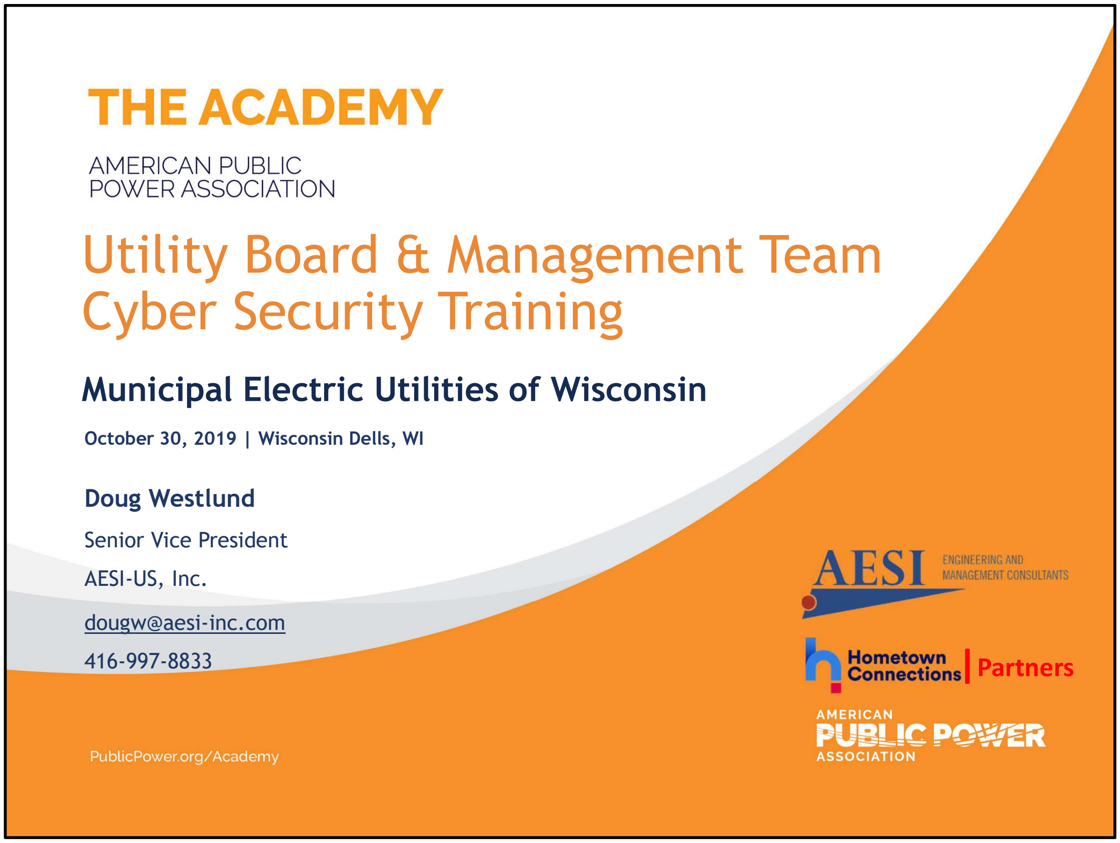


THE ACADEMY

AMERICAN PUBLIC
POWER ASSOCIATION

Utility Board & Management Team Cyber Security Training

Municipal Electric Utilities of Wisconsin

October 30, 2019 | Wisconsin Dells, WI

Doug Westlund

Senior Vice President

AESI-US, Inc.

dougw@aesi-inc.com

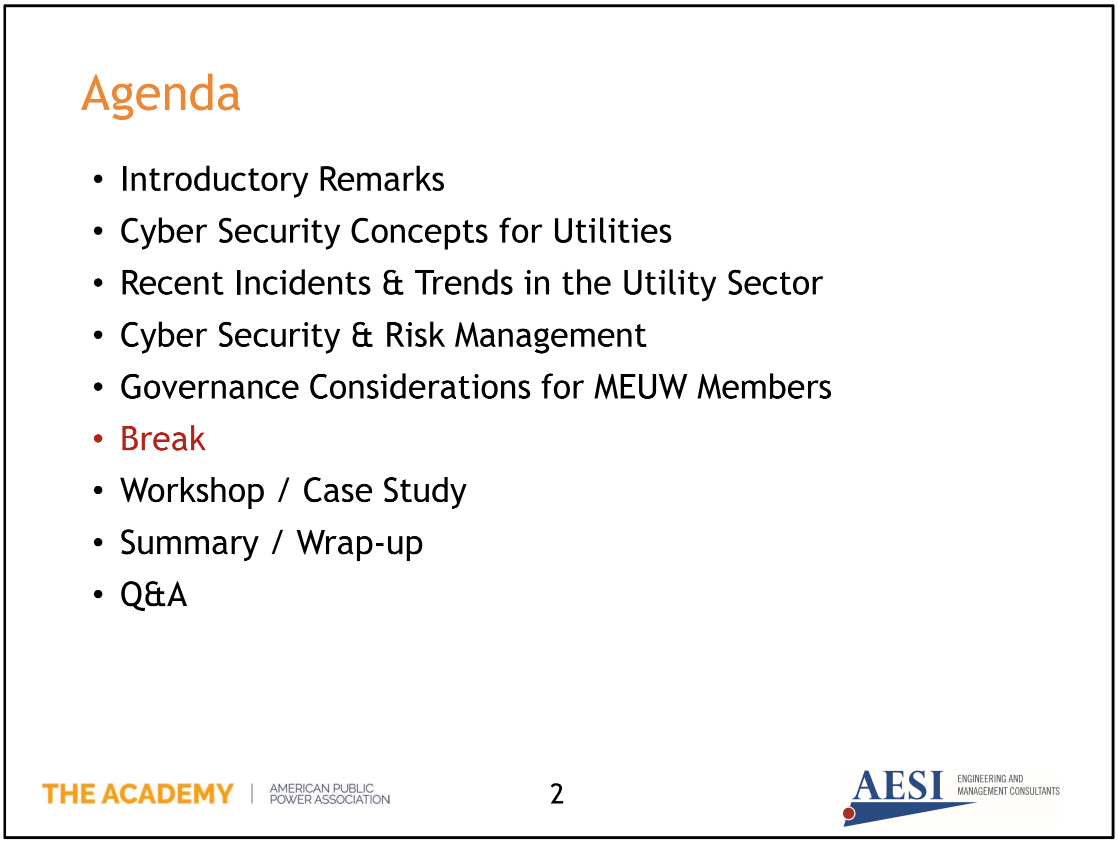
416-997-8833

AESI ENGINEERING AND MANAGEMENT CONSULTANTS

Hometown Connections | Partners

AMERICAN PUBLIC POWER ASSOCIATION

PublicPower.org/Academy



Agenda

- Introductory Remarks
- Cyber Security Concepts for Utilities
- Recent Incidents & Trends in the Utility Sector
- Cyber Security & Risk Management
- Governance Considerations for MEUW Members
- Break
- Workshop / Case Study
- Summary / Wrap-up
- Q&A

The purpose of this training session is to provide a high level summary of cyber security, the trends and relevance for Utilities, and the fundamental concept that cyber security is an element of risk management.
The training finishes with presentation of governance tools and considerations for MEUW Members.
In the training, physical security is included in the security perspectives as it relates to physical breaches that could lead to impairment or control of computing devices.

Overview of AESI

- Supporting utility clients since 1984 – providing engineering and management consulting services to over 500 utilities in North America and internationally
- Substantiated and proven long term public power experience with JAAs and distribution utilities
- Selected by Hometown Connections for cyber security, IT/OT and regulatory services for public power

Hometown Connections | Partner

Regulatory Compliance
sustainable compliance assurance

Cyber Security
holistic approach to risk management

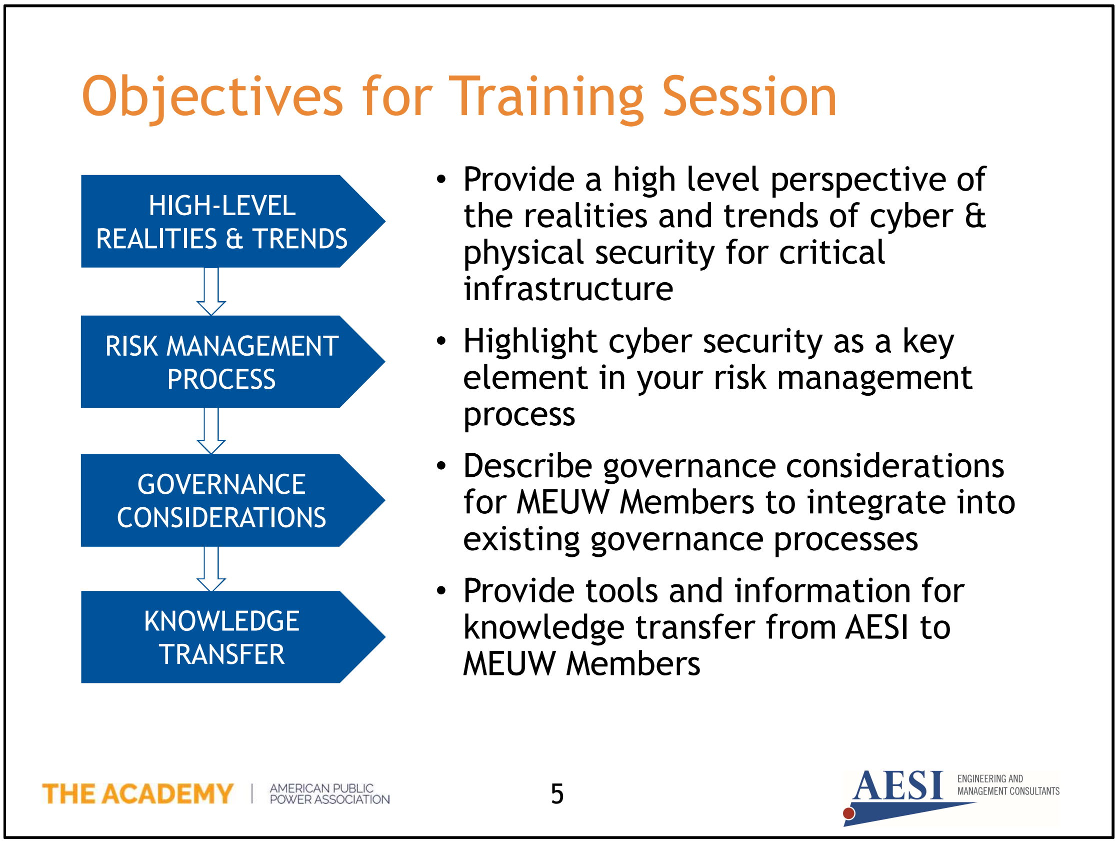
Operational Technology
managing operational complexities

Energy Advisory
pragmatic engineering support

About the Trainer

- SCADA Engineer by training
- ~20 years assisting utilities with their cybersecurity challenges
- Contracted by the APPA and the NRECA for cyber training for their members
- Additional areas of expertise: operational risk assessments, cyber governance, development of cyber programs
- Board Director

And a life long suffering Vikings fan …



Objectives for Training Session

HIGH-LEVEL REALITIES & TRENDS

RISK MANAGEMENT PROCESS

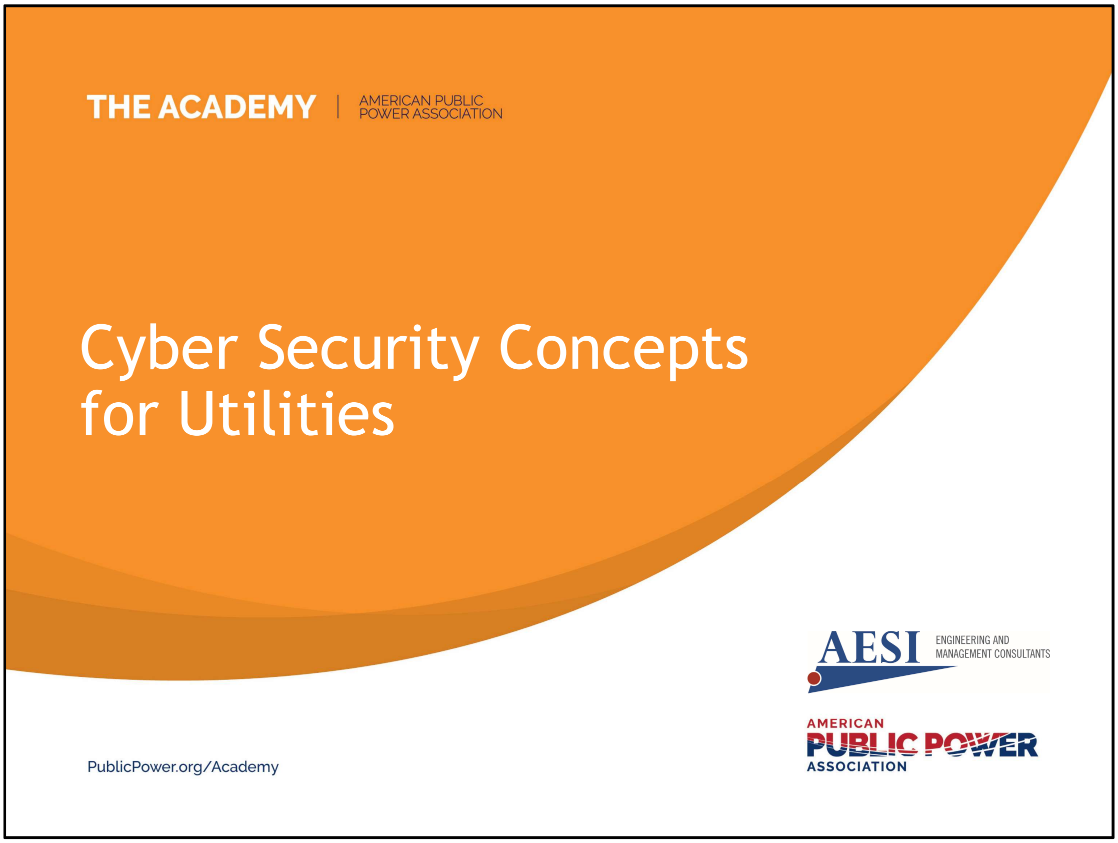
GOVERNANCE CONSIDERATIONS

KNOWLEDGE TRANSFER

- Provide a high level perspective of the realities and trends of cyber & physical security for critical infrastructure
- Highlight cyber security as a key element in your risk management process
- Describe governance considerations for MEUW Members to integrate into existing governance processes
- Provide tools and information for knowledge transfer from AESI to MEUW Members

Background on the Issue

- Not a new issue, but growing in importance for utilities due to:
  - Digitization of utility office and grid operations
  - Attractiveness of the energy sector to hackers ☹
  - Advancement of hacking tools and capabilities
- Over the last several years the industry has established common frameworks and standards for utilities ☺
- Utility associations such as the APPA are active in delivering tools, support and resources for their members ☺



THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION

Cyber Security Concepts for Utilities

AESI ENGINEERING AND MANAGEMENT CONSULTANTS

AMERICAN PUBLIC POWER ASSOCIATION

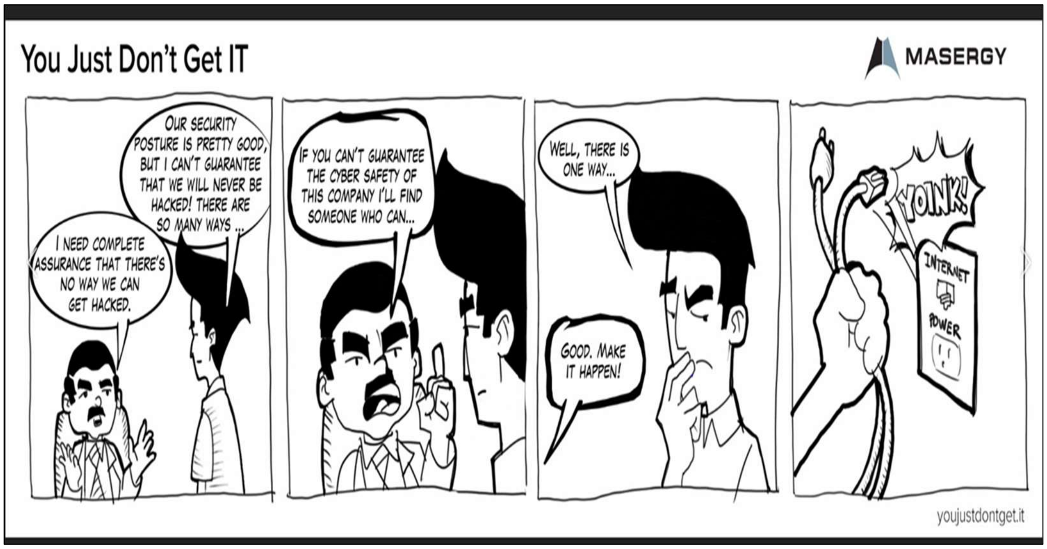
PublicPower.org/Academy

Cyber Security

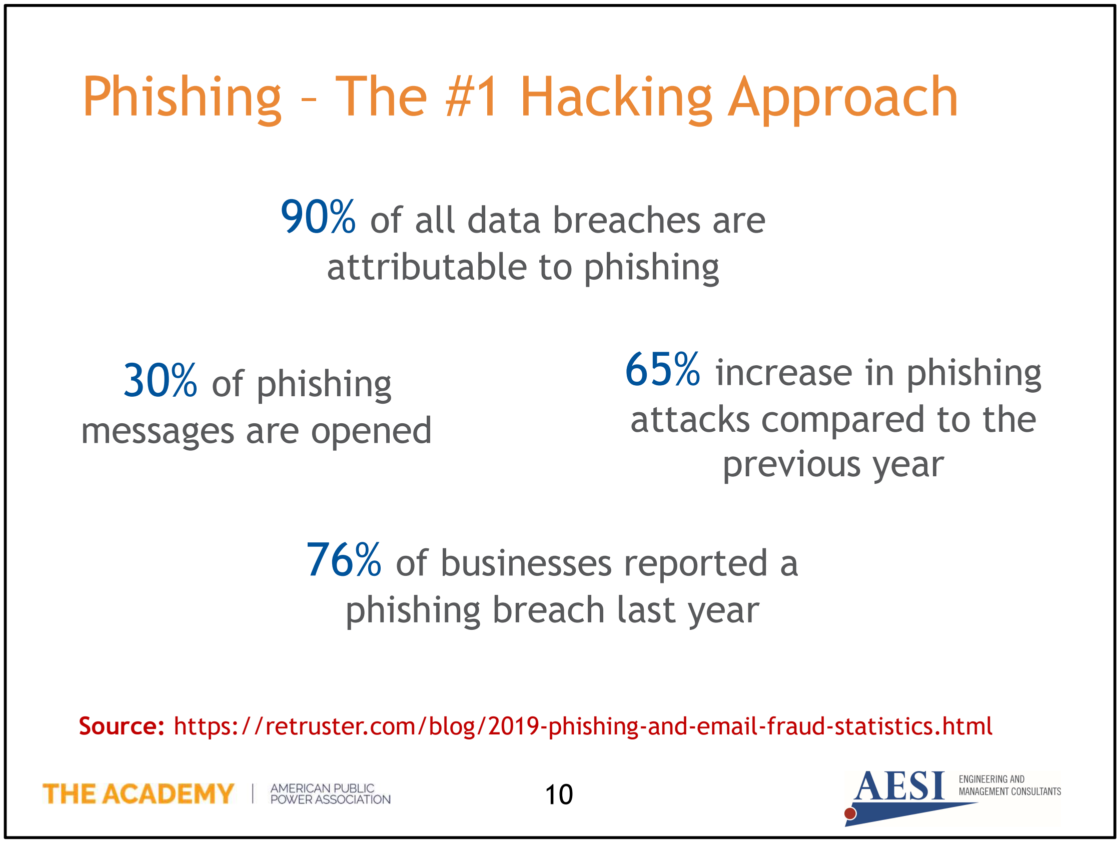
Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, training, best practices, and technologies that can be used to protect the cyber environment and organization and user’s assets.

Source: ITU-T X.1205, Overview of Cybersecurity

The Reality …


You Just Don't Get IT
MASERGY
I NEED COMPLETE ASSURANCE THAT THERE'S NO WAY WE CAN GET HACKED.
OUR SECURITY POSTURE IS PRETTY GOOD, BUT I CAN'T GUARANTEE THAT WE WILL NEVER BE HACKED! THERE ARE SO MANY WAYS ...
IF YOU CAN'T GUARANTEE THE CYBER SAFETY OF THIS COMPANY I'LL FIND SOMEONE WHO CAN...
WELL, THERE IS ONE WAY...
GOOD. MAKE IT HAPPEN!
YOINK!
INTERNET
POWER
youjustdontget.it

There is no such thing as being 100% secure.   All systems can be hacked.



