

AMERICAN
PUBLIC
POWERTM
ASSOCIATION
ACADEMY

ACADEMY

Public Power Cybersecurity Roadmap: Culture Changes Needed to Support Cybersecurity



Southeast Regional Municipal Cybersecurity Summit
July 10-11, 2019 Orlando, FL

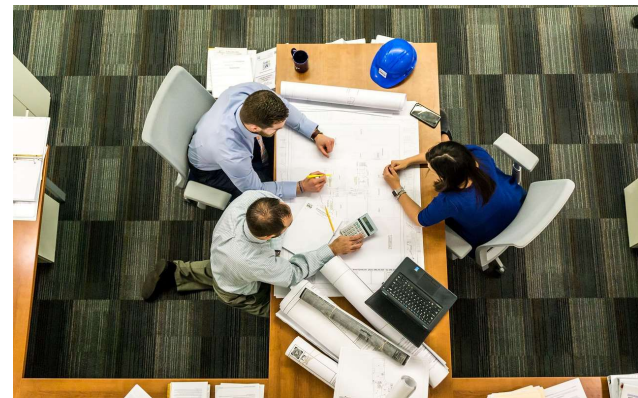
Christopher Kelley, PMP
Vice President
Beam Reach Consulting Group
ckelley@beamreachgroup.com
443.906.3513





Beam Reach Consulting Group

- Strategic planning, project management support for energy infrastructure and resilience programs
- Staff have supported over 75 advanced electric grid projects across the US
- Program management for energy infrastructure programs > \$7.9 billion
- APPA Associate Member, WOSB

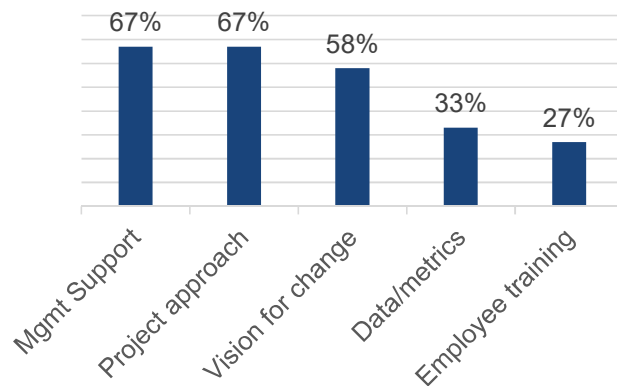


Public Power Cybersecurity Roadmap Advisory Council



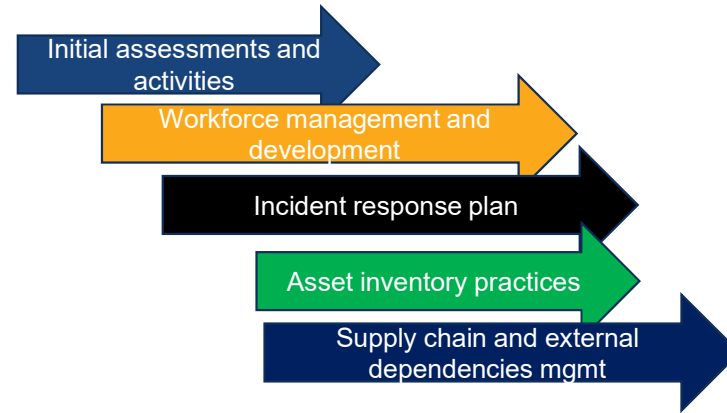
Designed approach to cybersecurity maturity implementation

- Establish management buy-in
 - Security program
 - Budget and resources
- Assess the need and set the vision
- Prioritize and treat cybersecurity maturity like a project
- Develop successful employee training
- Establish data/metrics for security program



Public Power Cybersecurity Roadmap

- Clear actions and outputs for small- to med-public power utilities
- Focused on priority pathways



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management	TIER 1
	Access Control	
	Awareness and Training	
	Data Security	
	Information Protection	
Detect	Processes & Procedures	
	Maintenance	
	Protective Technology	
Respond	Anomalies and Event	
	Security Continuous Monitoring	
	Detection Processes	
Recover	Response Planning	RC.RP
	Communications	RC.CO
	Improvements	RC.IM

- Driven by Cybersecurity Roadmap Advisory Council
- Informed by industry

Public Power Cybersecurity Roadmap bridges the gap between assessment and action.

