THE SALVATION ARMY, **DOING THE MOST GOOD**, **WINTRUST**, **BGE**, **POLICE**, **TARGET**, **UPS**
City of ROCHELLE, **VILLAGE OF ALGONQUIN**, **TEAM RUBICON**, **OSHA**, **CITY COLLEGES of CHICAGO**, **Wilbur Wright**, **State Farm**



Argonne National Lab
- PLC / SCADA Display



ICC's Other
Collaboration
Ideas - with
Utilities



Tech Summit 2018



Exercise or Tech Summit 2019 or 2020



<http://www.csoonline.com/article/3041383/security/how-to-conduct-a-tabletop-exercise.html>

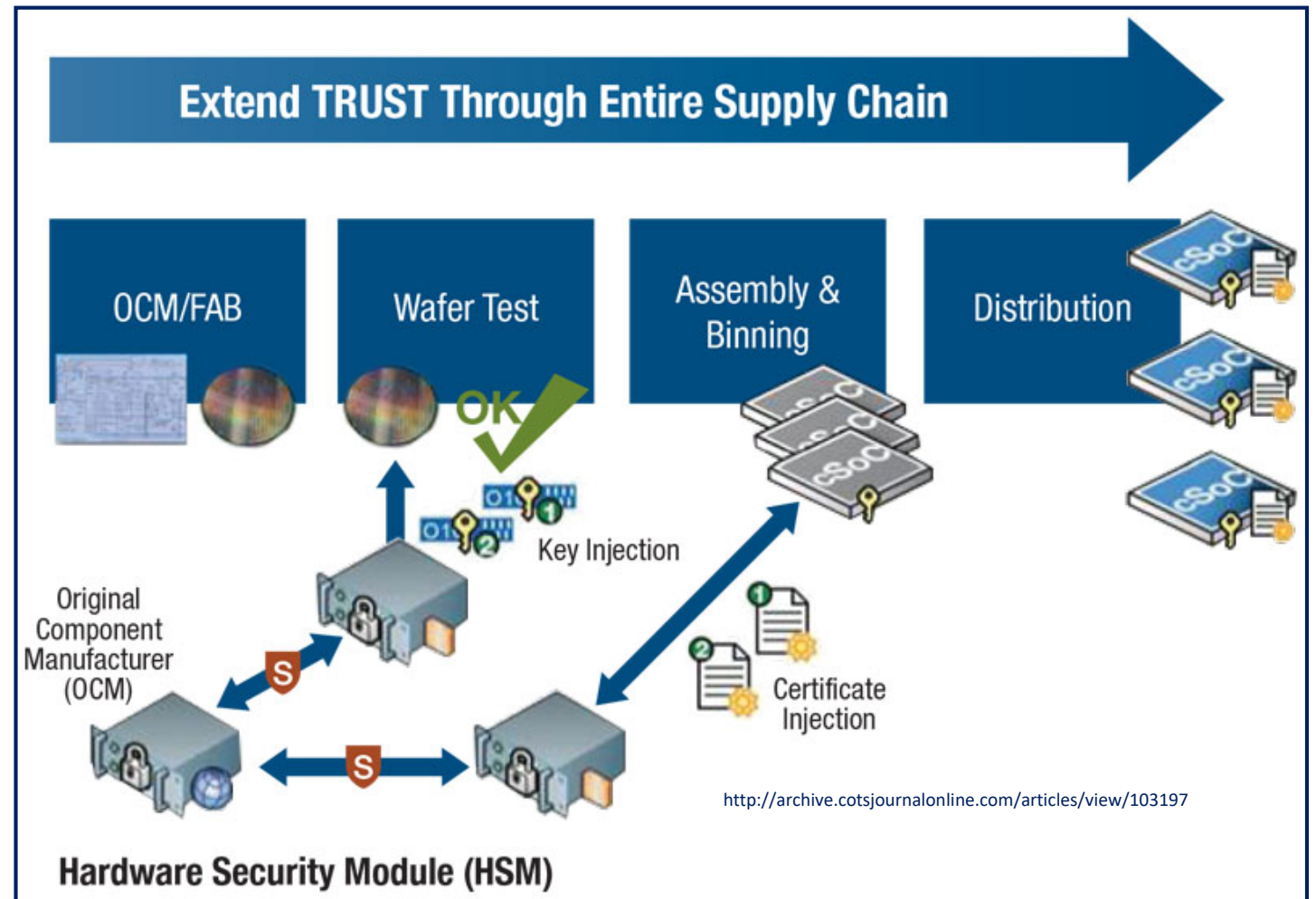


Other Content &
Topics ...