Phishing – The #1 Hacking Approach

90% of all data breaches are attributable to phishing

30% of phishing messages are opened

65% increase in phishing attacks compared to the previous year

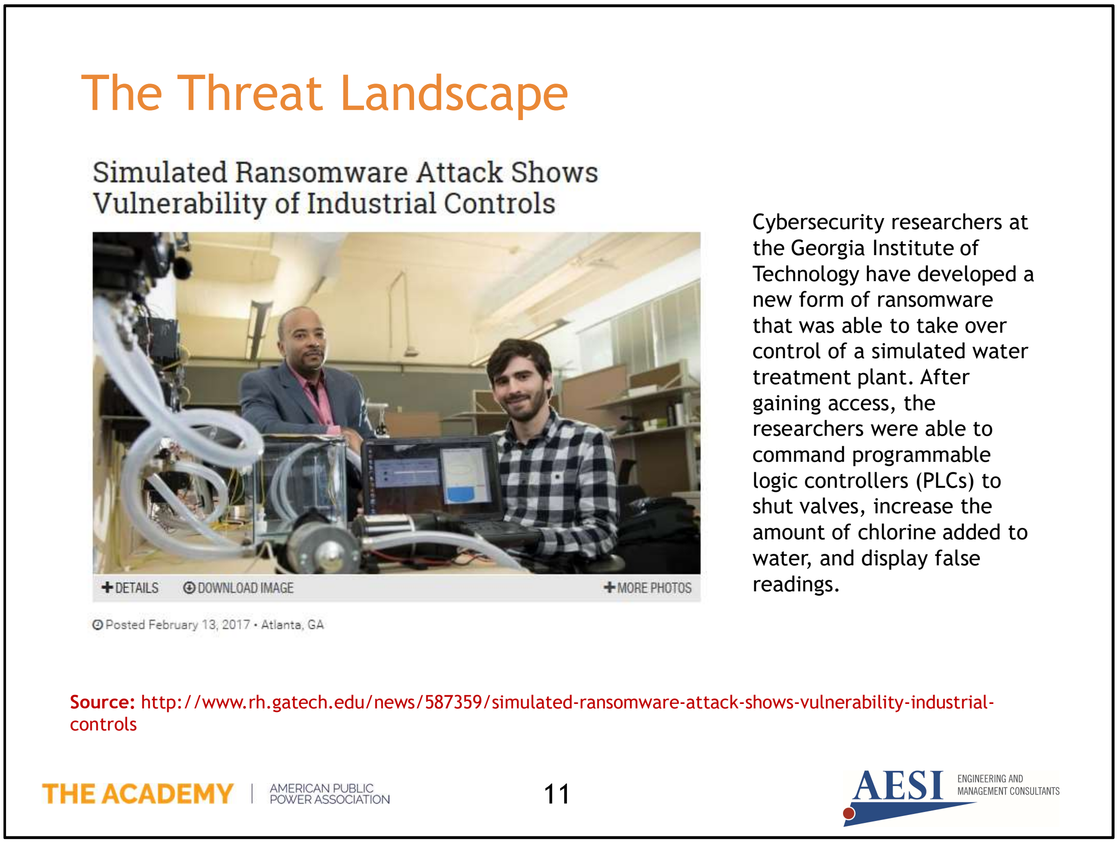
76% of businesses reported a phishing breach last year

Source: https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html

A phishing email is a fraudulent attempt to get sensitive data or information from people like their usernames, passwords, financial information or credit card details, by disguising as someone trustworthy.

Phishing is the #1 hacking tool of choice.   It is very effective and most typically the hackers can be well disguised.

Key to phishing protection for utilities are a) regular awareness training and b) a specific anti-phishing program.



The Threat Landscape

Simulated Ransomware Attack Shows Vulnerability of Industrial Controls

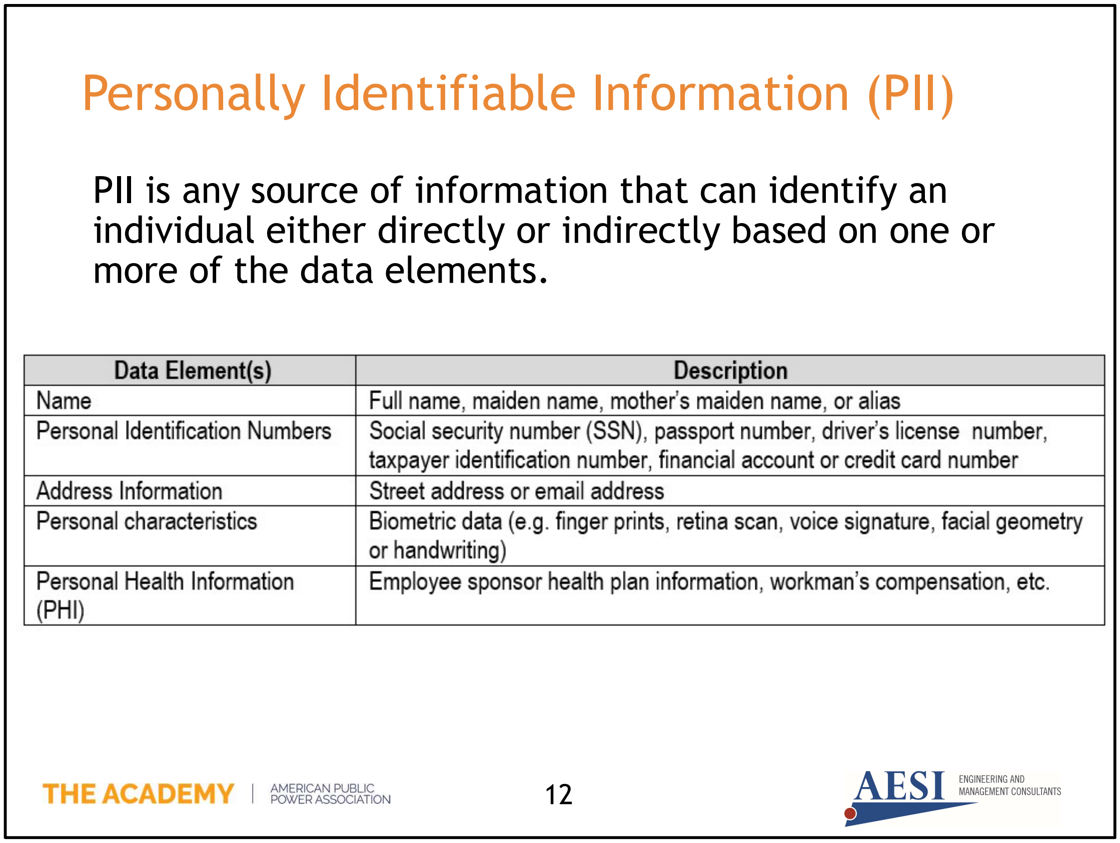
Posted February 13, 2017 • Atlanta, GA

Cybersecurity researchers at the Georgia Institute of Technology have developed a new form of ransomware that was able to take over control of a simulated water treatment plant. After gaining access, the researchers were able to command programmable logic controllers (PLCs) to shut valves, increase the amount of chlorine added to water, and display false readings.

Source: http://www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls

This article creates great concern for the utility sector.
This article describes from ransonware software has been adapted to gain control of industrial control systems including Programmable Logic Controllers (PLCs). The same PLCs are used in the water, gas and electric sectors.

Of most concern is the difficulty for utilities to monitor cyber attacks in their Operational Technology (OT) environments, and the high impact of such attacks on these OT systems. In the IT world good backups can be a solution to ransonware, but it would not be the case in such an attack on OT systems.



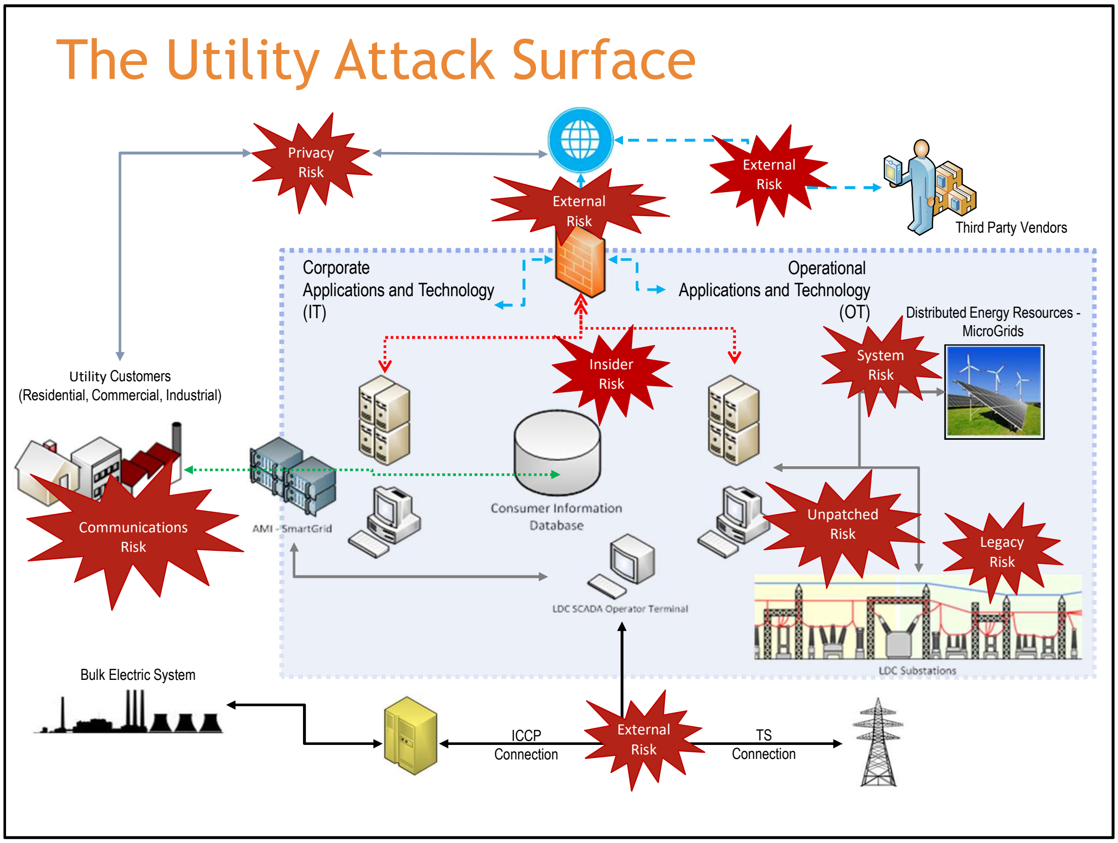
Personally Identifiable Information (PII)

PII is any source of information that can identify an individual either directly or indirectly based on one or more of the data elements.

Data Element(s)	Description
Name	Full name, maiden name, mother's maiden name, or alias
Personal Identification Numbers	Social security number (SSN), passport number, driver's license number, taxpayer identification number, financial account or credit card number
Address Information	Street address or email address
Personal characteristics	Biometric data (e.g. finger prints, retina scan, voice signature, facial geometry or handwriting)
Personal Health Information (PHI)	Employee sponsor health plan information, workman's compensation, etc.

Data privacy is an increasing concern. Key is to focus on the PII in your utility and protect.

Privacy and cyber security are inextricably linked. A good privacy program requires a solid cyber security foundation and program.



The Utility Attack Surface

Privacy Risk
External Risk
External Risk
Third Party Vendors
Corporate Applications and Technology (IT)
Operational Applications and Technology (OT)
Distributed Energy Resources - MicroGrids
Utility Customers (Residential, Commercial, Industrial)
Insider Risk
System Risk
Communications Risk
AMI - SmartGrid
Consumer Information Database
Unpatched Risk
Legacy Risk
LDC SCADA Operator Terminal
LDC Substations
Bulk Electric System
ICCP Connection
External Risk
TS Connection

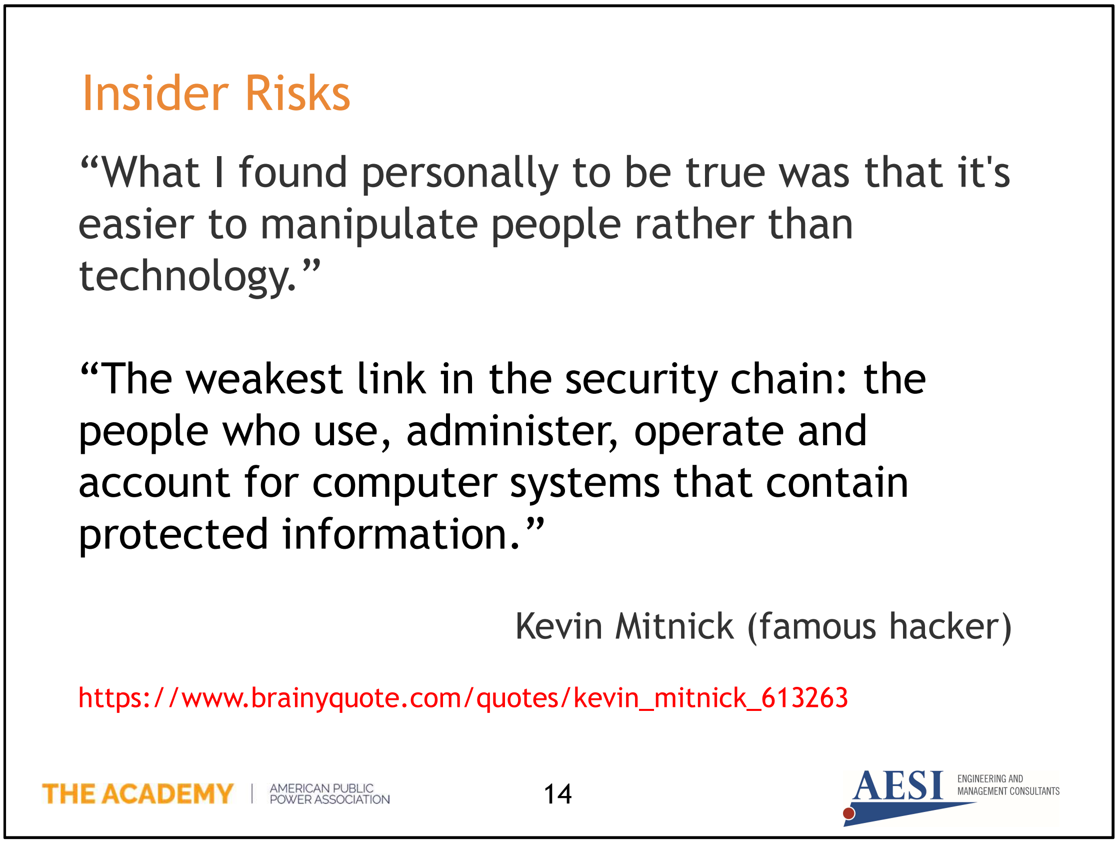
This is a key visual for MEUW Members to consider in its cyber security program. Cyber security mirrors many military strategies.   The military aim is to minimize the visibility and size of your attack surface.

Utilities however have a large and growing attack surface.   Automation (e.g. smart maters, distribution automation), new energy programs (e.g. demand response) and large service territories create a large attack surface.

Utilities such as MEUW Members should understand and depict their attack surface, draw a box around it, and then implement controls to protect its attack surface at the borders of the box and within.

The visual depicts major sources of risk (attack vectors) on a typical utility attack surface.

It is a good approach to prioritize insider risks and third party risks and manage them closely.



Insider Risks

“What I found personally to be true was that it's easier to manipulate people rather than technology.”

“The weakest link in the security chain: the people who use, administer, operate and account for computer systems that contain protected information.”

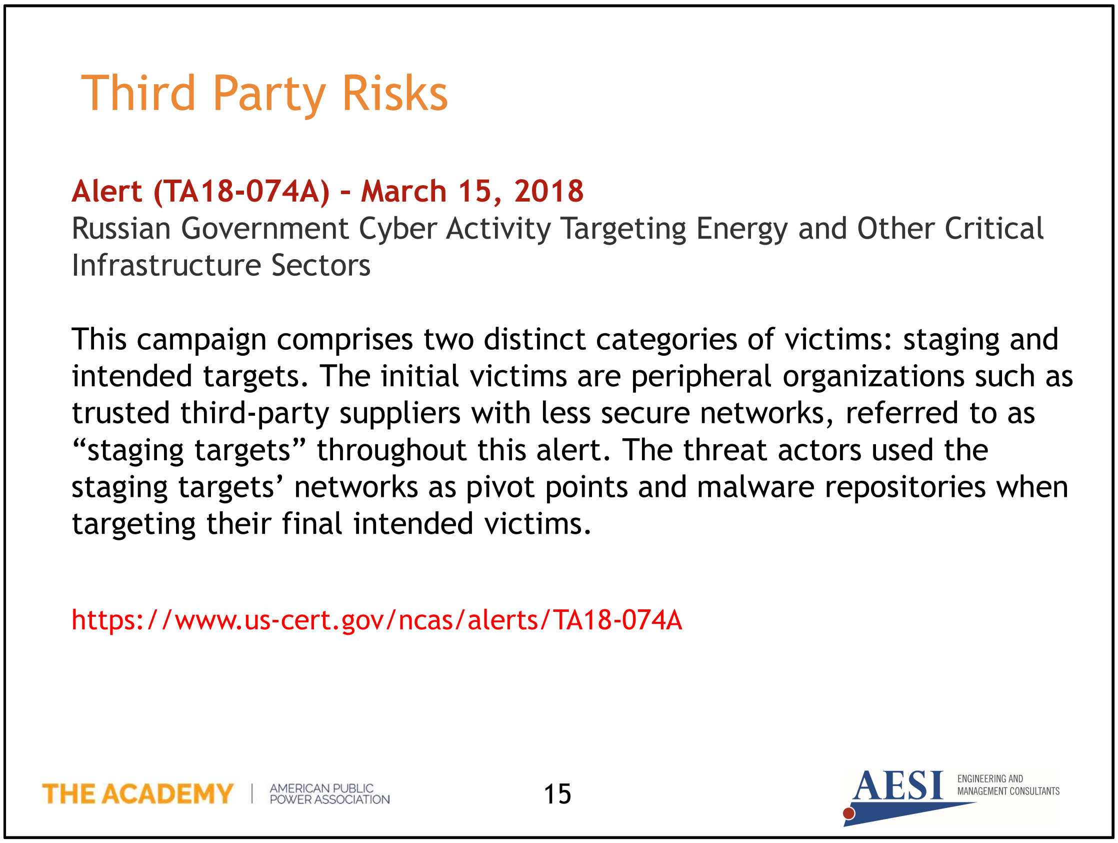
Kevin Mitnick (famous hacker)

https://www.brainyquote.com/quotes/kevin_mitnick_613263

Kevin Mitnick is one of the world’s most famous hackers.

He was arrested in 1995 for a series of high profile hacking crimes and spent 5 years in prison.

He regularly points to people as being the weakest link, and the easiest element to fool.