Initial assessments and activities

Getting Started on the Roadmap Path



- Target profile for small-to-medium public power utilities
- Dedicate time to planning, especially risk assessment and measurement
- Perform baseline assessment and consider independent review/assessment
- Follow a risk-based approach
- Gain senior management support and buy-in
- Establish a project-based approach to cybersecurity
 - Develop cybersecurity strategy
 - Create data and metrics to measure security program
 - Prioritize actions to take
 - Create a project management plan
 - Include communications, outreach, and continuous learning

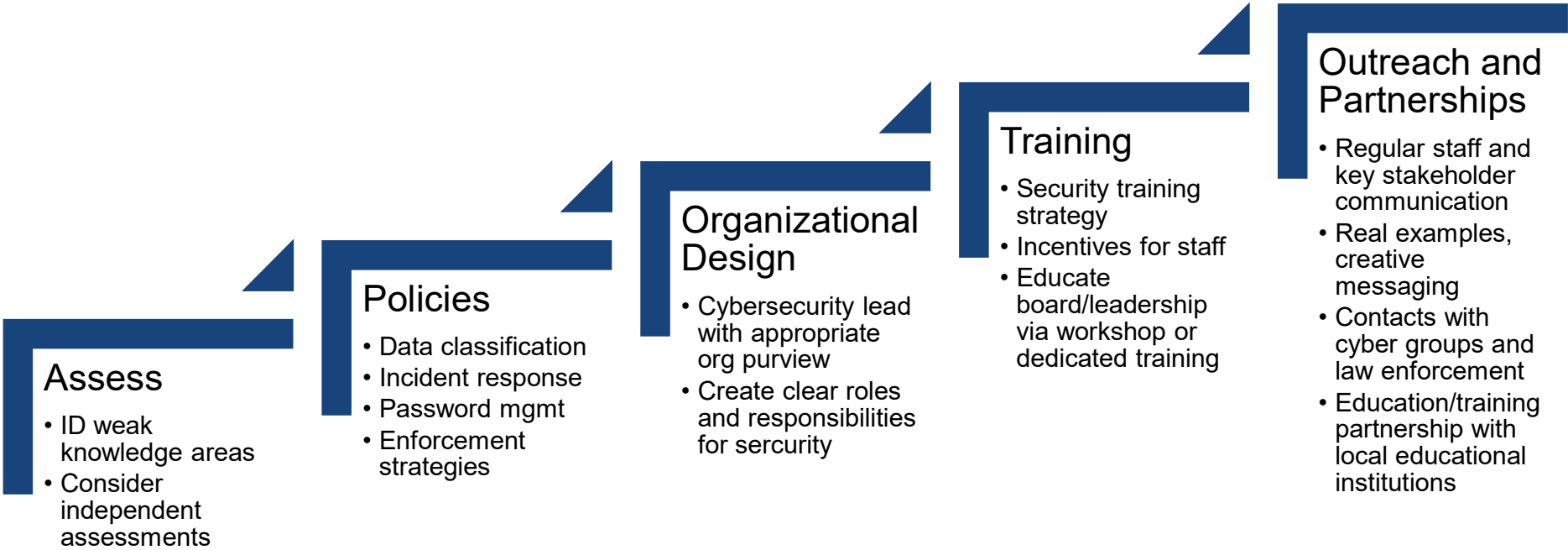


[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)



Workforce management and development

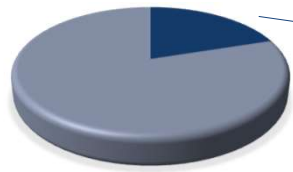
Developing a culture of awareness and building knowledge



Why is (organizational) Change Management so important to cybersecurity projects?

Focus on technology > Impact on people?

People make your organization work (or fail)