Top Priorities

(See following slides)

- Supply chain security;
- Optimizing threat intel sharing;
- Managing employee actions that increase risk;
- Cybersecurity workforce challenges (hiring & retaining capable workers);
- Leveraging automation technologies to streamline the role of workers toward critical thinking activities; &
- Improving cross sector collaboration, communication and best practice sharing.



Information Sharing and Intelligence



Homeland Security Protected Critical Infrastructure Information Program

ESCC

Electricity Subsector Coordinating Council

 **MS-ISAC**
Multi-State Information Sharing & Analysis Center®

CISA
CYBER+INFRASTRUCTURE



IEMA



ONG-ISAC



US-CERT







UNITED STATES COMPUTER EMERGENCY READINESS TEAM



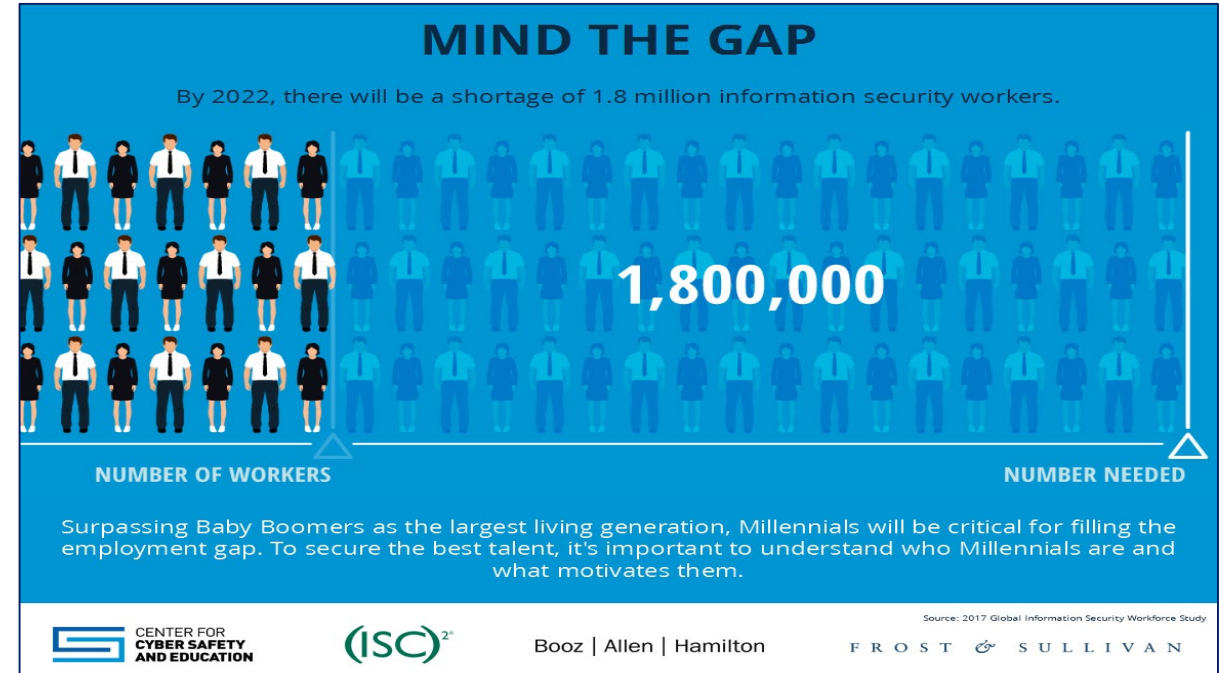
Cyber Talent Gap



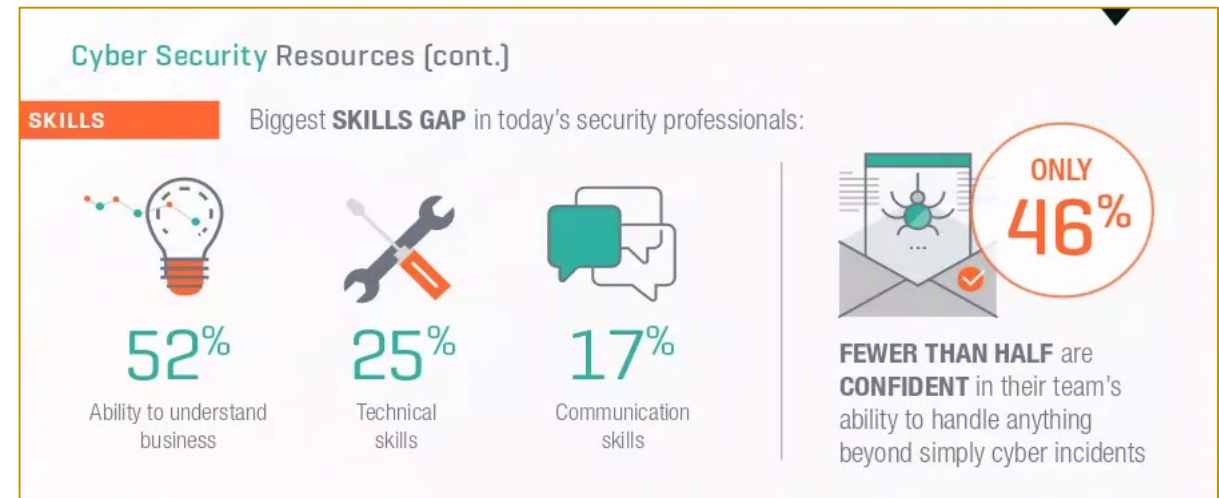
<https://medium.com/@drpolonski/can-we-teach-morality-to-machines-three-perspectives-on-ethics-for-artificial-intelligence-64fe479e25d3>

					
Core attributes	Explorer	Problem solver	Student	Guardian	Consultant
	Investigative and enjoys challenges	Analytic, methodical and detail oriented	Constantly learning	Protective, ethical and reliable	Can work with others to understand and solve their problems
Skills	An innate understanding of scenarios, risks and "what ifs"	Verifiable hands-on experience with references, certifications and/or micro-credentials Familiarity with and some ability to code—to figure out how to build and take things apart	Specific industry knowledge The ability to adapt to new and emerging security technologies	Familiarity with applicable regulations, laws and policies—and the ability to interpret them	The ability to work in dynamic and diverse teams Effective communication skills—can articulate complex concepts and clearly explain technical issues Experience educating others

<https://securityintelligence.com/cybersecurity-hiring-woes-time-to-consider-a-new-collar-approach/>



<https://www.boston.gov/news/demand-high-cybersecurity-workers>



<https://medium.com/@jayeshbahire/resolving-the-cyber-skills-gap-talent-shortage-d67c2ede7db1>

Selection of C&RM
Publications

Articles

PUBLIC UTILITIES FORTNIGHTLY

"In the Public Interest"