Third Party Risks

Alert (TA18-074A) - March 15, 2018
Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

This campaign comprises two distinct categories of victims: staging and intended targets. The initial victims are peripheral organizations such as trusted third-party suppliers with less secure networks, referred to as "staging targets" throughout this alert. The threat actors used the staging targets' networks as pivot points and malware repositories when targeting their final intended victims.

https://www.us-cert.gov/ncas/alerts/TA18-074A

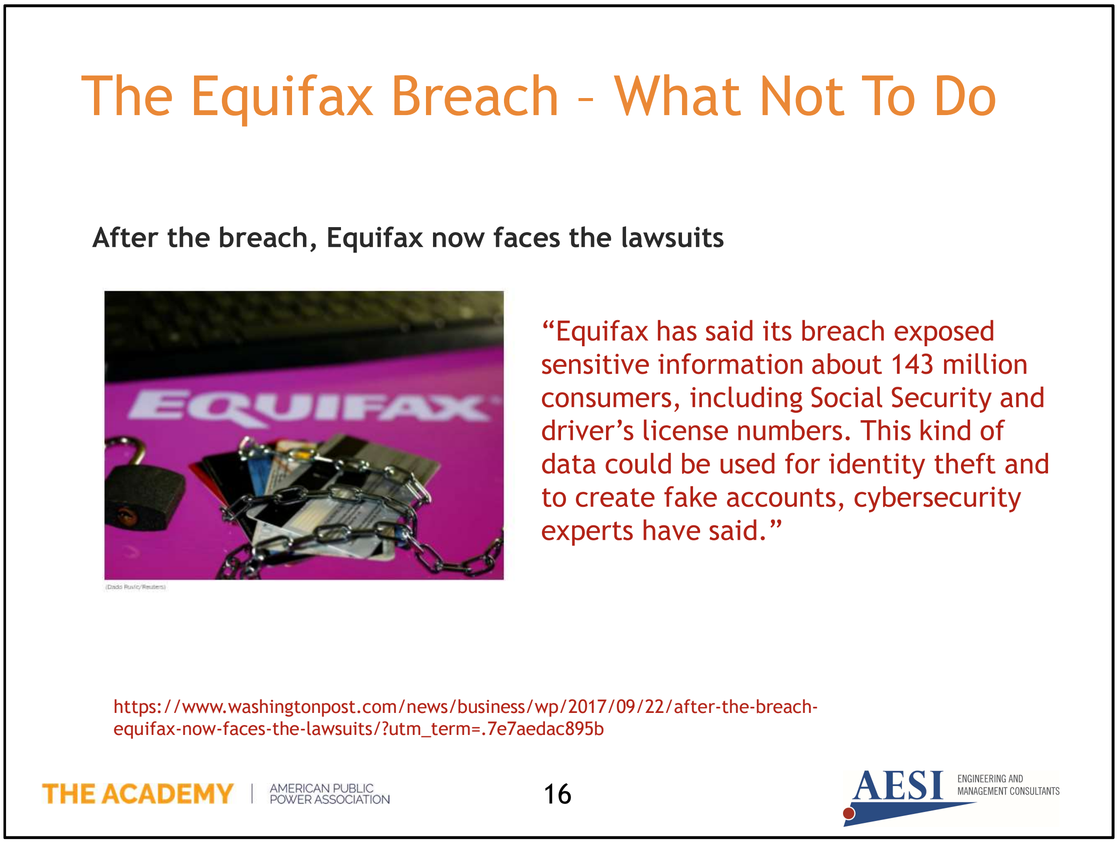
THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION 15 AESI ENGINEERING AND MANAGEMENT CONSULTANTS

This slide shows a subset of the US CERT alert on Russian government hacking attempts on US critical infrastructure including the grid.

Third parties represent a large source of attack vectors into a utility.

Diligence needs to be applied to third parties including:

- Contractual commitments to good security practices by the third party
- Acknowledgement of the utility's security policy by the third party
- Restricted and controlled access for the third party
- Monitoring of the third party's access and activity



The Equifax Breach – What Not To Do

After the breach, Equifax now faces the lawsuits

(Dado Ruvic/Reuters)

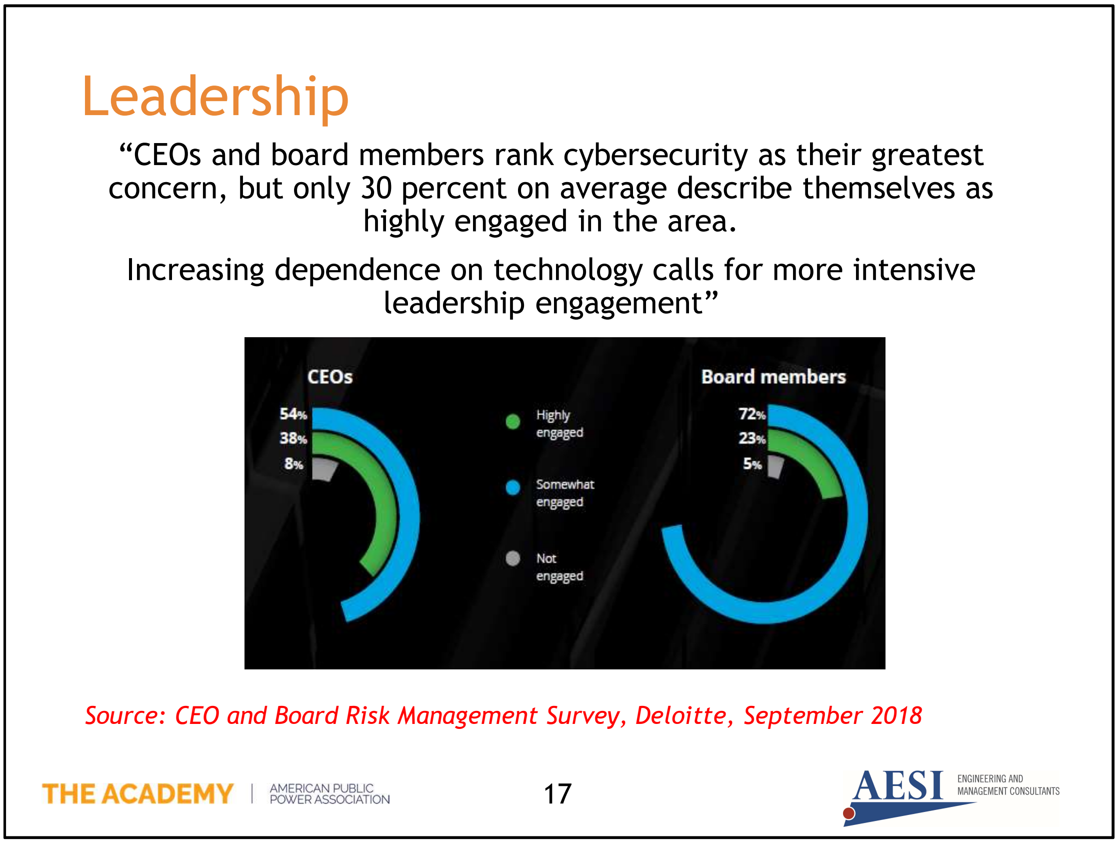
"Equifax has said its breach exposed sensitive information about 143 million consumers, including Social Security and driver's license numbers. This kind of data could be used for identity theft and to create fake accounts, cybersecurity experts have said."

https://www.washingtonpost.com/news/business/wp/2017/09/22/after-the-breach-equifax-now-faces-the-lawsuits/?utm_term=.7e7aedac895b

The Equifax breach is a massive privacy breach. And although not in the energy sector this breach is worth mentioning to highlight the impact of privacy breaches.

The hackers were in the Equifax systems and networks weeks before being detected. And then it was several more weeks before disclosure was made by Equifax.

Upon detection of a privacy breach legal counsel should be retained. And then disclosure to affected parties should happen as soon as possible.



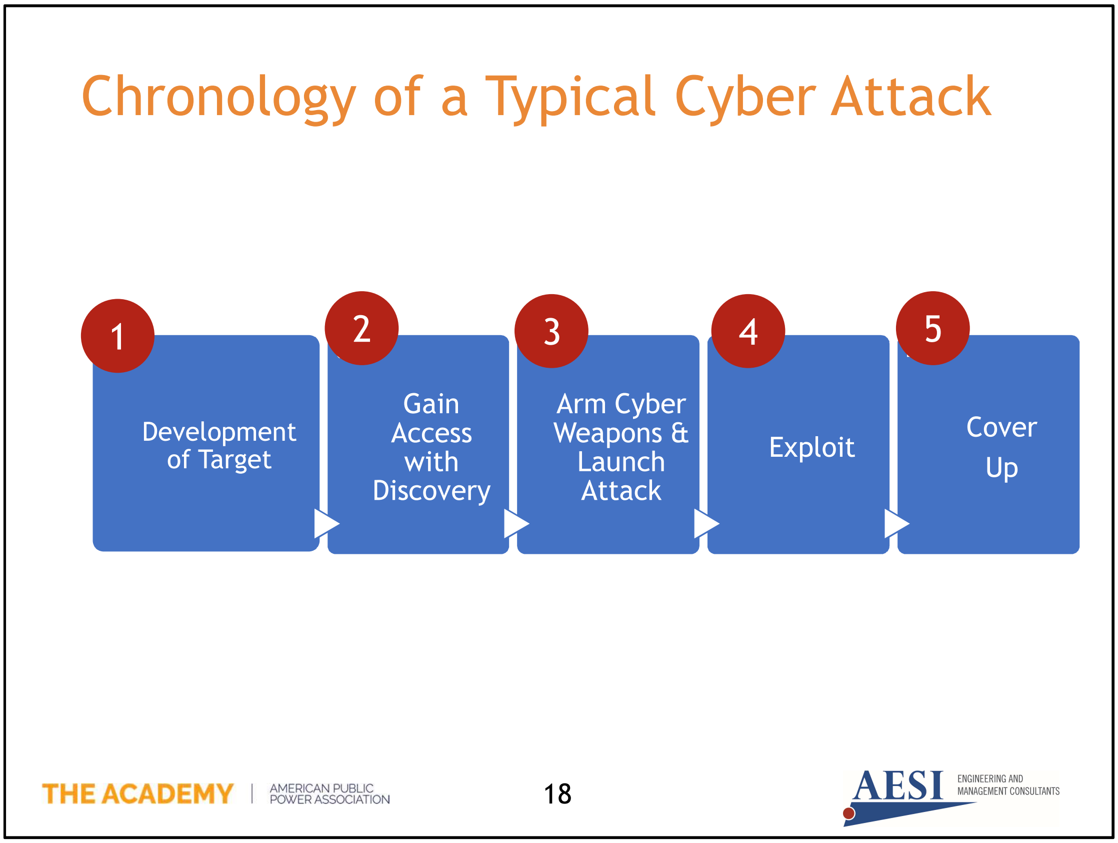
Leadership

“CEOs and board members rank cybersecurity as their greatest concern, but only 30 percent on average describe themselves as highly engaged in the area.

Increasing dependence on technology calls for more intensive leadership engagement”

Source: CEO and Board Risk Management Survey, Deloitte, September 2018

Engaged and supportive leadership from the Utility Board and Executive Team is a key requirement for any cyber security program. Without it the cyber program will fail.



Chronology of a Typical Cyber Attack

1 Development of Target

2 Gain Access with Discovery

3 Arm Cyber Weapons & Launch Attack

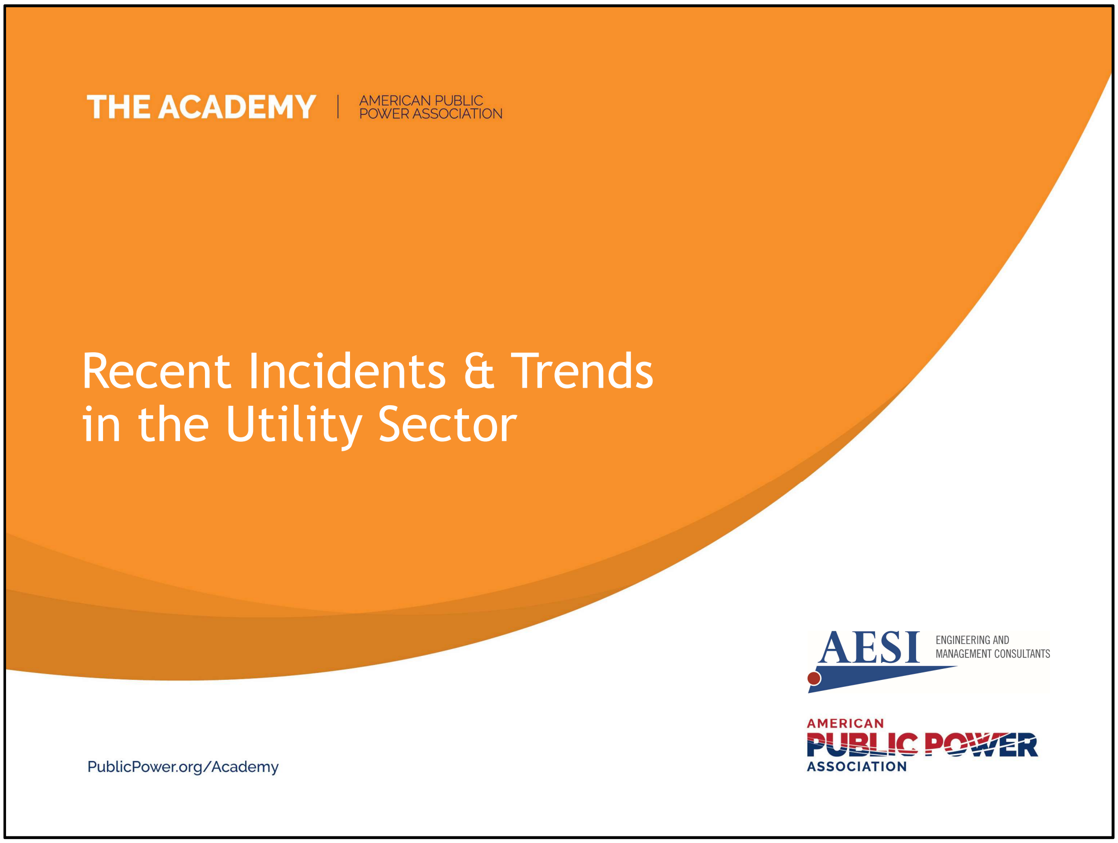
4 Exploit

5 Cover Up

THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION

AESI ENGINEERING AND MANAGEMENT CONSULTANTS

This slide depicts a typical cyber attack.
This first stage in the process is to develop the target. This could be a sector, a regional group, or an individual business. Or it could be an attack to exploit any entity with known vulnerabilities (e.g. unpatched vulnerabilities on web servers, open ports or services, etc.)
Access is gained through intelligence or through use of automated tools.
Once access is gained there is an automated discovery process to determine which systems and applications are in use. This information will then determine which cyber weapons to use.
The cyber weapons will then exploit the target system / application for its intended use. Cyber weapons are readily available in the hacking community and on the "dark web".
The most sophisticated hackers cover up after the hack so that you may never know that they have been in the systems.
This attack cycle can be very quick, sometimes less than a second or two.



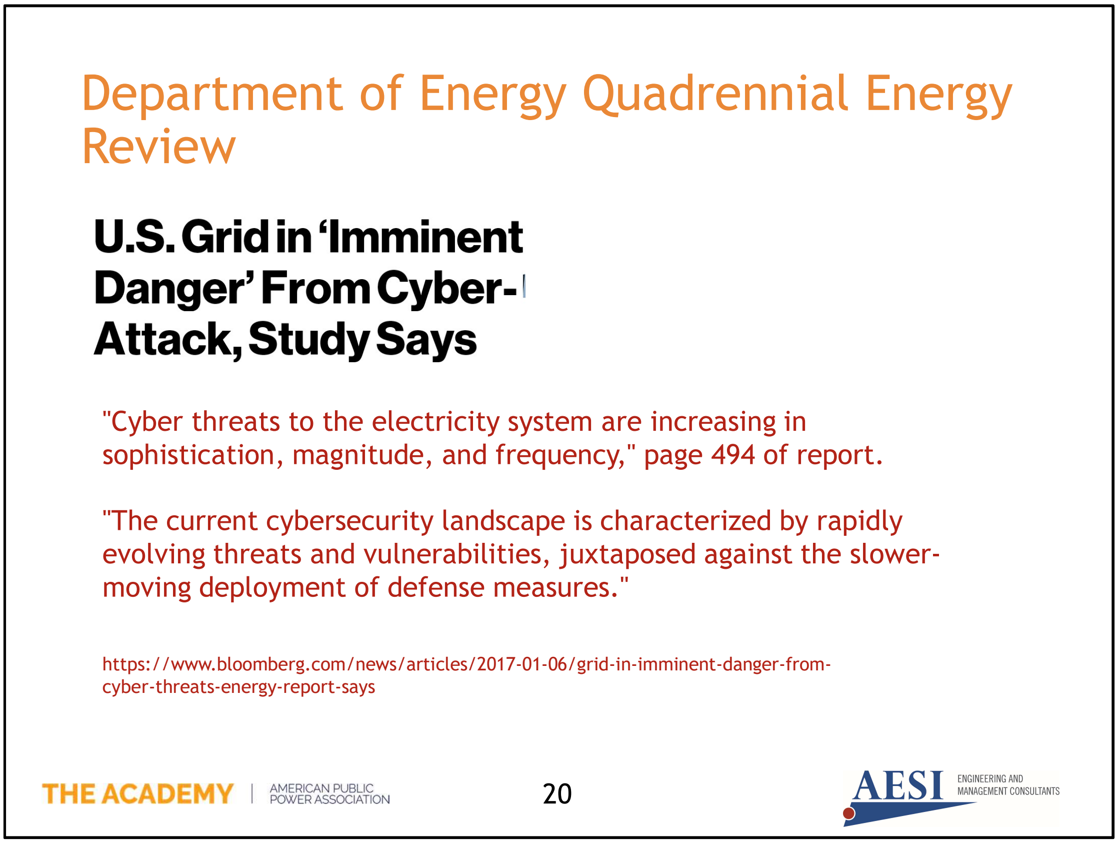
THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION

Recent Incidents & Trends in the Utility Sector

AESI ENGINEERING AND MANAGEMENT CONSULTANTS

AMERICAN PUBLIC POWER ASSOCIATION

PublicPower.org/Academy



Department of Energy Quadrennial Energy Review

U.S. Grid in 'Imminent Danger' From Cyber-Attack, Study Says

"Cyber threats to the electricity system are increasing in sophistication, magnitude, and frequency," page 494 of report.

"The current cybersecurity landscape is characterized by rapidly evolving threats and vulnerabilities, juxtaposed against the slower-moving deployment of defense measures."

https://www.bloomberg.com/news/articles/2017-01-06/grid-in-imminent-danger-from-cyber-threats-energy-report-says

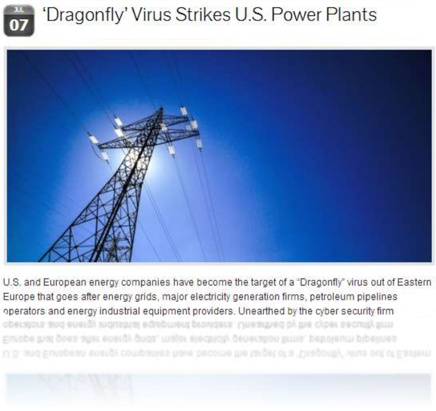
THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION

AESI ENGINEERING AND MANAGEMENT CONSULTANTS

This is from the recent DOE Quadrennial report.

“Rapidly evolving threats” compared to “slower-moving threats” is the DOE’s bottom line assessment.