20% of employees willing to sell passwords to a third party*

44% willing to do for less than \$1,000

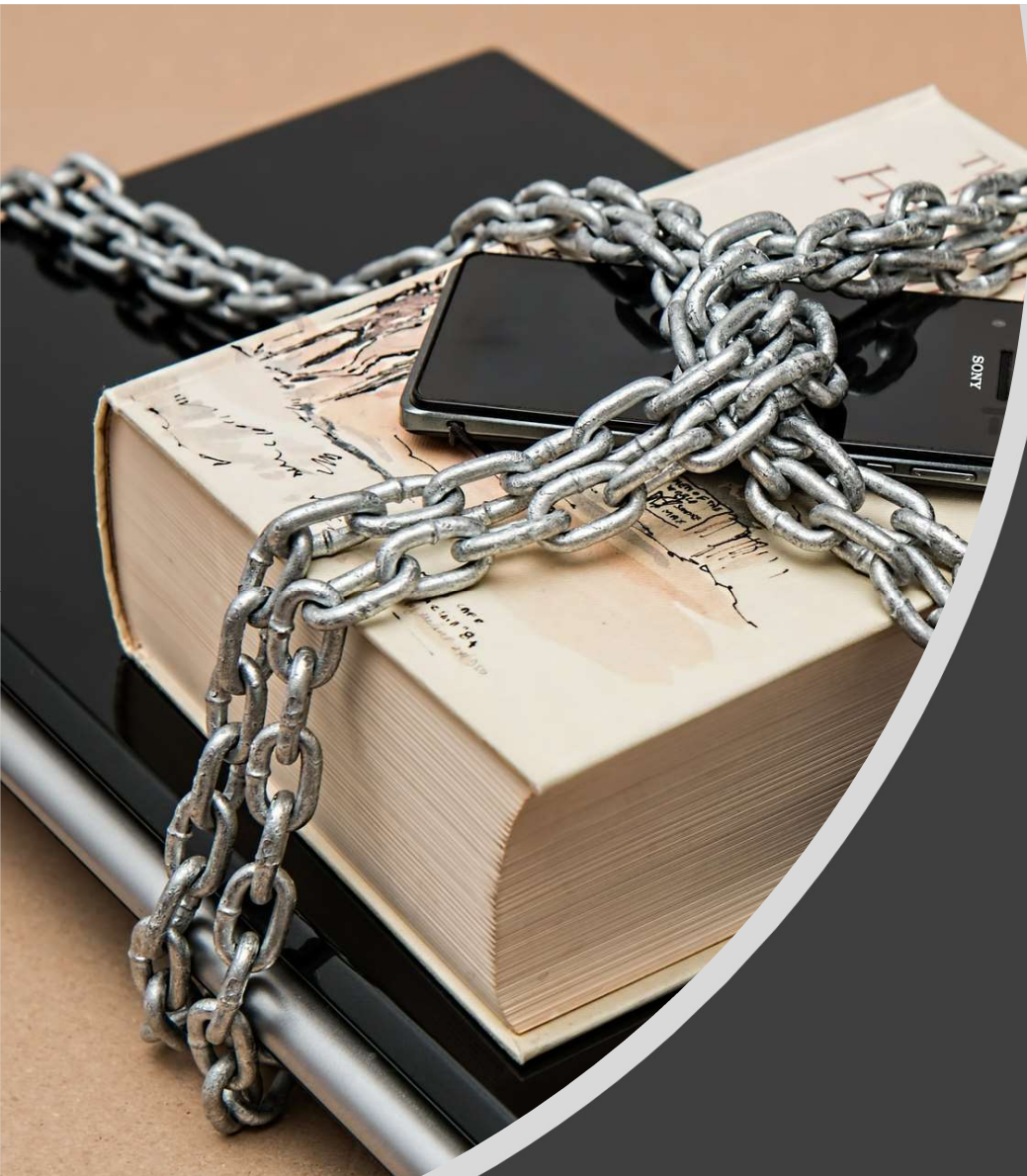
Some would do it for \$100



Trap: The value of technology improvements are self-evident

*SailPoint Market Pulse Survey (2016)





Change Management Challenges for Cybersecurity Adoption



- Security is the enemy of productivity!
- Cybersecurity has never been an issue for us before.
- We are a small utility in a small town. We're not on the radar screen.
- We can't afford it!
- I already have 3 day jobs. How do I have time for one more?

Playbook and Preparation

Incident response plan



- Make policies and actions very clear in advance (e.g. pre-approval for kill switch authority)
- Clear roles and responsibilities (staff, SMEs, vendors)
- Engage and share plan with law enforcement/FBI/National Guard
- Weigh pros and cons of engaging outside entities and be clear on actions for the plan.
- Use cyber mutual aid as both a communications and resource support tool
- Integration with corporate business continuity and emergency response plans
- Reinforce the plan through training, exercises
- Leadership signoff

Roles for APPA and Joint Action Agencies?



Developing a Culture of Awareness and Building Knowledge



- APPA CEDS Training Program for Joint Action Agencies
 - Cybersecurity 101
 - Deeper dive training
- Regional Cybersecurity Summits (April-August 2019)
 - Midwest (July 2019) – Kearney, NE
 - Western (August 2019) – Anaheim, CA
- Cybersecurity Roadmap Advisory Committee (CRAC)
- Joint Action Committee – Cybersecurity (JAC-C)
- GridEx V (November 13-14, 2019)
- National Cybersecurity Summit (November 18-20, 2019 – Nashville, TN)

More info: cybersecurity@publicpower.org

So what's next?



Assessment is step one
<https://publicpower.axio.com>



How much would we reduce risk by implementing all 51 recommendations?



How do we prioritize recommendations?



These are the key tenets to a successful cybersecurity program

Questions and Discussion