DECEMBER 2017

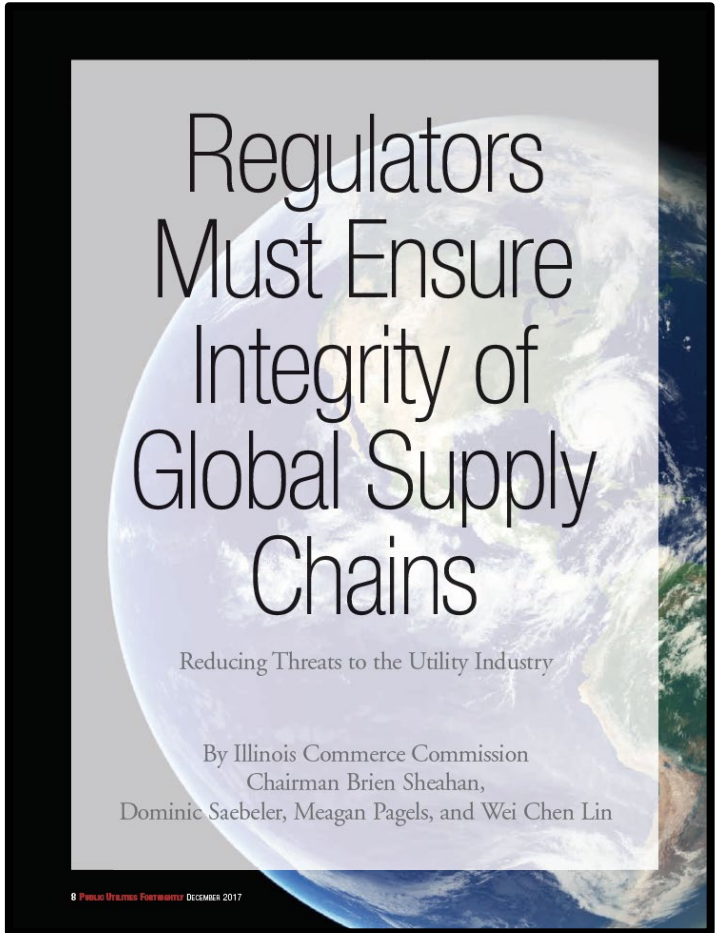
**Brien Sheahan, Bob Frenzel
Marty Lyons, Drew Marsh
Barbara Nick, Chris Gould
Dave Christian, Dave McCurdy
Don Clevenger, Bailey Bearss**

PUBLIC UTILITIES FORTNIGHTLY

Impact the Debate

APRIL 2019

**Brien Sheahan, Tom Flaherty
Gordon van Welie, Tom Linnquist
Dominic Saebeler, Wei Chen Lin
NRECA Annual Meeting & Expo**



Regulators Must Ensure Integrity of Global Supply Chains

Reducing Threats to the Utility Industry

By Illinois Commerce Commission
Chairman Brien Sheahan,
Dominic Saebeler, Meagan Pagels, and Wei Chen Lin



Vulnerability of SCADA Systems Underscore Urgent Need to Secure Utility Supply Chains