Targeted Cyber Attacks on Utilities



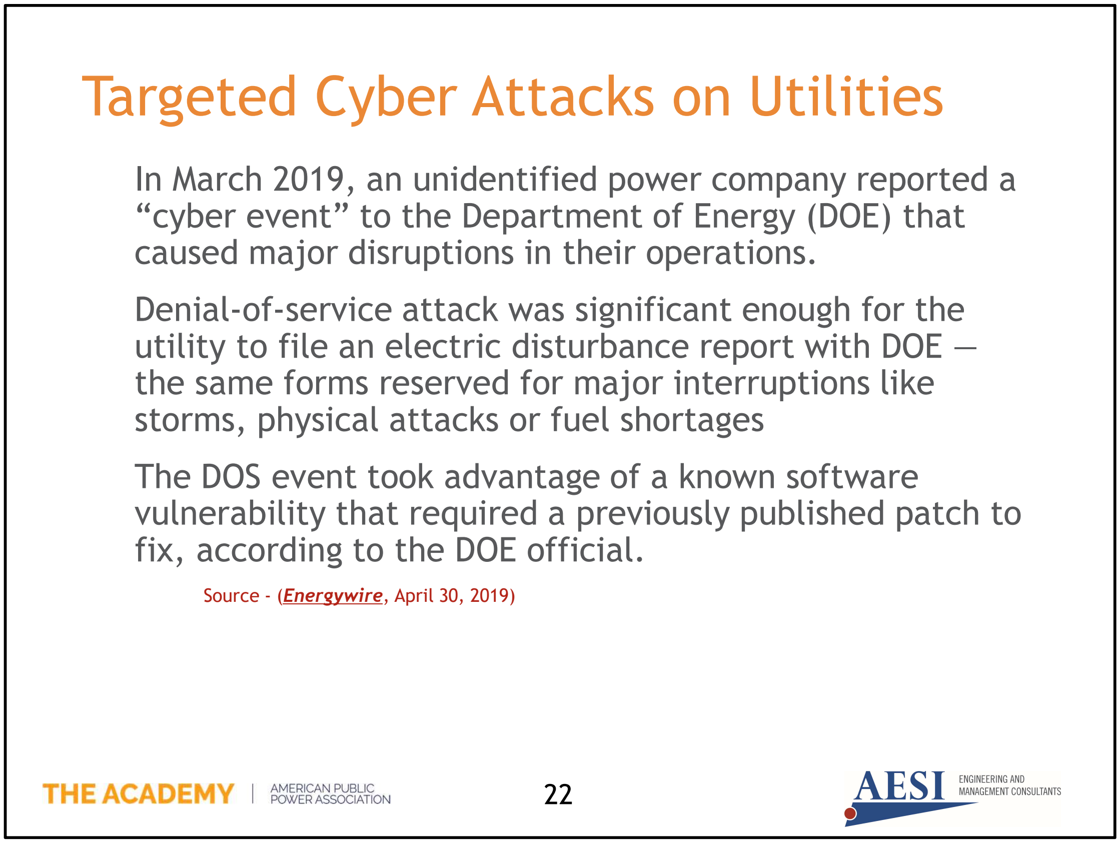
'Dragonfly' Virus Strikes U.S. Power Plants

U.S. and European energy companies have become the target of a "Dragonfly" virus out of Eastern Europe that goes after energy grids, major electricity generation firms, petroleum pipelines operators and energy industrial equipment providers. Unearthed by the cyber security firm

Happening NOW
FOX NEWS
UKRAINE POWER OUTAGE IS FIRST KNOWN "BLACKENERGY" MALWARE ATTACK

This slide depicts two very targeted cyber attacks on utilities.
The first is the Dragonfly virus that affected over 1000 power plants worldwide. The attacks have disrupted industrial control system equipment providers by installing the malware during downloaded updates for computers running the ICS equipment. Most of the targets were in the United States, Spain, France, Italy, Germany Turkey and Poland – all countries belonging to the North Atlantic Treaty Organization.
http://www.wnd.com/2014/07/dragonfly-virus-strikes-u-s-power-plants/#Ls5tpz3mcoDhXh5r.99

The Ukraine Power Outage was a significant outage caused by a phishing attack. Phishing attacks are disguised correspondence (usually e-mails) that aim to bait the recipient into providing access information and / or click on a specific link. This was a very professionally crafted e-mail that legitimately looked to be from the Ukrainian Government. When the recipient clicked on the link, in a matter of minutes the control of the SCADA system was with the hackers and eventually 20+ substations were taken off line creating the power outages.
http://video.foxnews.com/v/4687930728001/?#sp=show-clips



Targeted Cyber Attacks on Utilities

In March 2019, an unidentified power company reported a "cyber event" to the Department of Energy (DOE) that caused major disruptions in their operations.

Denial-of-service attack was significant enough for the utility to file an electric disturbance report with DOE — the same forms reserved for major interruptions like storms, physical attacks or fuel shortages

The DOS event took advantage of a known software vulnerability that required a previously published patch to fix, according to the DOE official.

Source - (***Energywire***, April 30, 2019)

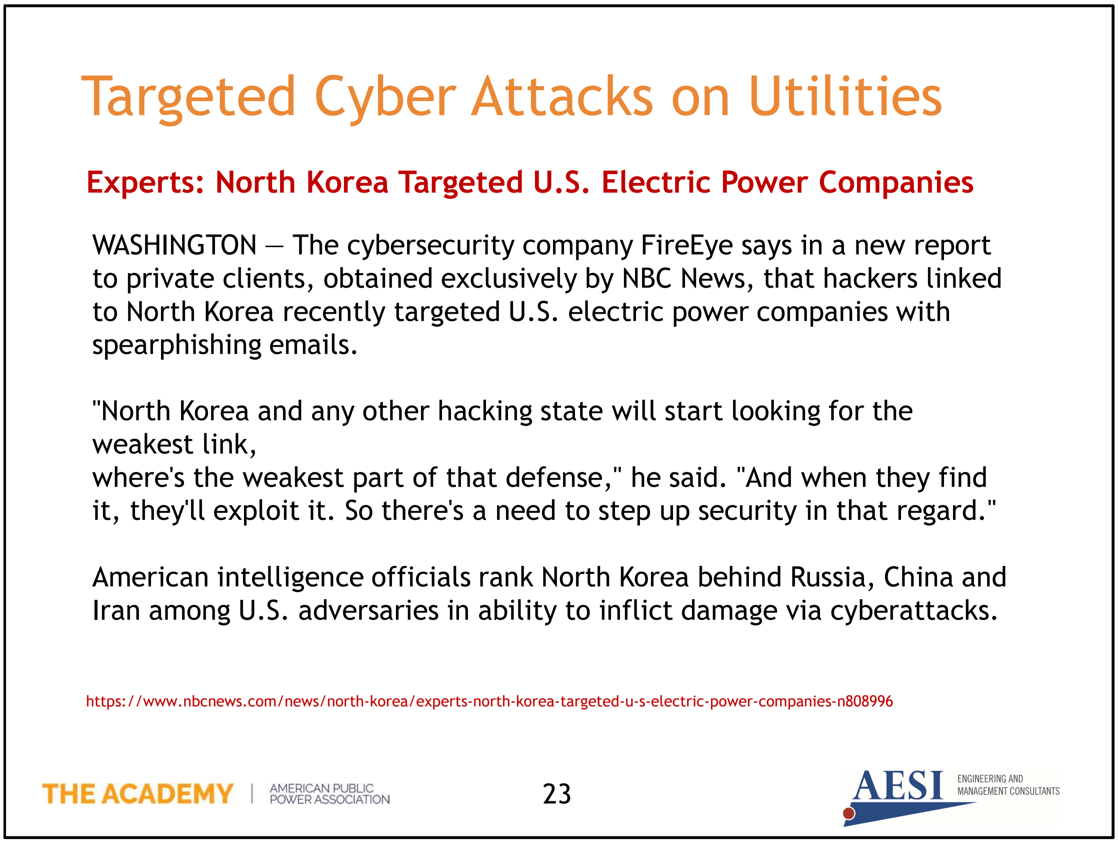
Event caused an undisclosed utility in the western United States to temporarily lose visibility of certain system parts. First time that remote hackers interfered with U.S. grid networks. Affected several states in the West, including California, Utah and Wyoming.

While the event did not cause a blackout or power shortage, it was likened to the impact of a major interruption, including events like severe storms, physical attacks, and fuel shortages.

The DOS occurred at a low-impact control center and multiple remote low-impact generation sites. The incident lasted for 10 hours with each device showing offline status for less than five minutes.

The hacker exploited a known firewall vulnerability at **one of the utility's vendors**, allowing an unauthenticated attacker to cause unexpected reboots of devices, according to NERC's analysis. These unexpected reboots resulted in brief communications outages — less than five minutes — between field devices and the control center.

NERC is urging all utilities to have **as few internet facing devices** as possible on their systems, use a layered defense and employ redundancies for resilience.



Targeted Cyber Attacks on Utilities

Experts: North Korea Targeted U.S. Electric Power Companies

WASHINGTON — The cybersecurity company FireEye says in a new report to private clients, obtained exclusively by NBC News, that hackers linked to North Korea recently targeted U.S. electric power companies with spearphishing emails.

"North Korea and any other hacking state will start looking for the weakest link,
where's the weakest part of that defense," he said. "And when they find it, they'll exploit it. So there's a need to step up security in that regard."

American intelligence officials rank North Korea behind Russia, China and Iran among U.S. adversaries in ability to inflict damage via cyberattacks.

https://www.nbcnews.com/news/north-korea/experts-north-korea-targeted-u-s-electric-power-companies-n808996

This is an article from NBC News on October 17 2017.

Many countries have nation state cyber armies. And they are targeting critical infrastructure in the US. As stated in the article these hackers will look for the weakest link in the grid.

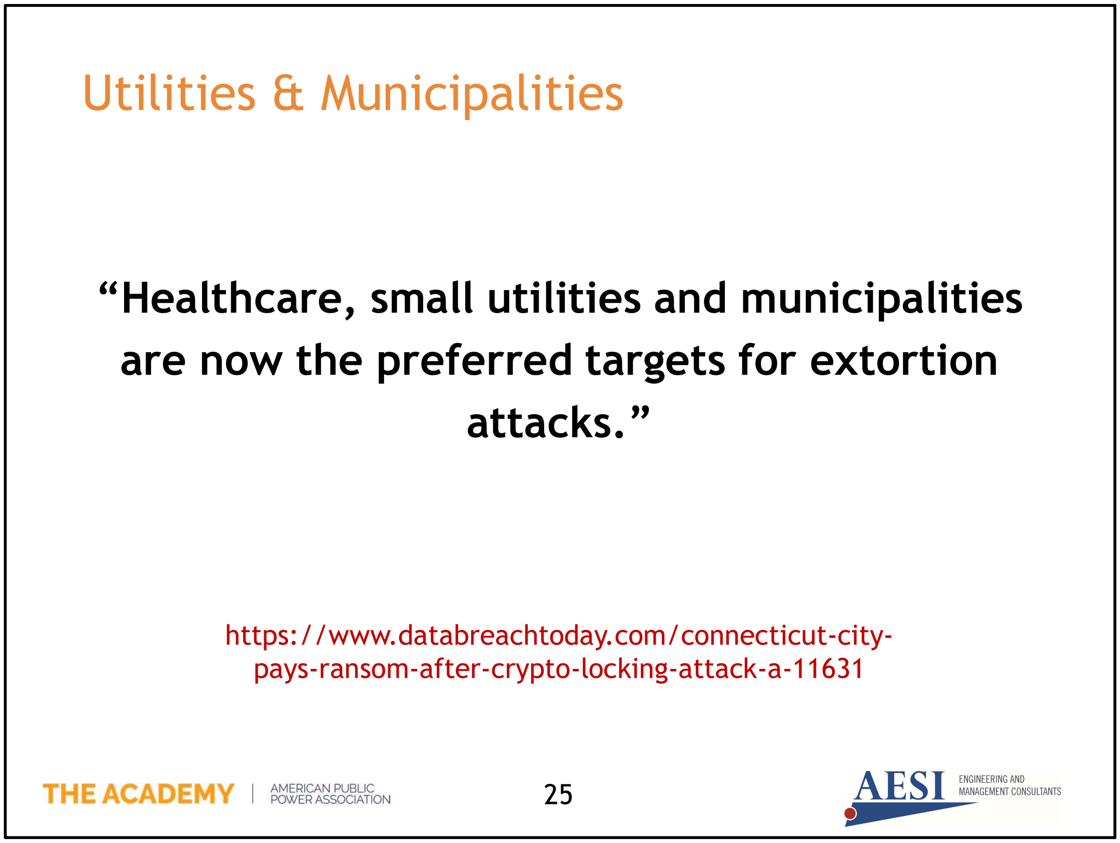
Utility Data Breach

“San Francisco-based PG&E Corp. was identified as the large utility that authorities had fined in May for leaving confidential information about its operations exposed on the internet for over two months…

An investigation into the data breach found that an unnamed vendor hired by PG&E downloaded data to his own computer—without the utility’s permission and in violation of company policy—then left it exposed to the internet until it was brought to PG&E’s attention.”

PG&E was fined $2.7M.

Wall Street Journal, Energy Journal, “PG&E Identified as Utility That Lost Control of Confidential Information”, Aug 27 2018



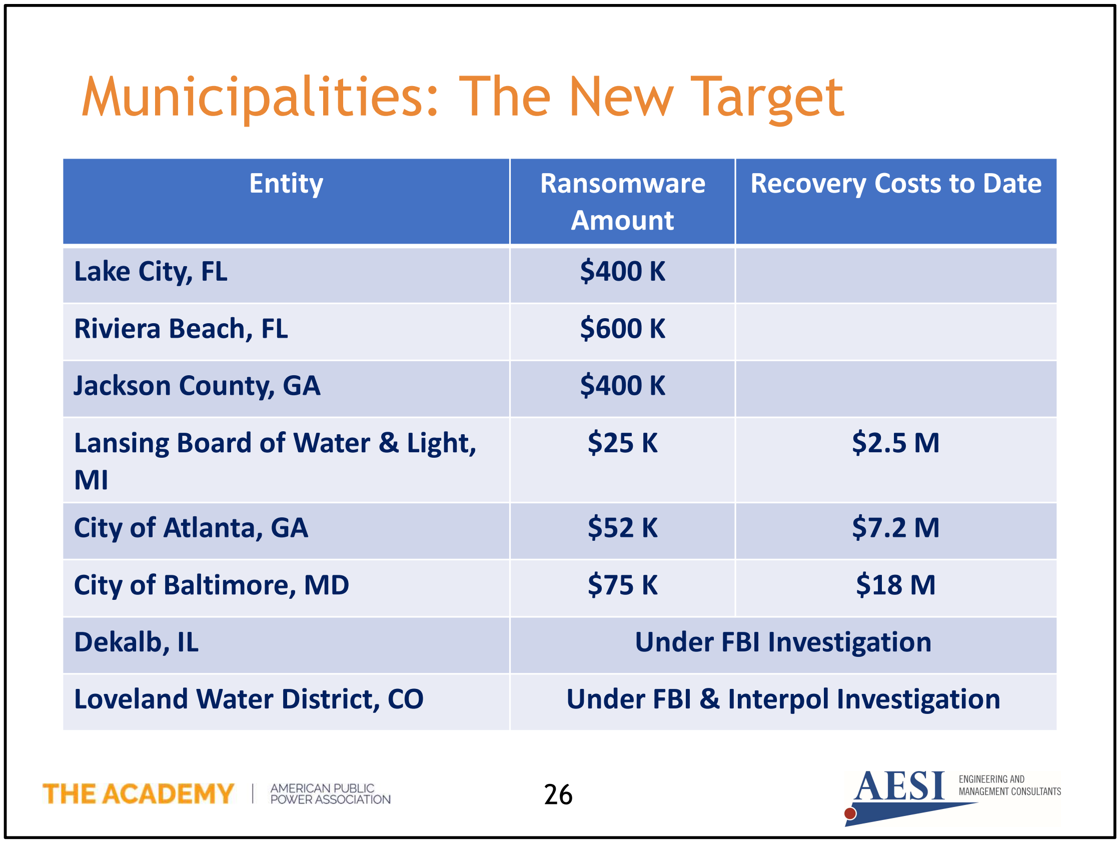
Utilities & Municipalities

“Healthcare, small utilities and municipalities are now the preferred targets for extortion attacks.”

https://www.databreachtoday.com/connecticut-city-pays-ransom-after-crypto-locking-attack-a-11631

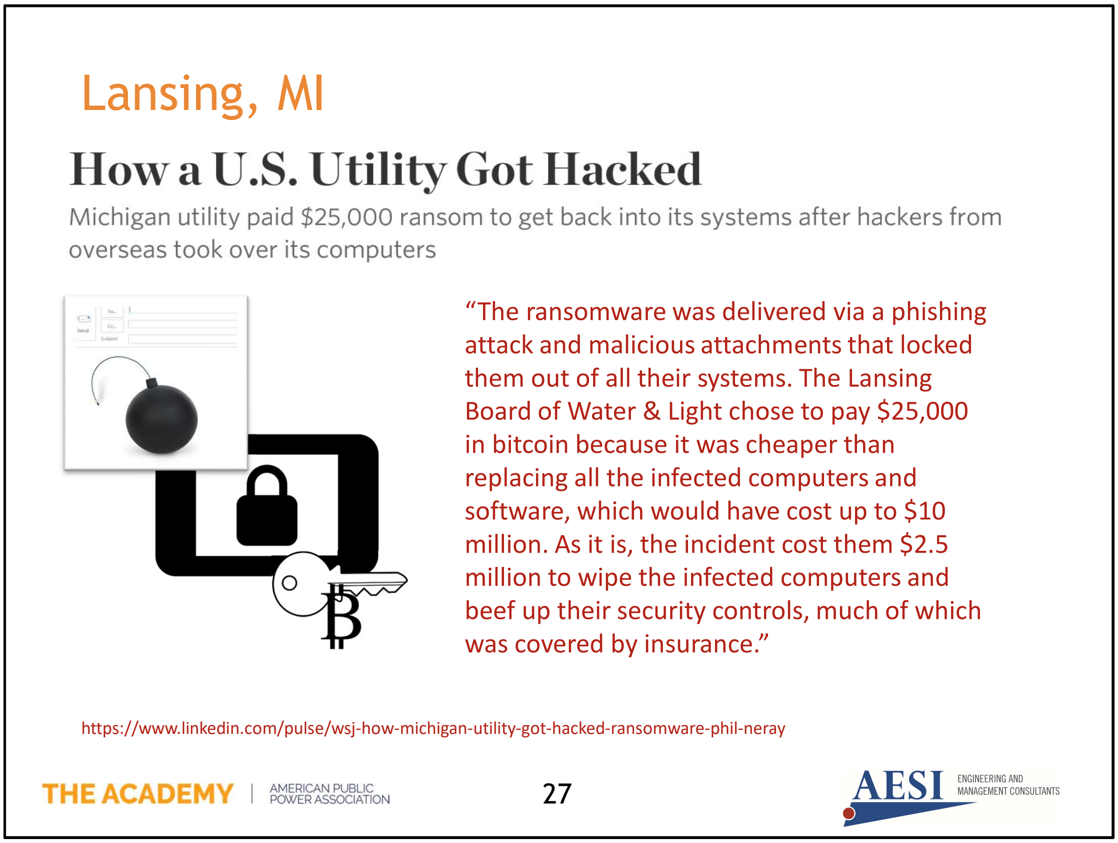
Financial Services will always be a top target for breaches since “they have the money”.

But utilities and municipalities are now becoming a preferred target since they a) have a large attack surface b) have many vuleranbilites and c) have the ability to pay ransomware.



Municipalities: The New Target

Entity	Ransomware Amount	Recovery Costs to Date
Lake City, FL	$400 K	
Riviera Beach, FL	$600 K	
Jackson County, GA	$400 K	
Lansing Board of Water & Light, MI	$25 K	$2.5 M
City of Atlanta, GA	$52 K	$7.2 M
City of Baltimore, MD	$75 K	$18 M
Dekalb, IL	Under FBI Investigation	
Loveland Water District, CO	Under FBI & Interpol Investigation	



Lansing, MI

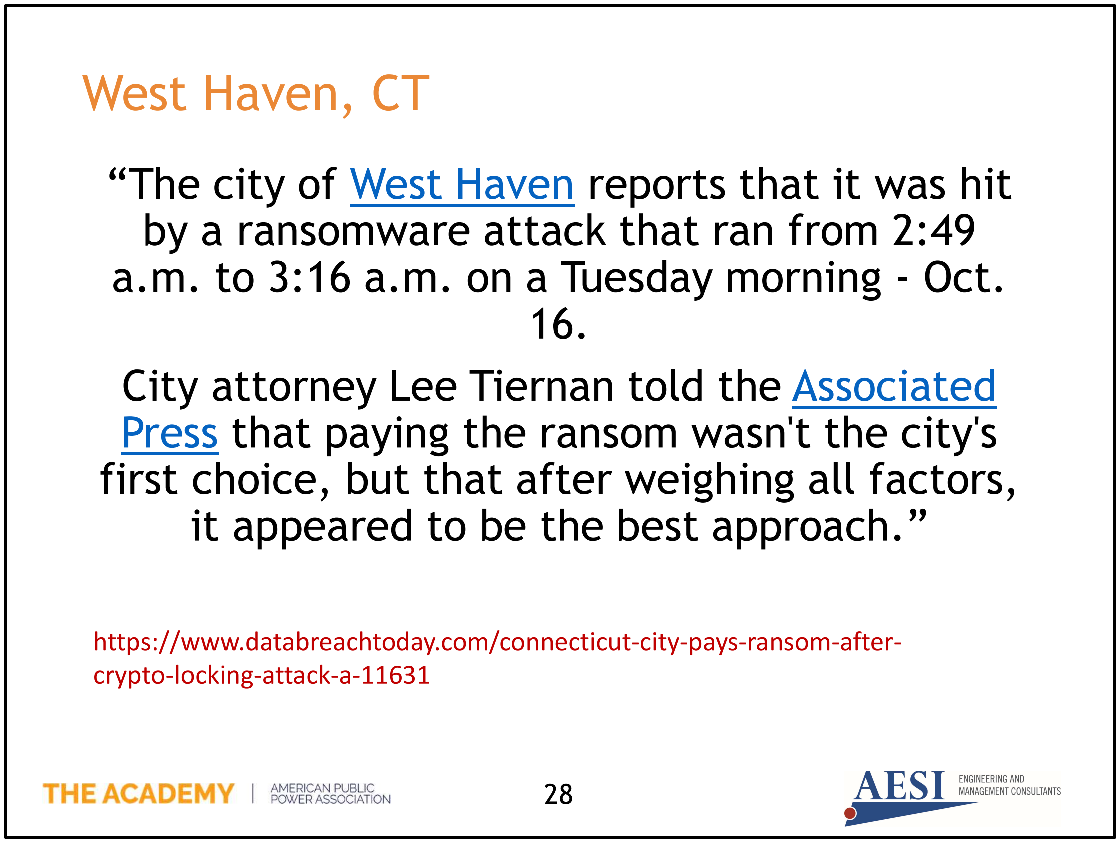
How a U.S. Utility Got Hacked

Michigan utility paid $25,000 ransom to get back into its systems after hackers from overseas took over its computers

"The ransomware was delivered via a phishing attack and malicious attachments that locked them out of all their systems. The Lansing Board of Water & Light chose to pay $25,000 in bitcoin because it was cheaper than replacing all the infected computers and software, which would have cost up to $10 million. As it is, the incident cost them $2.5 million to wipe the infected computers and beef up their security controls, much of which was covered by insurance."

https://www.linkedin.com/pulse/wsj-how-michigan-utility-got-hacked-ransomware-phil-neray

This article describes a very painful and expensive process for a public power entity after a ransomware attack.

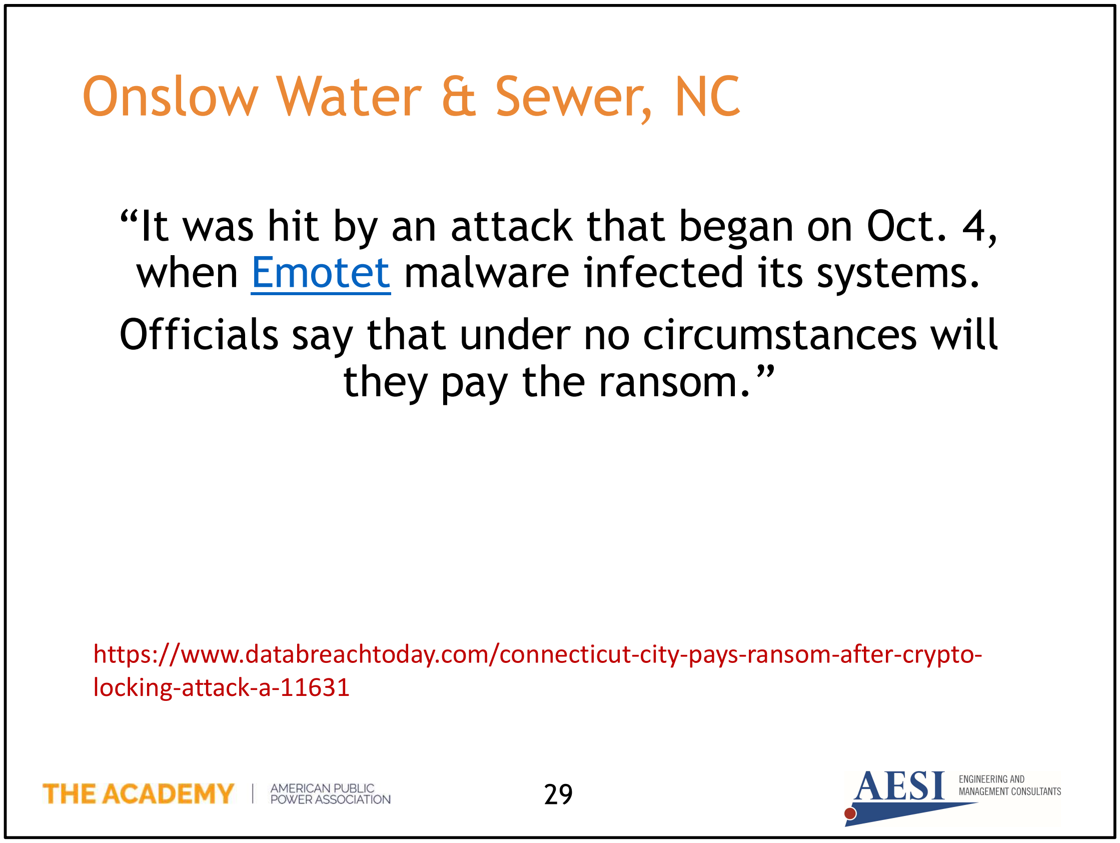


West Haven, CT

“The city of West Haven reports that it was hit by a ransomware attack that ran from 2:49 a.m. to 3:16 a.m. on a Tuesday morning - Oct. 16.

City attorney Lee Tiernan told the Associated Press that paying the ransom wasn't the city's first choice, but that after weighing all factors, it appeared to be the best approach.”

https://www.databreachtoday.com/connecticut-city-pays-ransom-after-crypto-locking-attack-a-11631

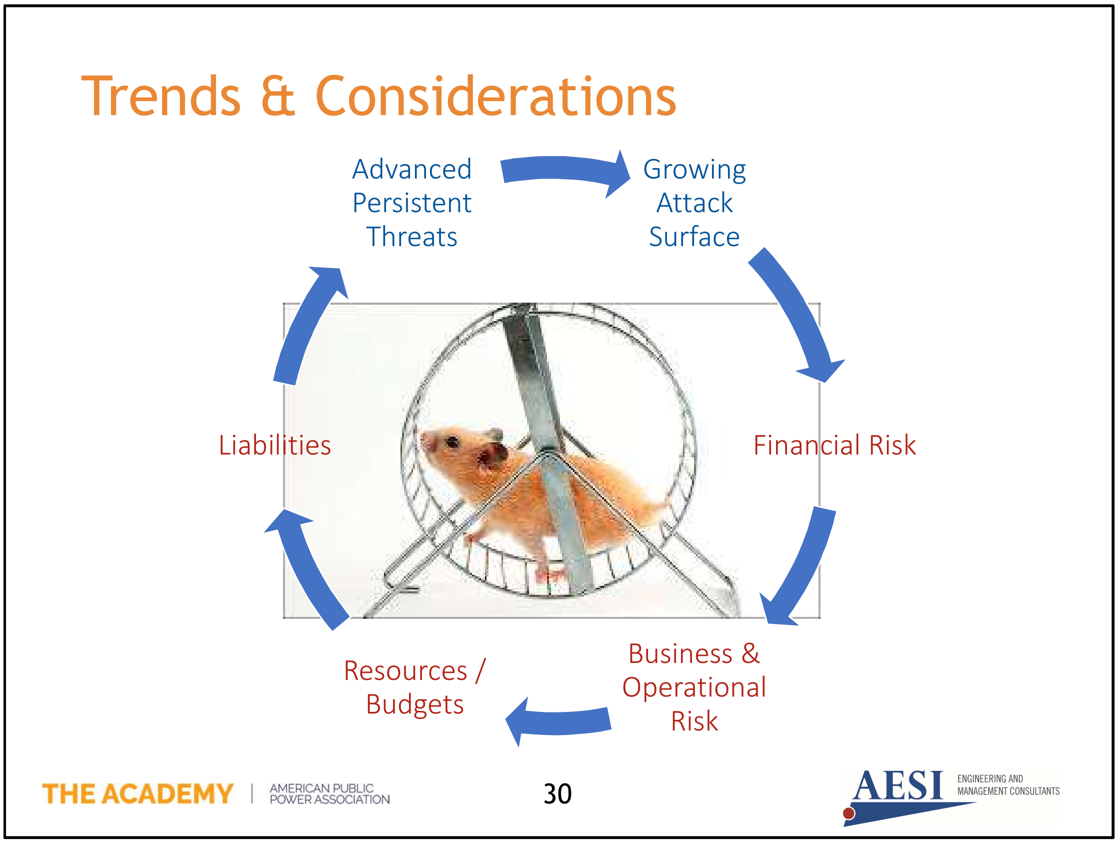


Onslow Water & Sewer, NC

"It was hit by an attack that began on Oct. 4, when Emotet malware infected its systems.

Officials say that under no circumstances will they pay the ransom."

https://www.databreachtoday.com/connecticut-city-pays-ransom-after-crypto-locking-attack-a-11631



Trends & Considerations

Advanced Persistent Threats

Growing Attack Surface

Financial Risk

Business & Operational Risk

Resources / Budgets

Liabilities

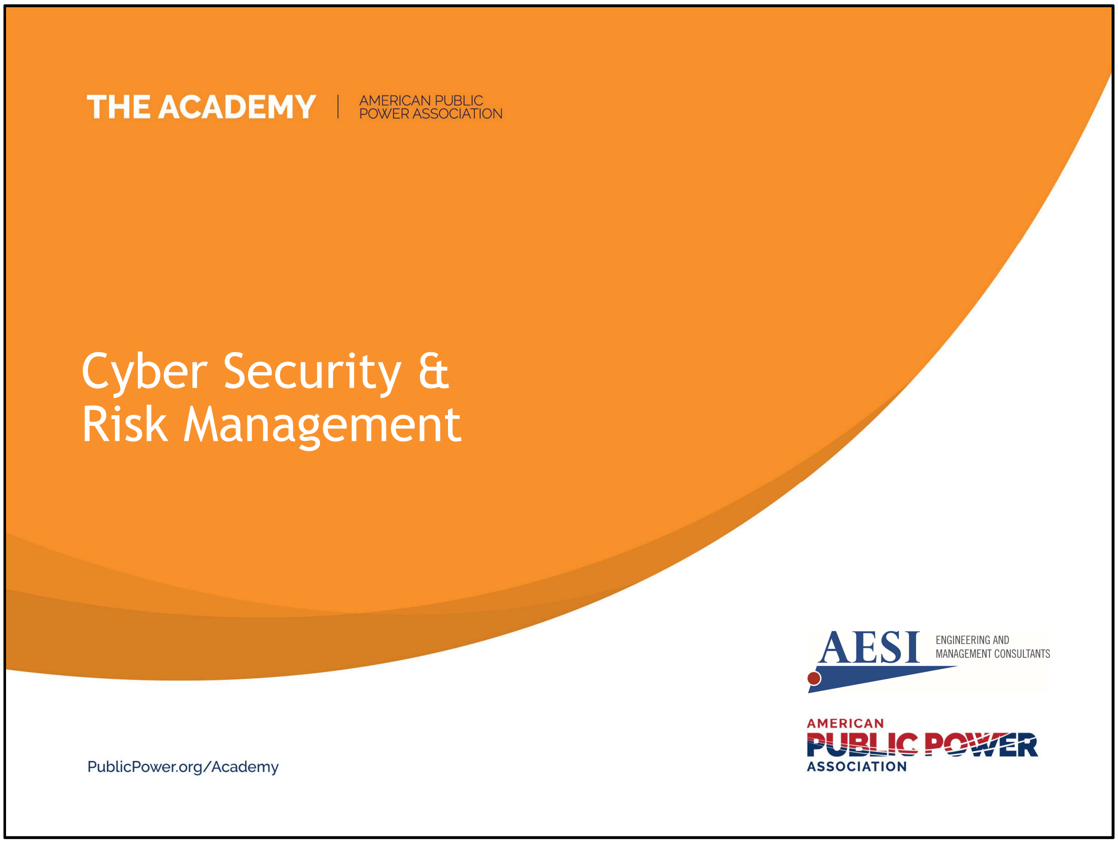
THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION

30

AESI ENGINEERING AND MANAGEMENT CONSULTANTS

Going forward, the threat landscape will continue to see increasing Advanced Persistent Threats (APTs) on critical infrastructure. With increasing automation and increasing grid connectivity the utilities attack surface will continue to grow. Utilities such as MEUW Members need to be concerned about growing litigation in this area and potential financial risk from cyber attacks.

Further on in the training session we will describe how to look at business & operational risk and will provide some proxies and references for appropriate budgets.



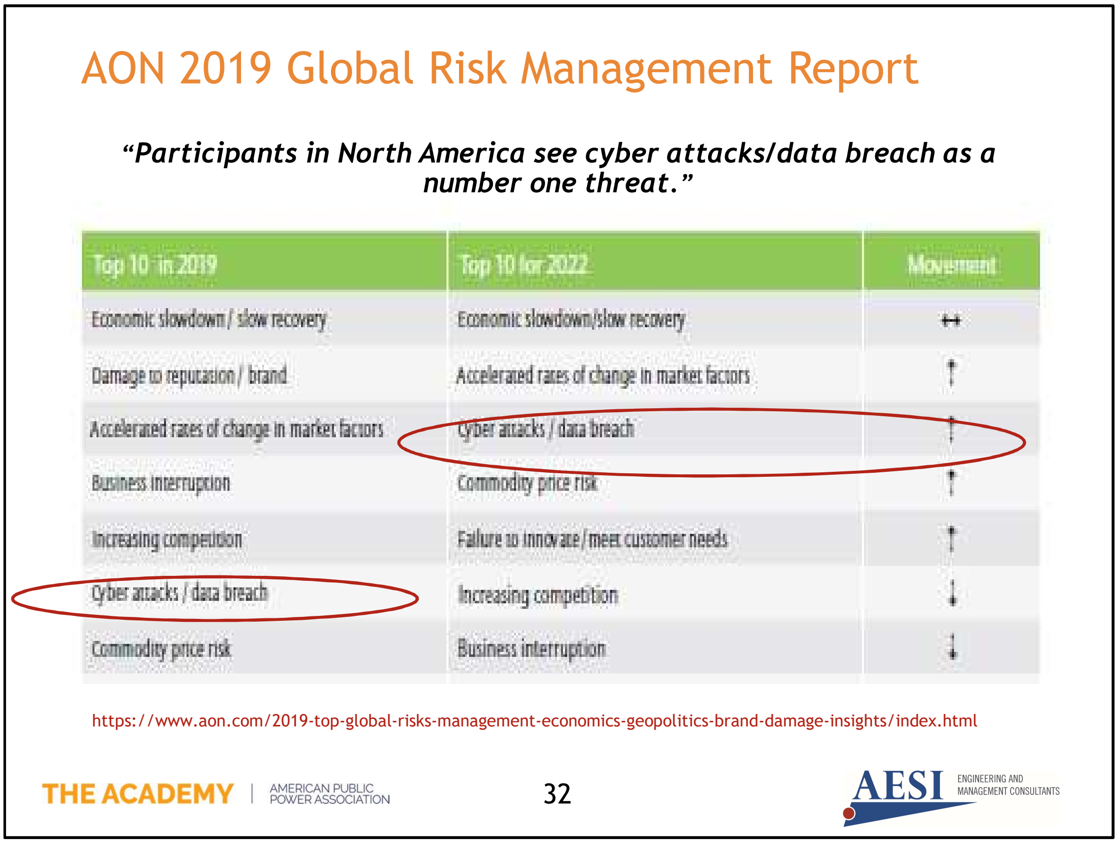
THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION

Cyber Security & Risk Management

AESI ENGINEERING AND MANAGEMENT CONSULTANTS

AMERICAN PUBLIC POWER ASSOCIATION

PublicPower.org/Academy



AON 2019 Global Risk Management Report

"Participants in North America see cyber attacks/data breach as a number one threat."

Top 10 in 2019	Top 10 for 2022	Movement
Economic slowdown / slow recovery	Economic slowdown/slow recovery	↔
Damage to reputation / brand	Accelerated rates of change in market factors	↑
Accelerated rates of change in market factors	Cyber attacks / data breach	↑
Business interruption	Commodity price risk	↑
Increasing competition	Failure to innovate / meet customer needs	↑
Cyber attacks / data breach	Increasing competition	↓
Commodity price risk	Business interruption	↓

https://www.aon.com/2019-top-global-risks-management-economics-geopolitics-brand-damage-insights/index.html

THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION

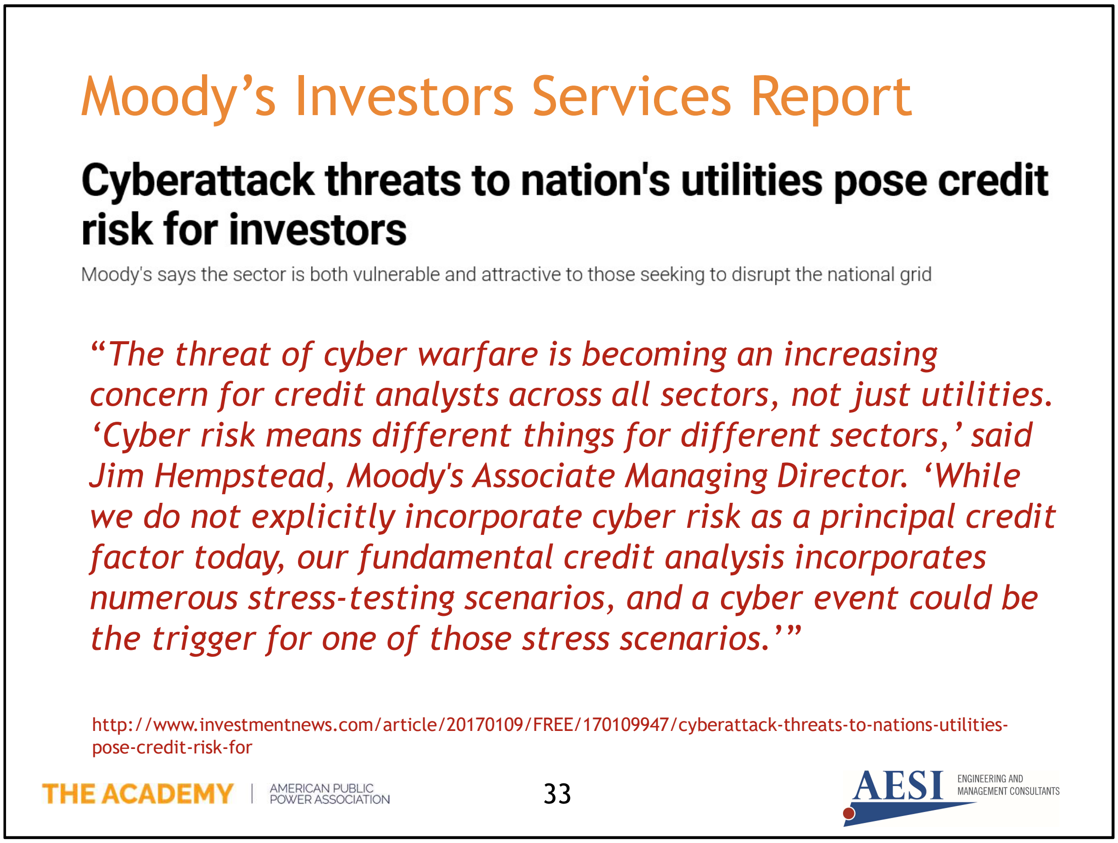
32

AESI ENGINEERING AND MANAGEMENT CONSULTANTS

This slide is a summary of the Top Risks from AON's 2019 Global Risk report.

Computer crimes / hacking emerged as an overall Top 10 risk for enterprises for the first time in 2015, and was up four spots to #5 in 2017. Further, there is clearly a link between computer crimes / hacking and the #1 risk of Damage to Reputation / Brand.

The projections show that cyber breaches will increase from a risk perspective.