Regulatory Courage Required

By Brien J. Sheahan, Dominic Saebeler, and Wei Chen Lin

**Report to the
100th General Assembly
Regarding HJR 59
Cybersecurity Task Force**



December 2018



NARUC

National Association of Regulatory
Utility Commissioners



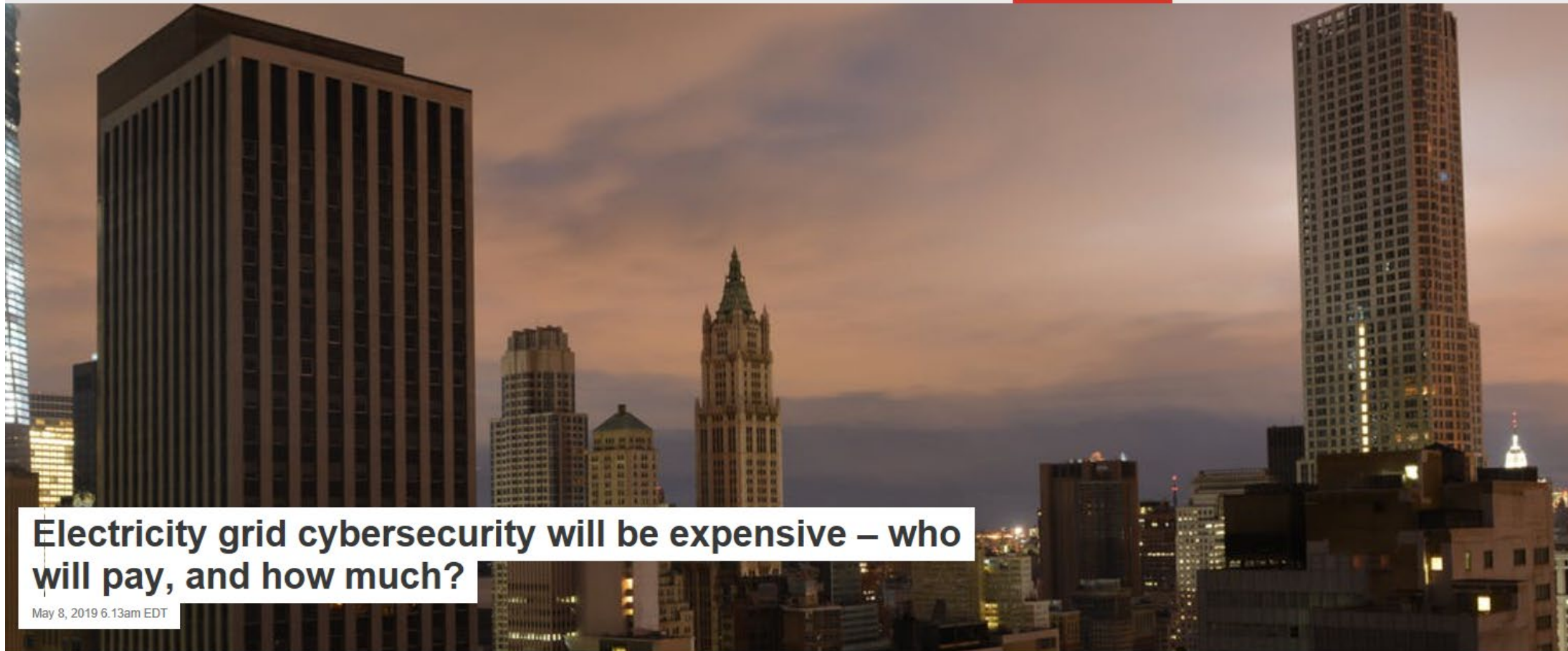
THE BULLETIN

Is there a Role for PUCs in Cybersecurity Exercises?

By Dominic Saebeler, Director of Cybersecurity and Risk Management, and Wei Chen Lin, Policy Advisor, Illinois Commerce Commission

Is there a productive role for a public utility commission (PUC) to design and facilitate a cybersecurity tabletop exercise for utilities that focuses on testing responsiveness and levels of preparation in the face of a simulated cyber attack?

It depends on the objectives, resources, and skillsets of a PUC and its staff. A great deal also depends on the willingness of investor-owned utilities to actively participate in an exercise over which they may have limited design control and where the utilities may be uncertain as to the value of participating. In the summer of 2017, the Illinois Commerce Commission (ICC) Office of Cybersecurity and Risk Management (C&RM) decided to answer this question. The experiences and lessons learned from that exercise can provide insights for commissions as they manage cybersecurity issues in their states.



Electricity grid cybersecurity will be expensive – who will pay, and how much?

May 8, 2019 6.13am EDT

In a power outage, some lights are on, but others are not. Felix Lipov/Shutterstock.com

Email

Twitter

Facebook

LinkedIn

Print

19

30

Recently, a neighbor asked one of us whether Russia, China, North Korea and Iran really are capable of hacking into the [computers that control](#) the U.S. electricity grid. The answer, based on [available evidence](#), is “Yes.” The follow-up question was, “How expensive will it be to prevent, and who will end up paying for it?”

The answers are: Likely tens of billions of dollars, and probably us, the electricity customers. This is a major – and, in our view, vital – investment in community and national

Authors



Dominic Saebeler

Adjunct Instructor of Business Administration,
University of Illinois at Springfield



Manimaran Govindarasu

Professor of Electrical and Computer Engineering,
Iowa State University

A Few Observations & Takeaways

- SCADA Systems are a complex target - but becoming more accessible;
 - Operational Technology is different than IT and requires different thinking and different defense approaches
- Collaboration is essential in preparing for potential cyber disruptions;
 - Don't try this at home alone – (or don't swim without a lifeguard)
- Communication and practicing together serves to strengthen resiliency;
 - There will be language (jargon) barriers and human error that will create response complexities
- Active participation in exercises is the best way to find out what isn't going to work during a real crisis;
 - Unless you want to find out during the crisis
- Service Providers need to continually promote a culture of security;
 - And share & learn from each other so everyone gets smarter and mistakes are avoided
- Meeting with peers and similarly situated teams is a great way to learn and test approaches;
 - Learning from the mistakes and trial and error of others with ICS systems is beneficial;
- Regulators have a role in ensuring shortcuts are not taken as a result of economic decisions
 - Legislators will try to help – sometimes that works and other times it does not – we need to have them listen to us