Moody’s Investors Services Report

Cyberattack threats to nation's utilities pose credit risk for investors

Moody's says the sector is both vulnerable and attractive to those seeking to disrupt the national grid

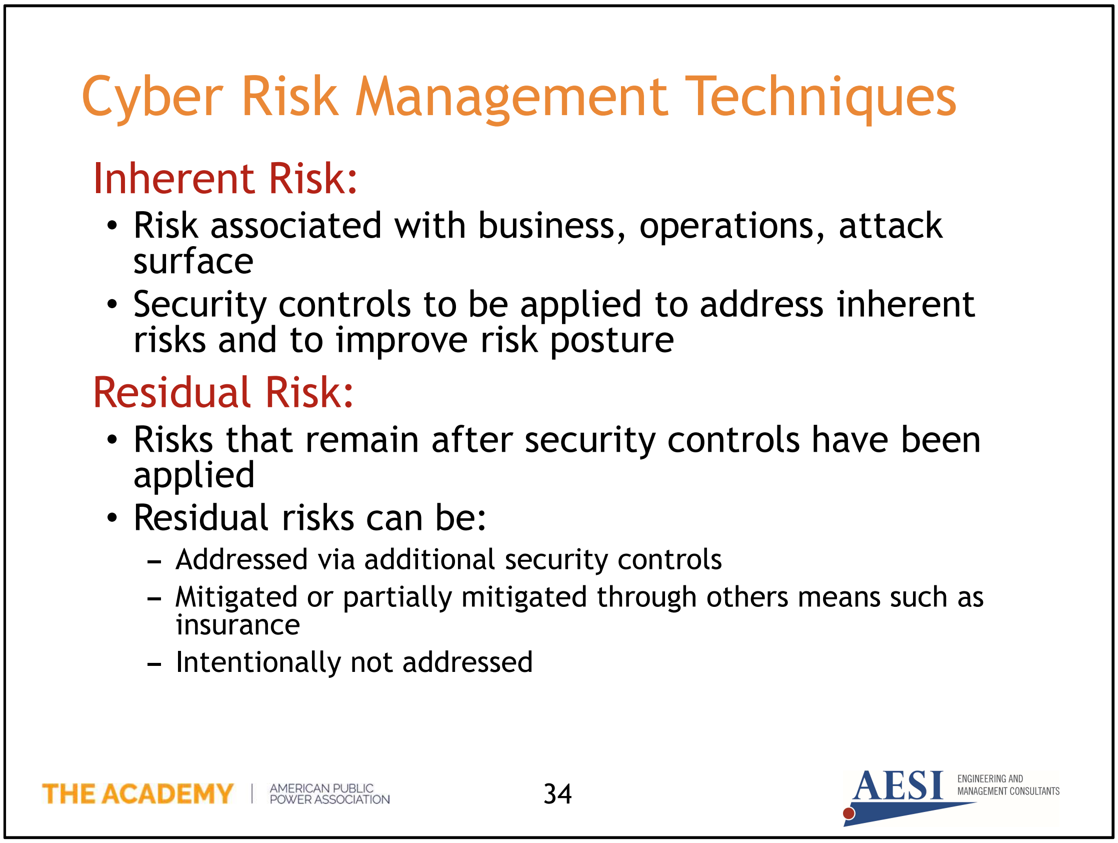
“The threat of cyber warfare is becoming an increasing concern for credit analysts across all sectors, not just utilities. ‘Cyber risk means different things for different sectors,’ said Jim Hempstead, Moody's Associate Managing Director. ‘While we do not explicitly incorporate cyber risk as a principal credit factor today, our fundamental credit analysis incorporates numerous stress-testing scenarios, and a cyber event could be the trigger for one of those stress scenarios.’”

http://www.investmentnews.com/article/20170109/FREE/170109947/cyberattack-threats-to-nations-utilities-pose-credit-risk-for

Credit analysts are now looking at the cyber security issue.

Ability to prove due diligence in cyber security will become a more important in the credit process.

Due diligence includes development, implementation and documentation of the utility’s cyber security program, all commensurate with risk.



Cyber Risk Management Techniques

Inherent Risk:

- Risk associated with business, operations, attack surface
- Security controls to be applied to address inherent risks and to improve risk posture

Residual Risk:

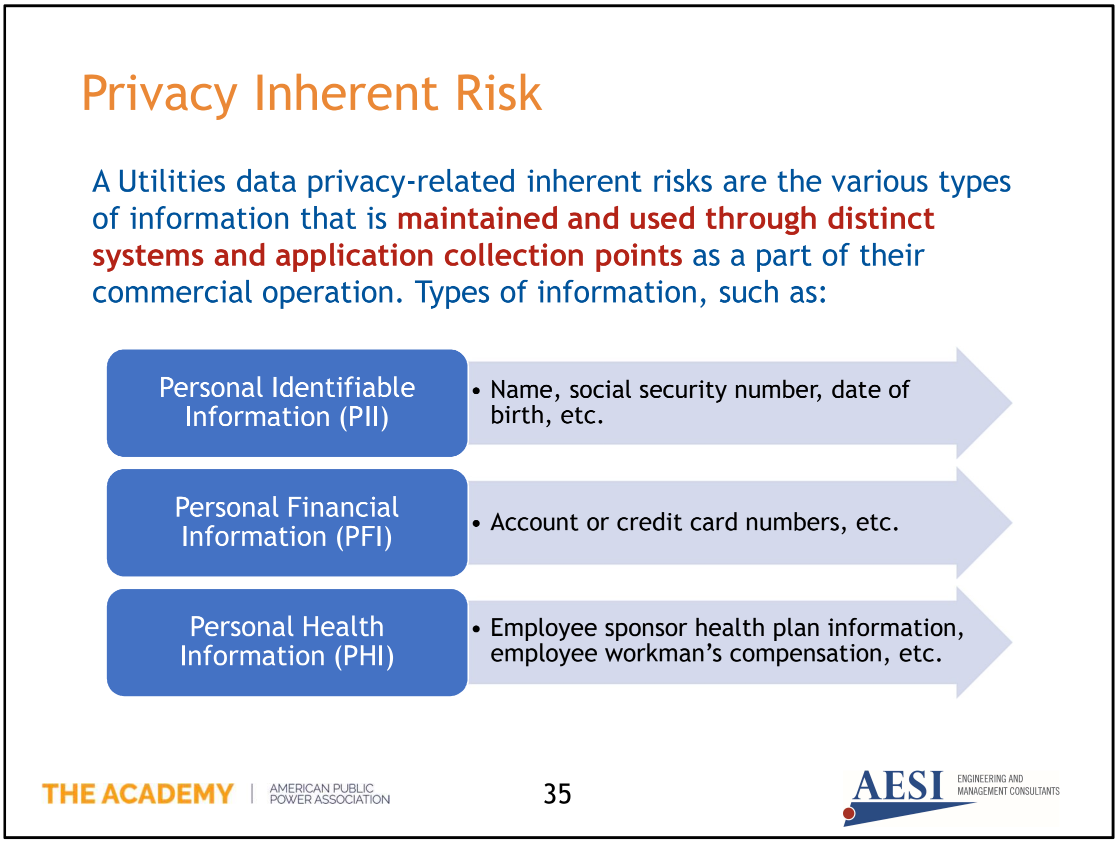
- Risks that remain after security controls have been applied
- Residual risks can be:
  - Addressed via additional security controls
  - Mitigated or partially mitigated through others means such as insurance
  - Intentionally not addressed

THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION 34 AESI ENGINEERING AND MANAGEMENT CONSULTANTS

To address risk management related to cyber security it is important to distinguish between inherent risk and residual risk.

Inherent risk is the risk that is fundamental to the aspects of the business and the operation. The attack surface is a large determinant of inherent risk. You want to first address your inherent risk and then implement security controls. Too many entities will jump to security controls (e.g. install a firewall) before assessing their inherent risk.

After security controls are implemented there will always be some residual risk remaining, which goes to the adage that nothing is ever 100% secure. Residual risk can then be addressed via one or more of the areas shown on the slide.



Privacy Inherent Risk

A Utilities data privacy-related inherent risks are the various types of information that is **maintained and used through distinct systems and application collection points** as a part of their commercial operation. Types of information, such as:

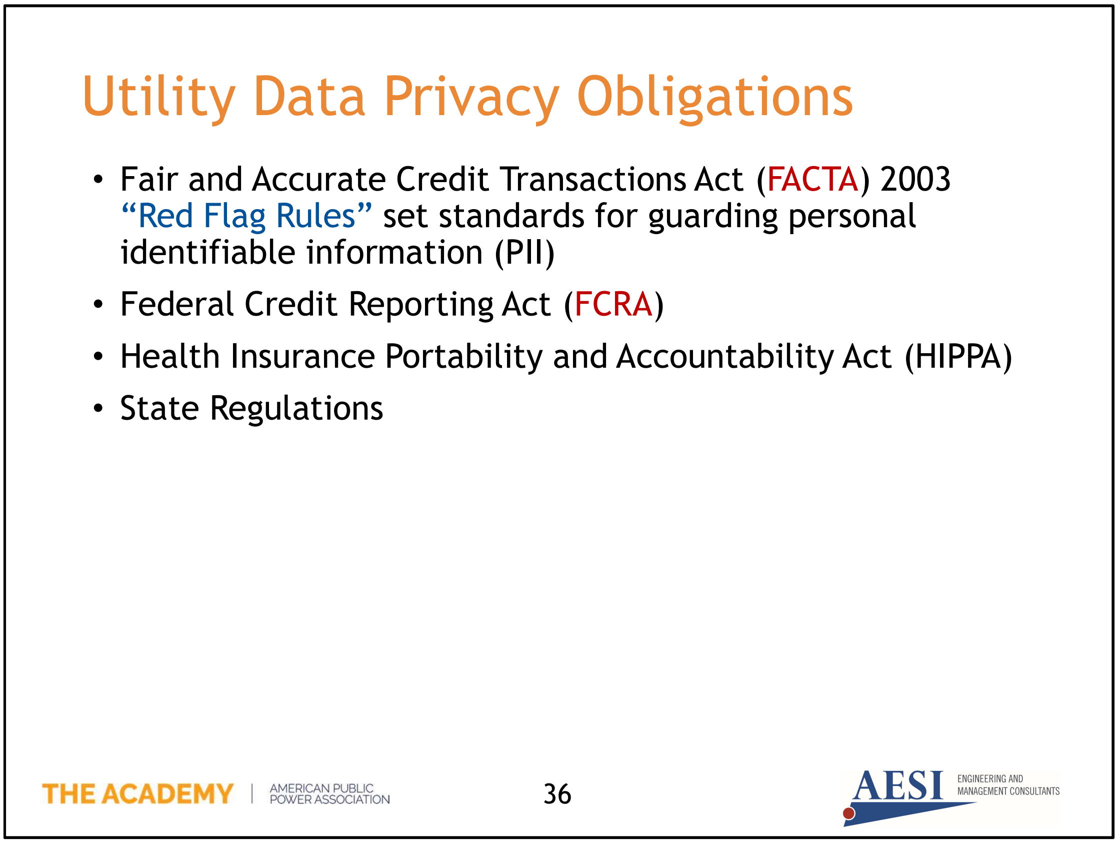
Personal Identifiable Information (PII)
- Name, social security number, date of birth, etc.

Personal Financial Information (PFI)
- Account or credit card numbers, etc.

Personal Health Information (PHI)
- Employee sponsor health plan information, employee workman’s compensation, etc.

Privacy is tightly linked with security, as Utilities maintain and use various types personal information through distinct systems and application collection points.

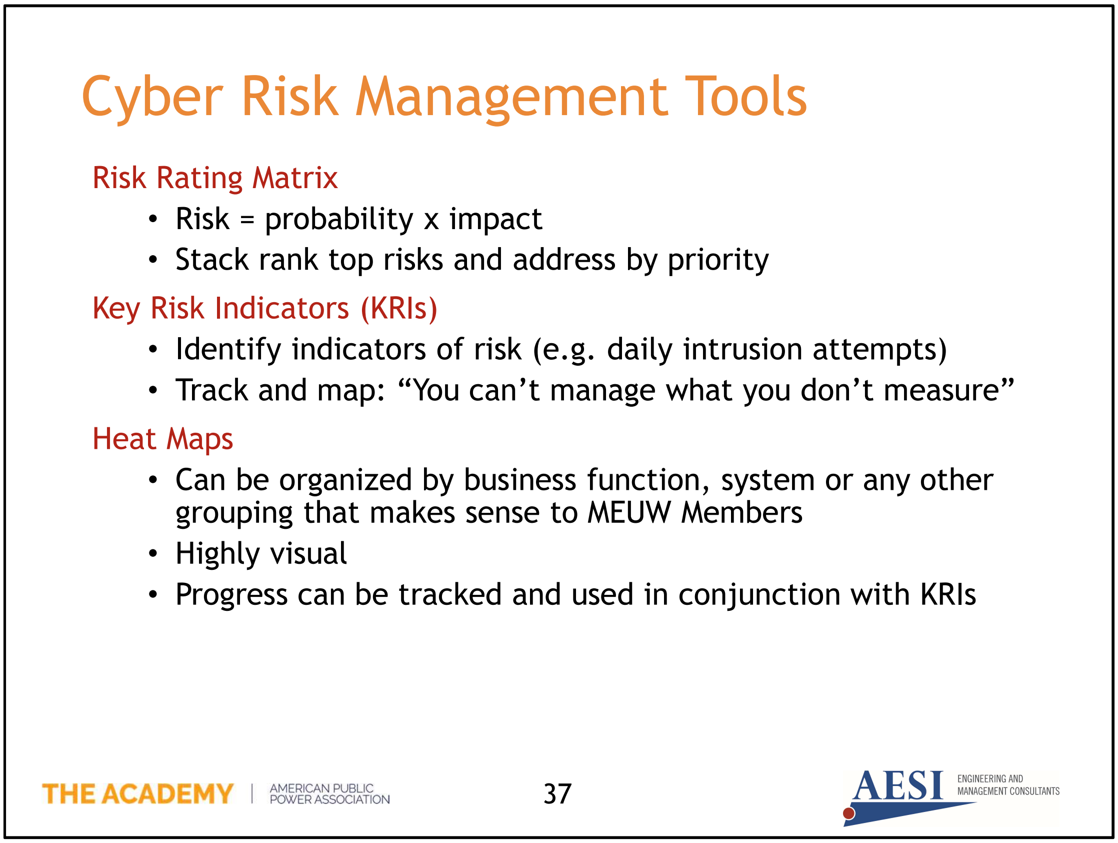
We recommend that utilities address privacy with their cyber security program. This is much more effective and efficient approach.



Utility Data Privacy Obligations

- Fair and Accurate Credit Transactions Act (FACTA) 2003 "Red Flag Rules" set standards for guarding personal identifiable information (PII)
- Federal Credit Reporting Act (FCRA)
- Health Insurance Portability and Accountability Act (HIPPA)
- State Regulations

- As a creditor, Utilities are accountable under the Red Flag Rules for preventing identity theft of it's employee and customer personal data.
- Utilities are required to accurately report and correct discrepancies associated with consumer data to nationwide consumer reporting agency
- Utilities are applicable to HIPAA as administrators of employer sponsored employee healthcare plans. Including continuation of coverage per COBRA requirements
- To date Privacy has been address at the State-level. However, privacy is evolving in the U.S. at the federal level



Cyber Risk Management Tools

Risk Rating Matrix

- Risk = probability x impact
- Stack rank top risks and address by priority

Key Risk Indicators (KRIs)

- Identify indicators of risk (e.g. daily intrusion attempts)
- Track and map: “You can’t manage what you don’t measure”

Heat Maps

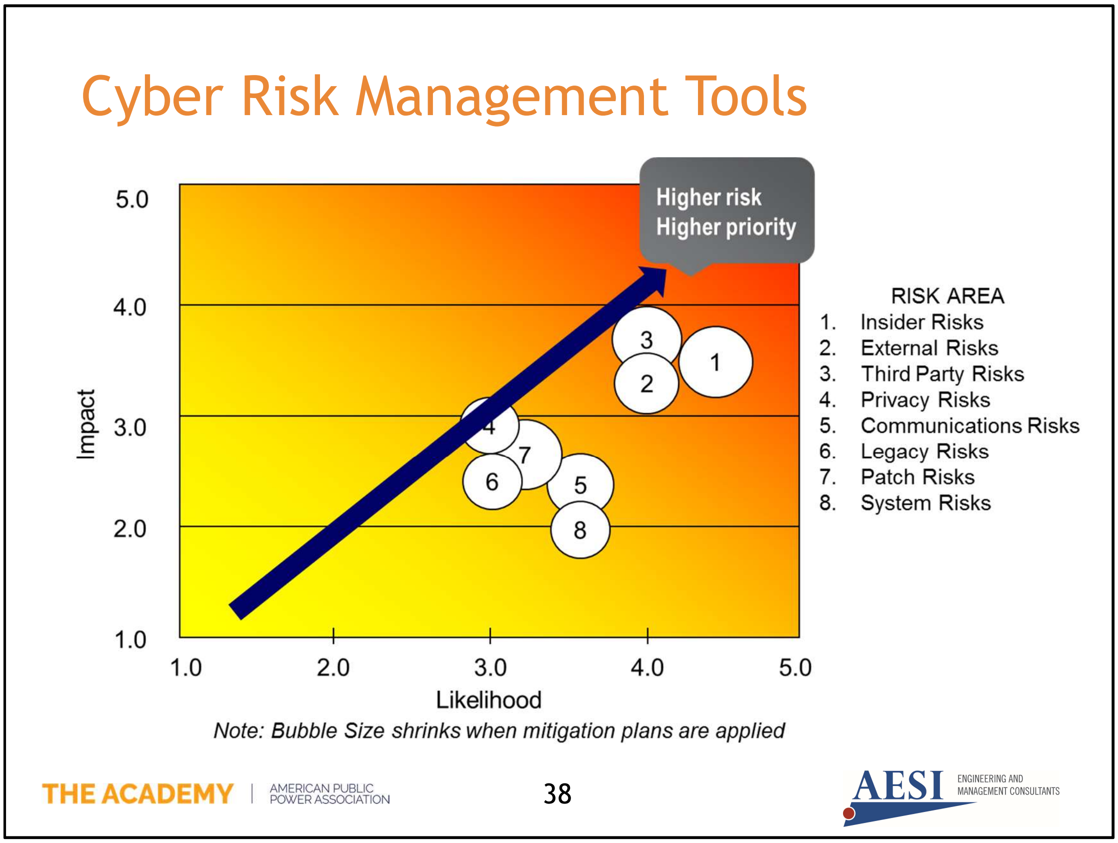
- Can be organized by business function, system or any other grouping that makes sense to MEUW Members
- Highly visual
- Progress can be tracked and used in conjunction with KRIs

There are various tools that MEUW Members can use to identify and manage its risk.   Identifying risk areas is the start.

Once the risk areas have been identified they should be ranked.   One technique is to develop a risk rating matrix in which risk = probability * impact.   In doing this you will recognize that there will be subjectivity to the exercise.   The results will be better if group discussions are used to identify probability and impact.

Coming from this exercise MEUW Members can determine a set of key metrics to focus on, and they are called Key Risk Indicators (KRIs).   Similar to KPIs for processes, KRIs are indicators that are important to monitor and understand as it relates to understanding and improving MEUW Members' risk posture.

Heat Maps are an excellent tool for Boards and Executive Teams and are described on the next slide.



Cyber Risk Management Tools

RISK AREA

1. Insider Risks
2. External Risks
3. Third Party Risks
4. Privacy Risks
5. Communications Risks
6. Legacy Risks
7. Patch Risks
8. System Risks

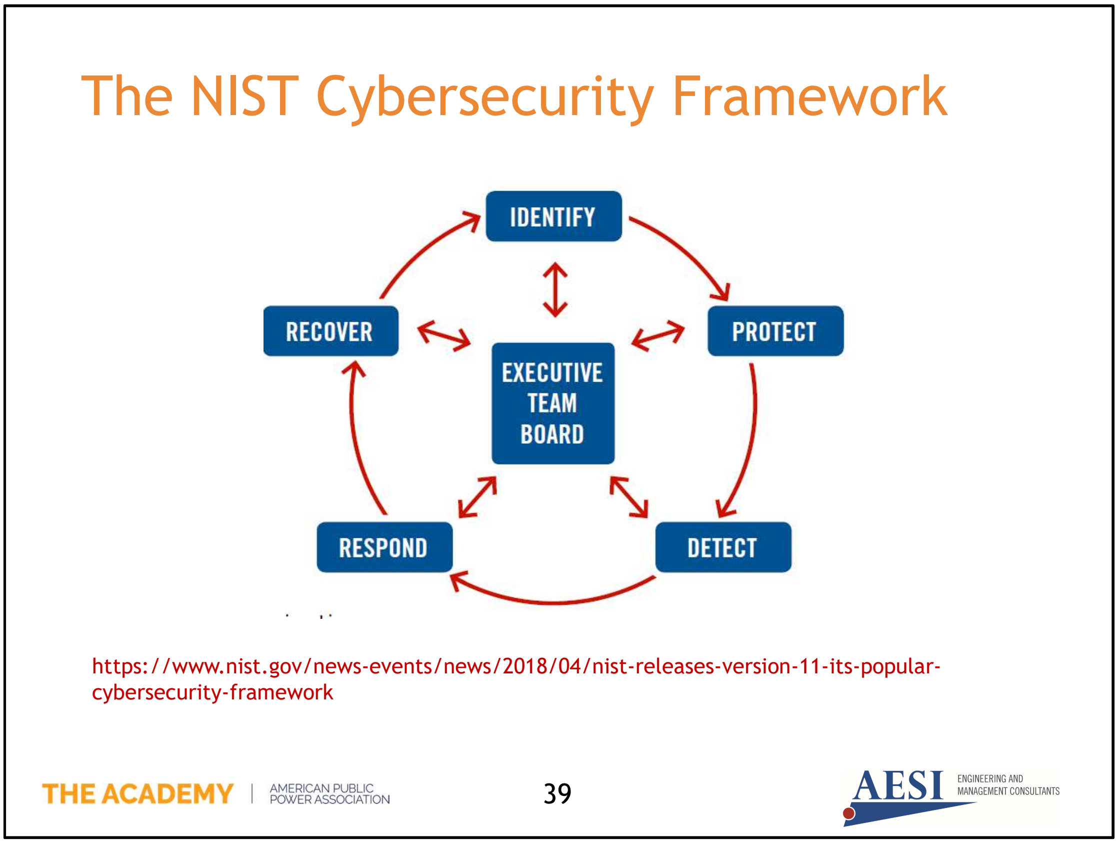
Note: Bubble Size shrinks when mitigation plans are applied

THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION 38 AESI ENGINEERING AND MANAGEMENT CONSULTANTS

Heat Maps are used as a visual tool to illustrate and manage risk. The x and y axis are the same characteristics as used in the Risk Rating Matrix described in the previous slide.

MEUW Members can choose to map whatever elements make sense to them. It could be system type (e.g. SCADA, AMI, Billing, etc.); it could be function (e.g. Field Operations, Engineering, Customer Service, etc.) or it could even be by facility (e.g. Head Office, Control Centre, Substations, etc.). It is important to select the elements that best roll-up into MEUW Members' overall risk management program.

After you position the element on the map you determine the amount of security controls that have been applied to that element. A low number of controls translates into a larger bubble. As you begin to apply more controls the bubble size shrinks. You can overall Heat Maps from one period to another (e.g. from Q2 to Q1) to visually see progress and changes.



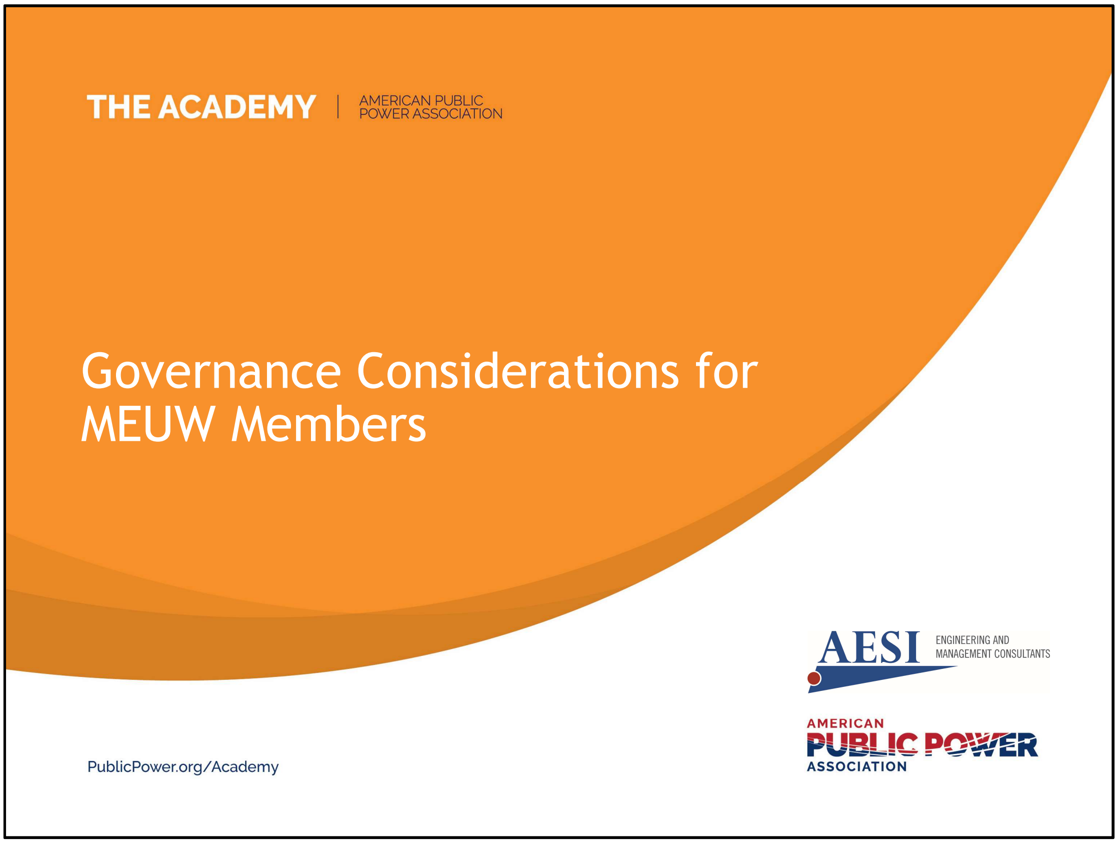
The NIST Cybersecurity Framework

https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

This slide illustrate how MEUW Members can think of the NIST Framework i.e. a closed loop process that can feed information to Executive / Management Teams and their Boards of Directors.

NERC CIP is very much as asset-based standard focusing on protection of large assets such as power plants, control centres, and substations.

The NIST Cybersecurity Framework takes a more holistic approach and includes all IT and OT elements, including business and operational risk to the entity.



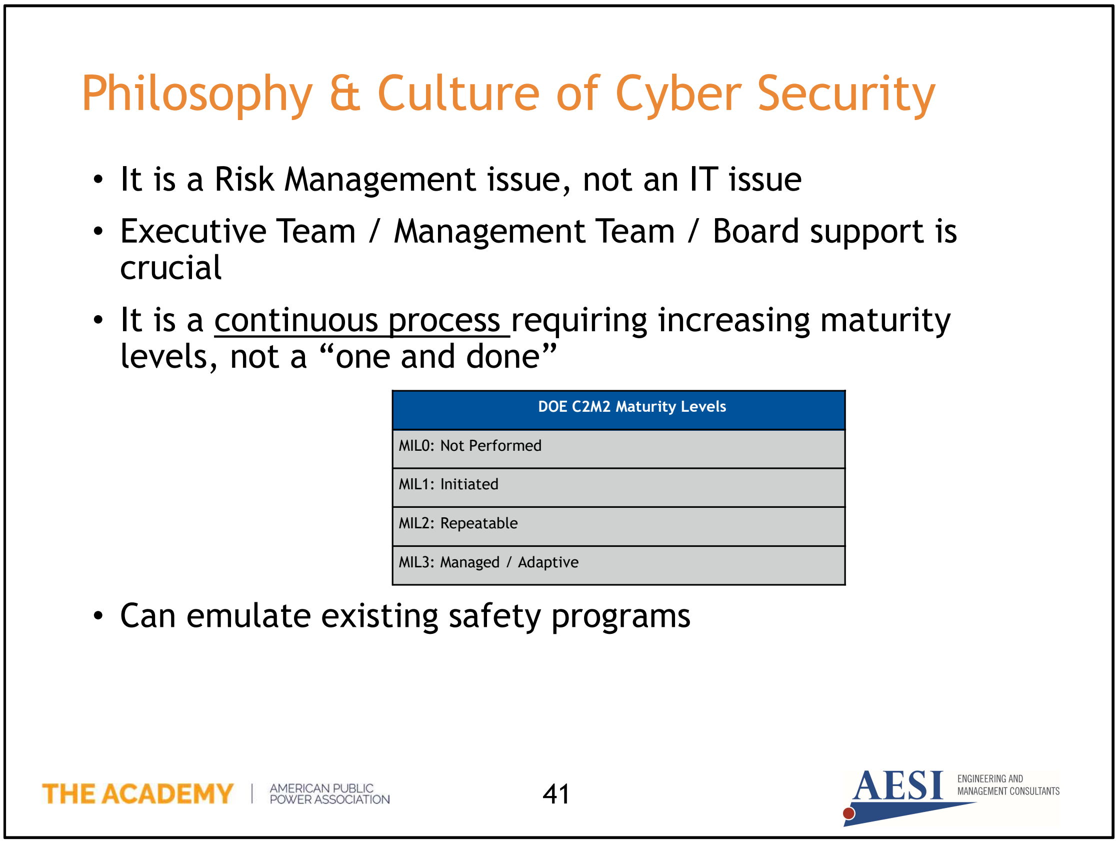
THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION

Governance Considerations for MEUW Members

AESI ENGINEERING AND MANAGEMENT CONSULTANTS

AMERICAN PUBLIC POWER ASSOCIATION

PublicPower.org/Academy



Philosophy & Culture of Cyber Security

- It is a Risk Management issue, not an IT issue
- Executive Team / Management Team / Board support is crucial
- It is a continuous process requiring increasing maturity levels, not a “one and done”

DOE C2M2 Maturity Levels
MIL0: Not Performed
MIL1: Initiated
MIL2: Repeatable
MIL3: Managed / Adaptive

- Can emulate existing safety programs

Key point: Cyber security is a risk management issue, not an IT issue.

The Executive / Management Team / Board support is crucial. Without it the entity’s cyber security program will fail.

The previously mentioned US DOE C2M2 maturity levels are shown on this slide. The vast majority of the initial compliance levels required for utility frameworks today will be at the MIL1 level.

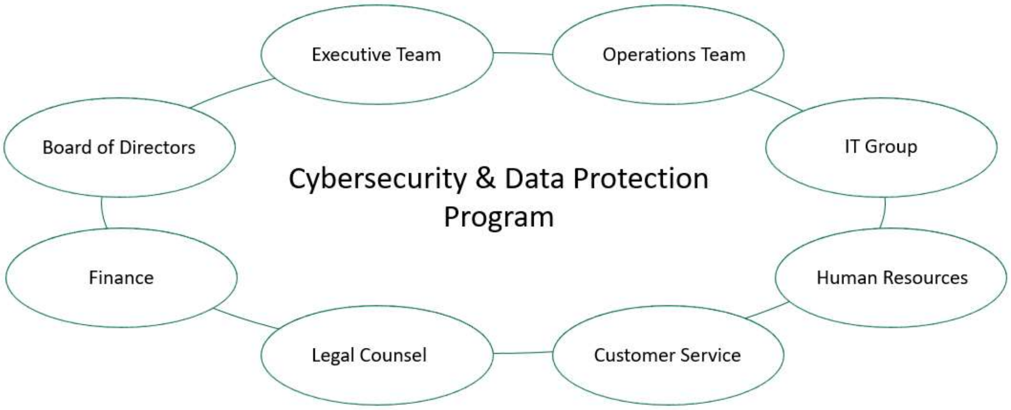
For many utilities thinking about cyber security in the same way as safety can be beneficial. Many of AESI’s clients are emulating aspects of their safety program for their cyber security program.

Engage Leadership

“Boards of directors and executive management teams cannot afford to manage risks (including cybersecurity) casually on a reactive basis, especially in light of the rapid pace of disruptive innovation and technological developments in a digital world”

Source: Key Issues Being Discussed in the Boardroom and C-Suite, NC State, Poole College of Management

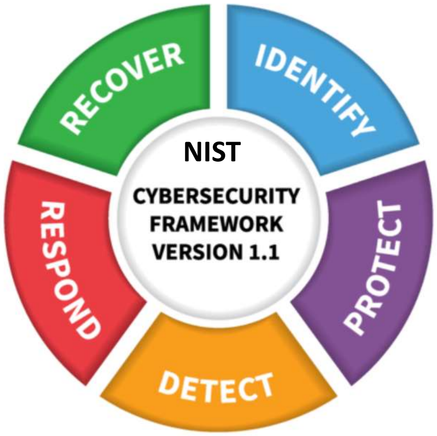
Build a Cross-Functional Team



Use the APPA Scorecard

APPA Cybersecurity Resources:
www.publicpower.org/gridsecurity

Align to Standards



NIST

CYBERSECURITY FRAMEWORK VERSION 1.1

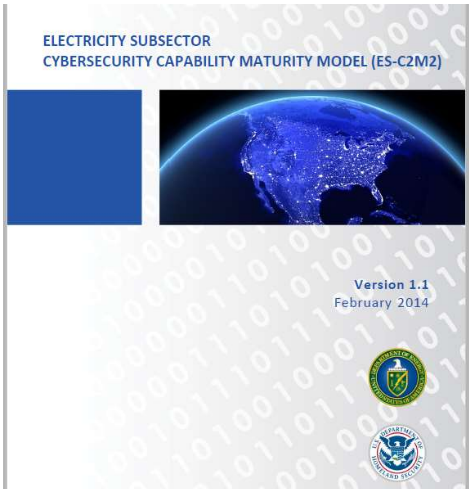
IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER



ELECTRICITY SUBSECTOR
CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

Version 1.1
February 2014

Manage Third Parties

- Incorporate cybersecurity requirements into your RFPs as contractual commitments
- View third parties as “untrusted” – specific access control required
- Request that the third party sign <u>your</u> cybersecurity policy
- Ensure that proper notification, respond and recover processes are in place
- Request regular cybersecurity reporting from the third party

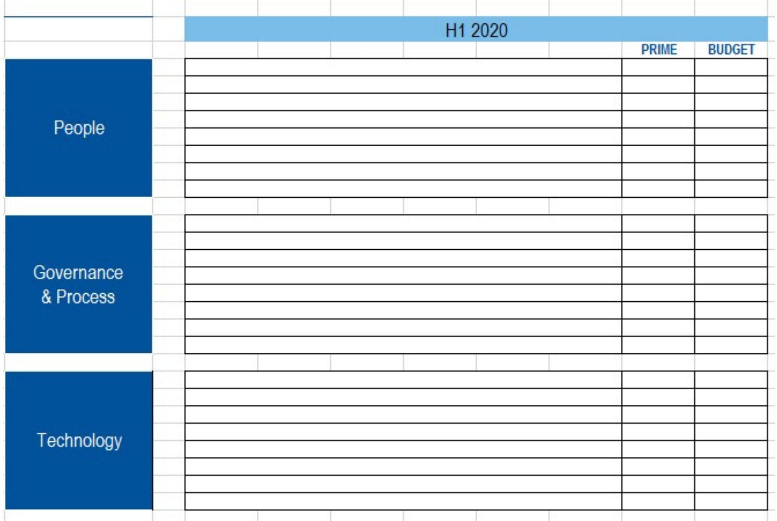
Address all Three Legs of the "Cyber Stool"

People

Process

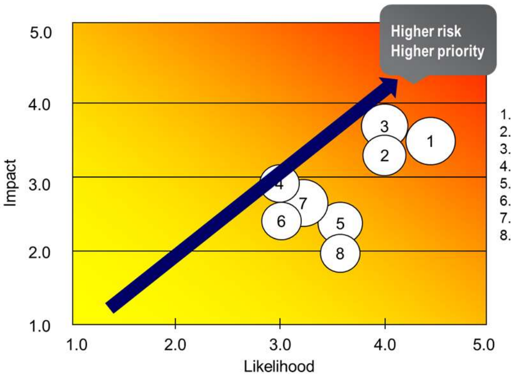
Technology

Build a Roadmap with Task Owners & Budget



	H1 2020		
		PRIME	BUDGET
People			
Governance & Process			
Technology			

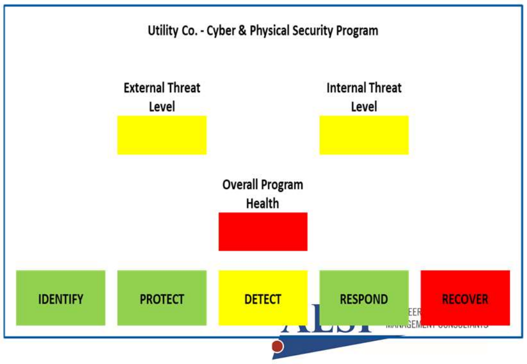
Report and Communicate – Visuals Work Well



Note: *Bubble Size shrinks when mitigation plans are applied*

RISK AREA

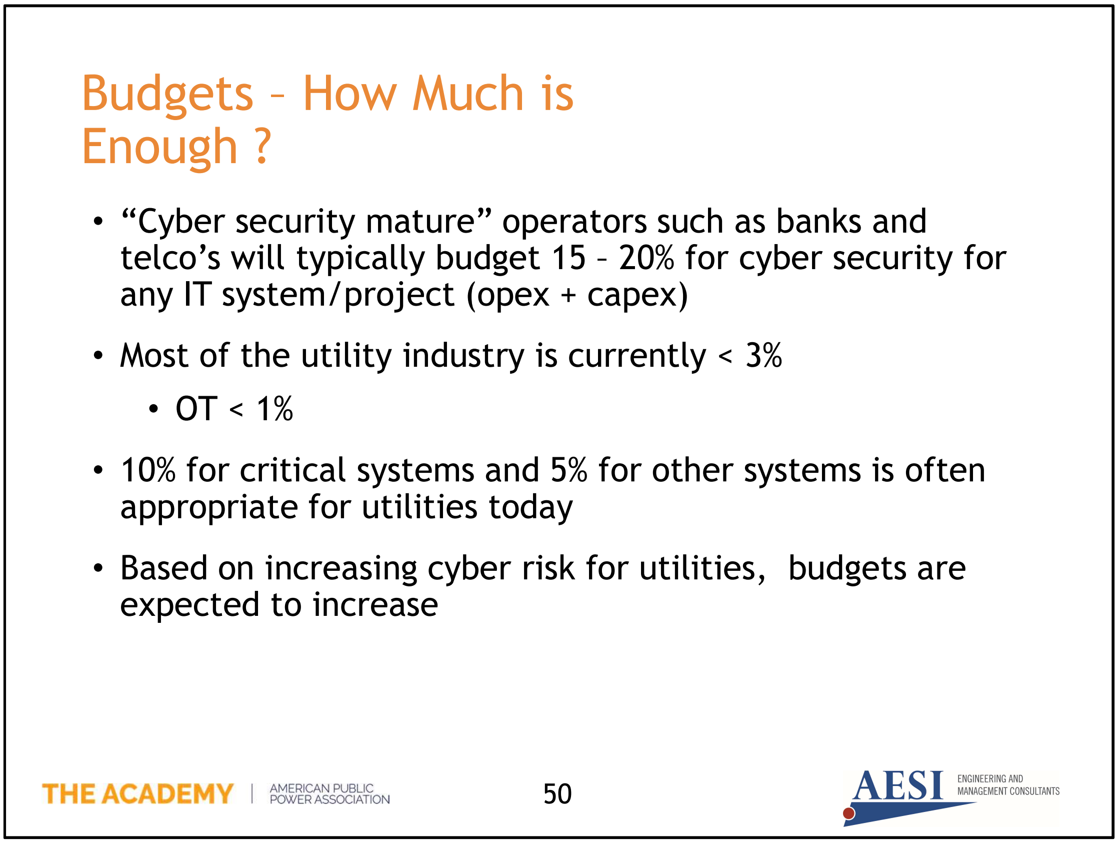
1. Insider Risks
2. External Risks
3. Third Party Risks
4. Privacy Risks
5. Communications Risks
6. Legacy Risks
7. Patch Risks
8. System Risks



Utility Co. - Cyber & Physical Security Program

External Threat Level	Overall Program Health	Internal Threat Level
🟨	🟥	🟨

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
🟩	🟩	🟨	🟩	🟥



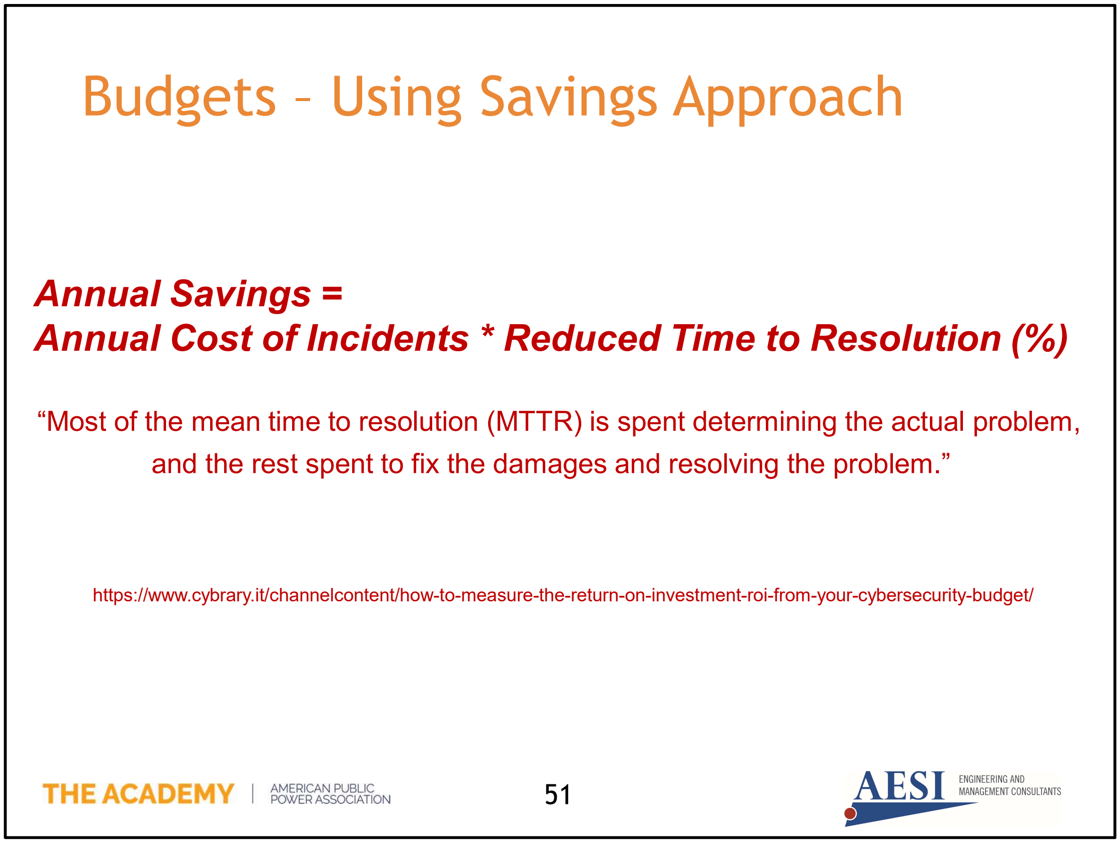
Budgets – How Much is Enough ?

- "Cyber security mature" operators such as banks and telco's will typically budget 15 – 20% for cyber security for any IT system/project (opex + capex)
- Most of the utility industry is currently < 3%
  - OT < 1%
- 10% for critical systems and 5% for other systems is often appropriate for utilities today
- Based on increasing cyber risk for utilities, budgets are expected to increase

THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION
50
AESI ENGINEERING AND MANAGEMENT CONSULTANTS

Budgets are always difficult to gauge for cyber security.

This slide shows some proxies for cyber mature industries such as banks and telcos, and also shows where utilities typically are today.



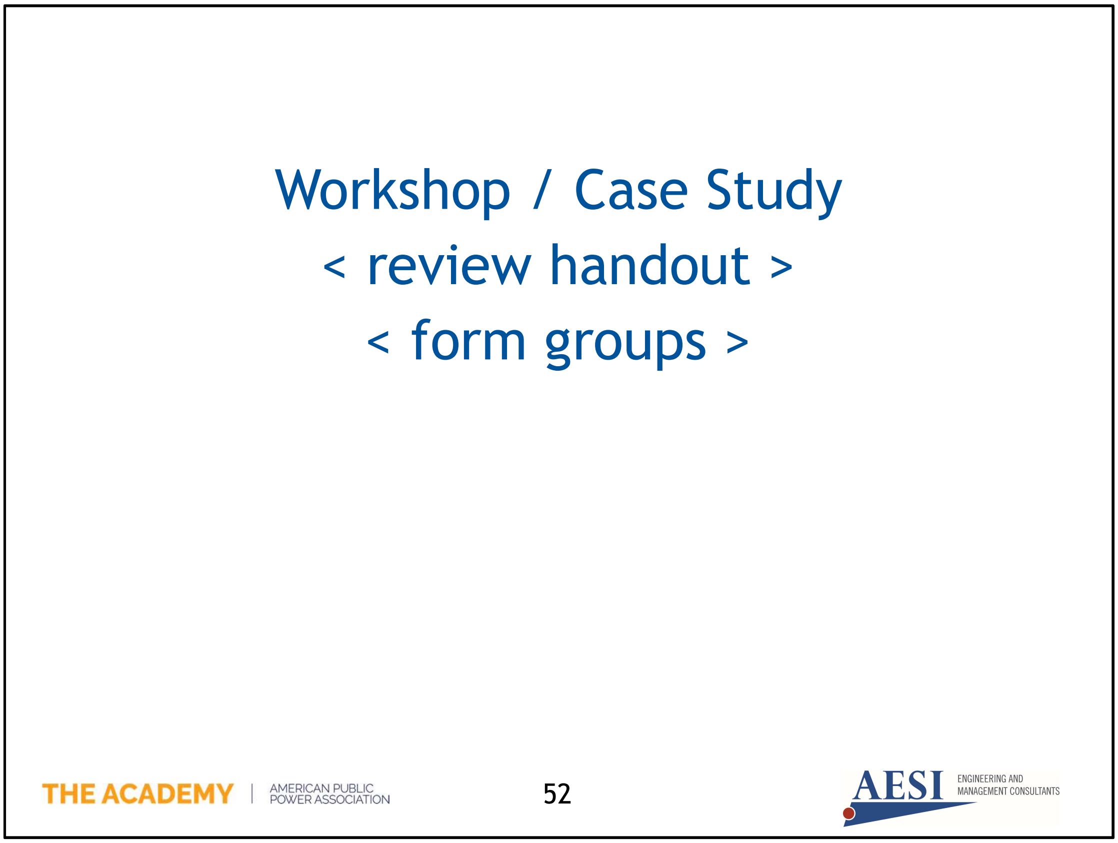
Budgets – Using Savings Approach

Annual Savings =
Annual Cost of Incidents * Reduced Time to Resolution (%)

"Most of the mean time to resolution (MTTR) is spent determining the actual problem, and the rest spent to fix the damages and resolving the problem."

https://www.cybrary.it/channelcontent/how-to-measure-the-return-on-investment-roi-from-your-cybersecurity-budget/

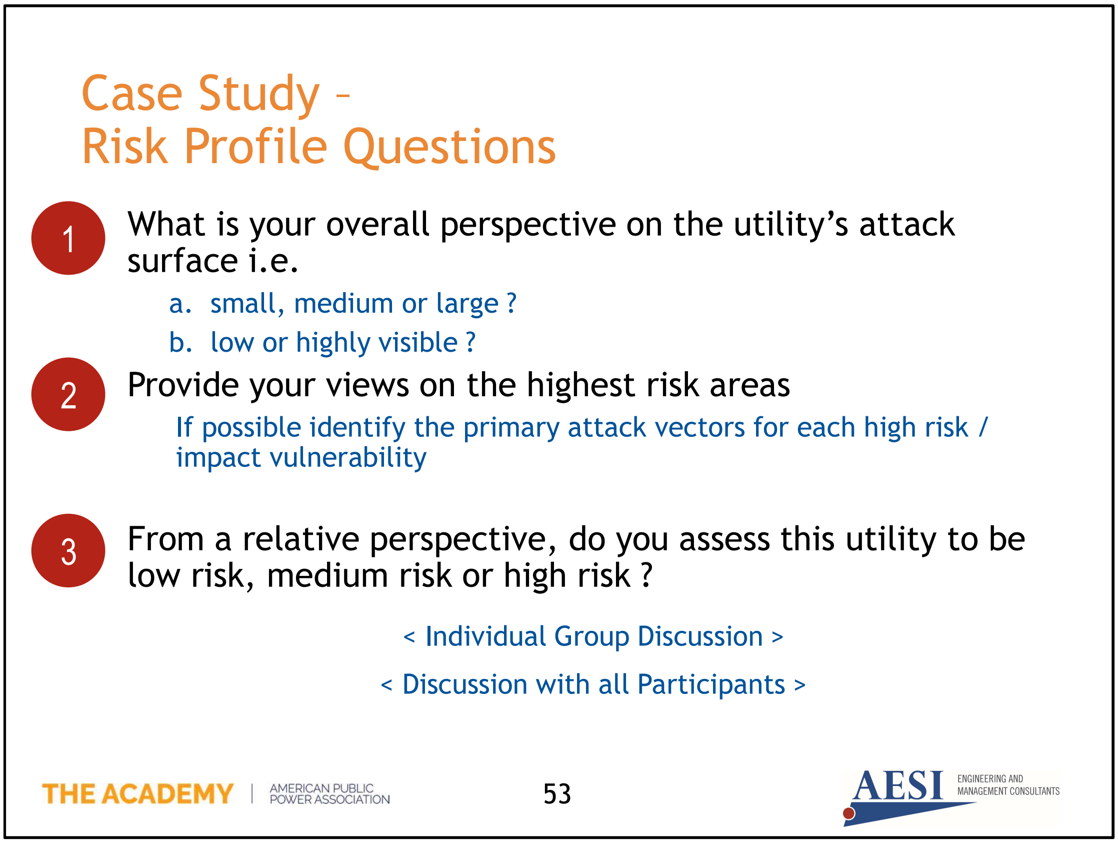
This is another method to determine budgets. This is all about reducing the time to resolution.



Workshop / Case Study

< review handout >

< form groups >



Case Study – Risk Profile Questions

1 What is your overall perspective on the utility’s attack surface i.e.

   a. small, medium or large ?
   b. low or highly visible ?

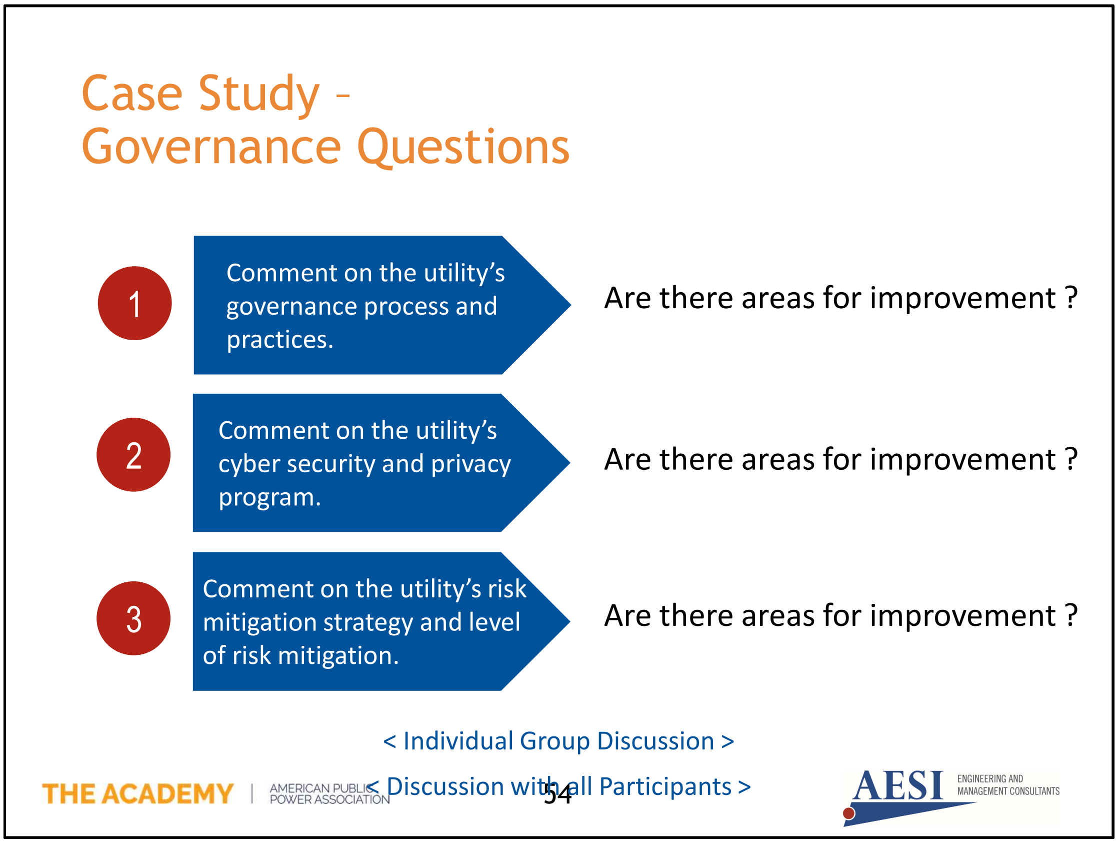
2 Provide your views on the highest risk areas

   If possible identify the primary attack vectors for each high risk / impact vulnerability

3 From a relative perspective, do you assess this utility to be low risk, medium risk or high risk ?

< Individual Group Discussion >

< Discussion with all Participants >



Case Study – Governance Questions

1. Comment on the utility's governance process and practices. — Are there areas for improvement ?

2. Comment on the utility's cyber security and privacy program. — Are there areas for improvement ?

3. Comment on the utility's risk mitigation strategy and level of risk mitigation. — Are there areas for improvement ?

< Individual Group Discussion >

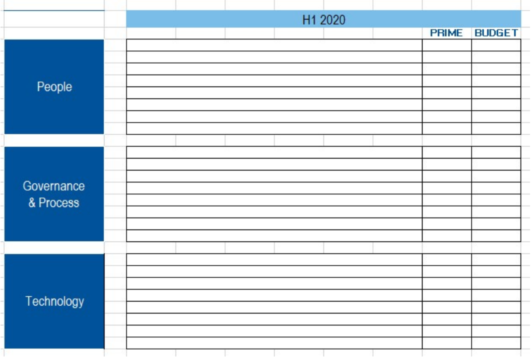
< Discussion with all Participants >

Case Study – Cyber Security Program Roadmap

< Individual Group Discussion >

< Discussion with all Participants >

Develop a phased cyber security program roadmap with the tool provided.



H1 2020

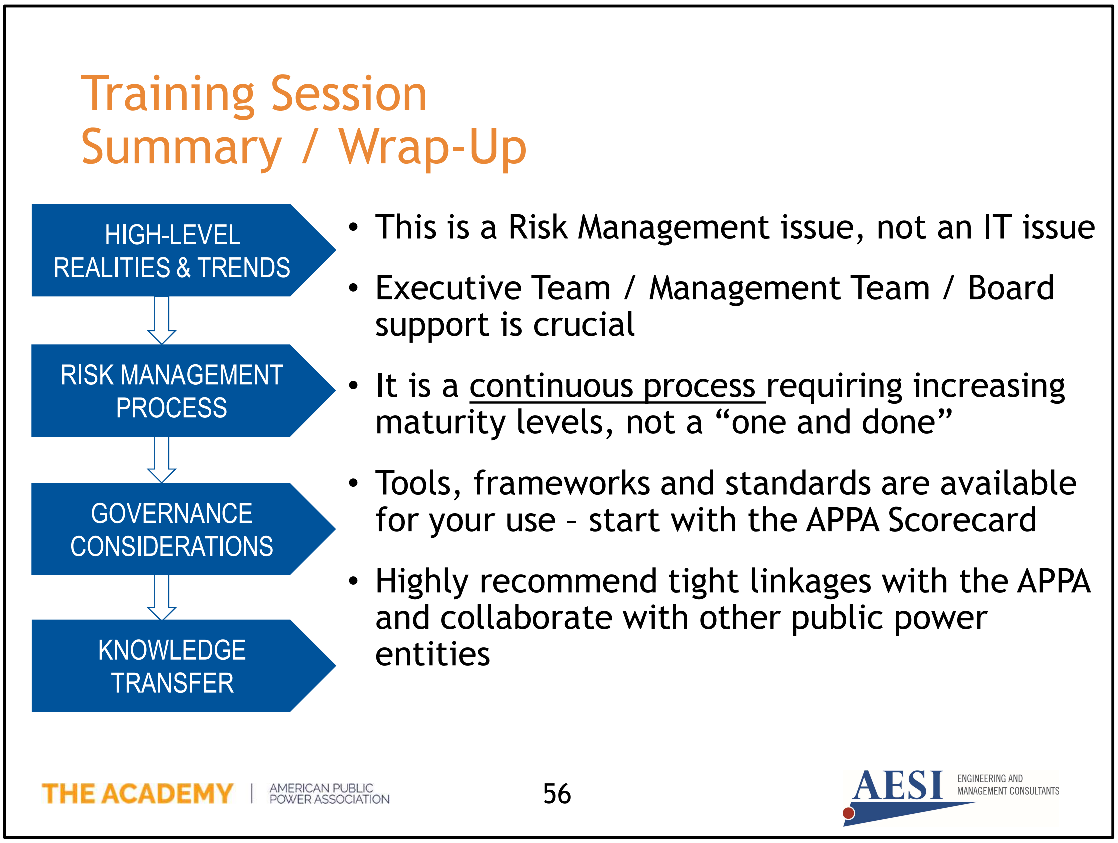
PRIME

BUDGET

People

Governance & Process

Technology



Training Session Summary / Wrap-Up

HIGH-LEVEL REALITIES & TRENDS

RISK MANAGEMENT PROCESS

GOVERNANCE CONSIDERATIONS

KNOWLEDGE TRANSFER

- This is a Risk Management issue, not an IT issue
- Executive Team / Management Team / Board support is crucial
- It is a continuous process requiring increasing maturity levels, not a “one and done”
- Tools, frameworks and standards are available for your use – start with the APPA Scorecard
- Highly recommend tight linkages with the APPA and collaborate with other public power entities

APPA Cyber Security Training

- Deliver low cost **cybersecurity training and exercises** that align with the Scorecard
- Conduct Regional facilitated workshops **(JAA/State Association sites)**
- Host a year end public power **cybersecurity summit (November 18-20, 2019 Nashville, TN)**
- Develop a public power cyber **response playbook and conduct exercises**

APPA References and Contacts

Nathan Mitchell
Sr. Director of Electric
Reliability Standards and
Security

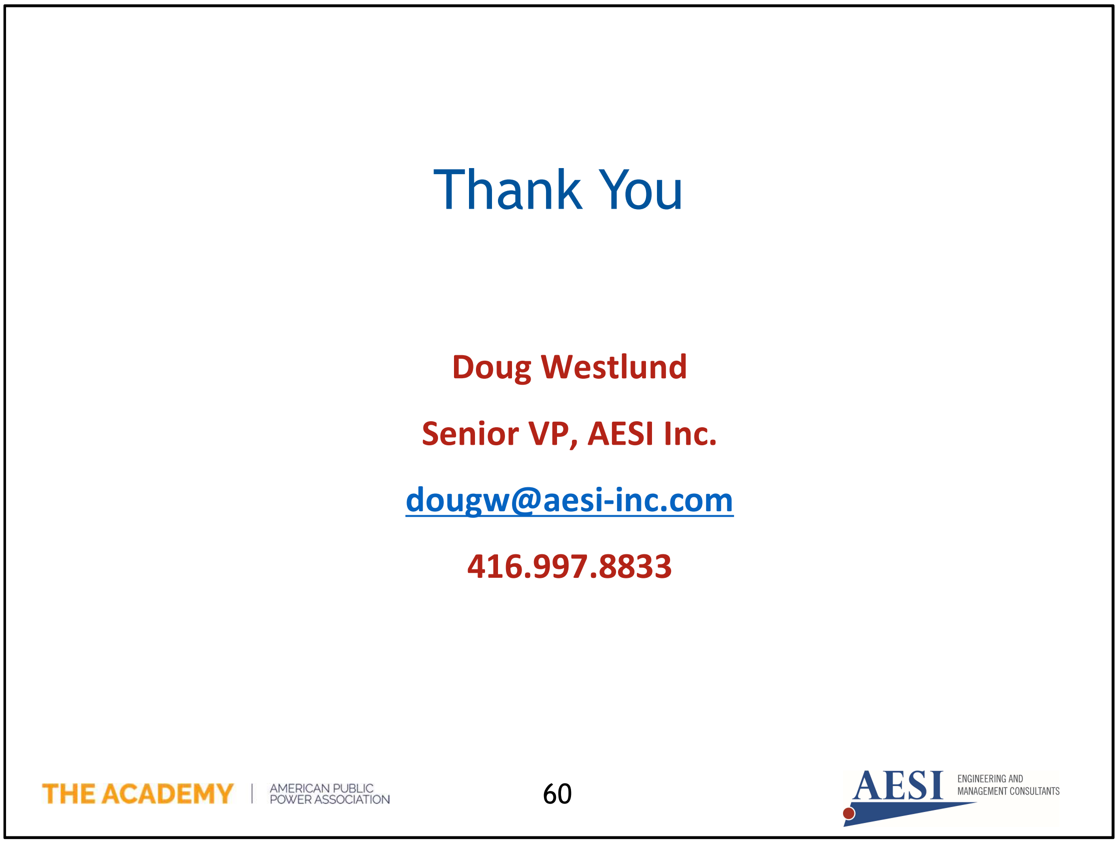
**American Public Power
Association**
2451 Crystal Dr., Suite 1000,
Arlington, VA 22202

Direct: 202.467.2925
nmitchell@publicpower.org

Resources page:
www.publicpower.org/gridsecurity

Email: cybersecurity@publicpower.org

Questions
Answers



Thank You

Doug Westlund

Senior VP, AESI Inc.

dougw@aesi-inc.com

416.997.8833