AMERICAN PUBLIC POWER™ ASSOCIATION

ACADEMY

ACADEMY

Cybersecurity Roadmap: Onward and Upward

Joint Action Conference
January 6-8, 2019 Key West, FL

Carter Manucy
Cyber Security Manager
Florida Municipal Power Agency
carter.manucy@fmpa.com
407-355-7767

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

Mission: Low-Cost, Clean and Reliable Power

32 Municipals Are Members of FMPA

Alachua
Bartow
Blountstown
Bushnell
Chattahoochee
Clewiston
Fort Meade
Fort Pierce
Gainesville
Green Cove Springs
Town of Havana
Homestead
Jacksonville Beach
Key West
Kissimmee
Lake Worth
Lakeland
Leesburg
Moore Haven
Mount Dora
New Smyrna Beach
Newberry
Ocala
Orlando
Quincy
St. Cloud
Starke
Tallahassee
Vero Beach
Wauchula
Williston
Winter Park

Serving 2.4 million, or 11%, of Floridians

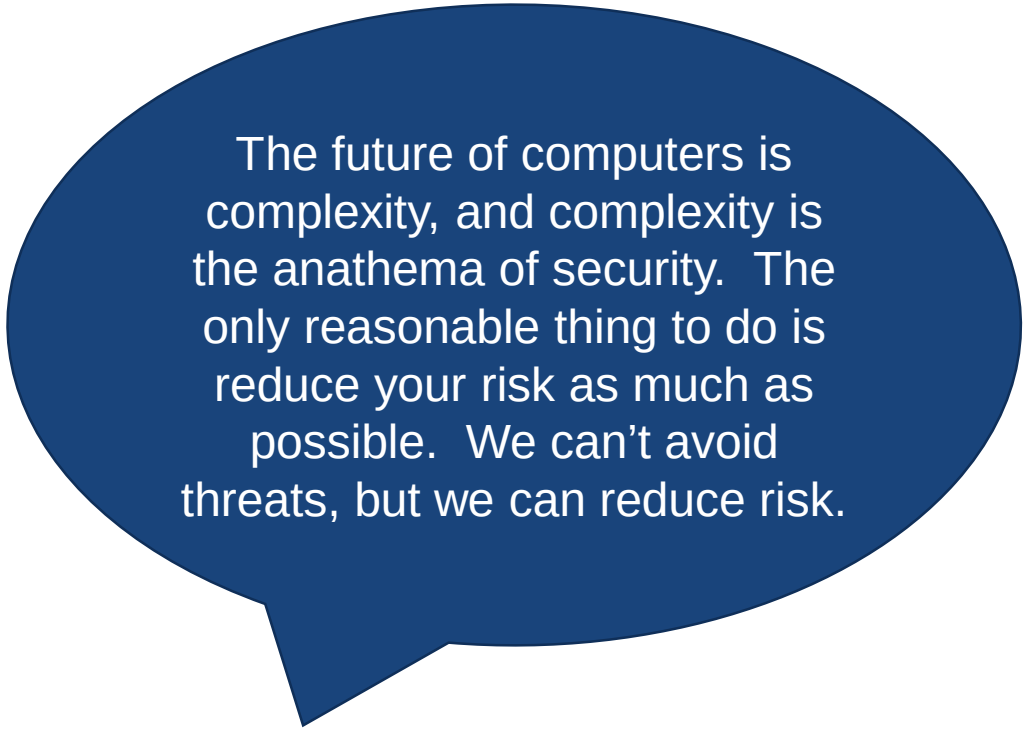
Beam Reach Consulting Group

- 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

BEAM REACH
CONSULTING GROUP
Make the most of your resources.

What's the concern?

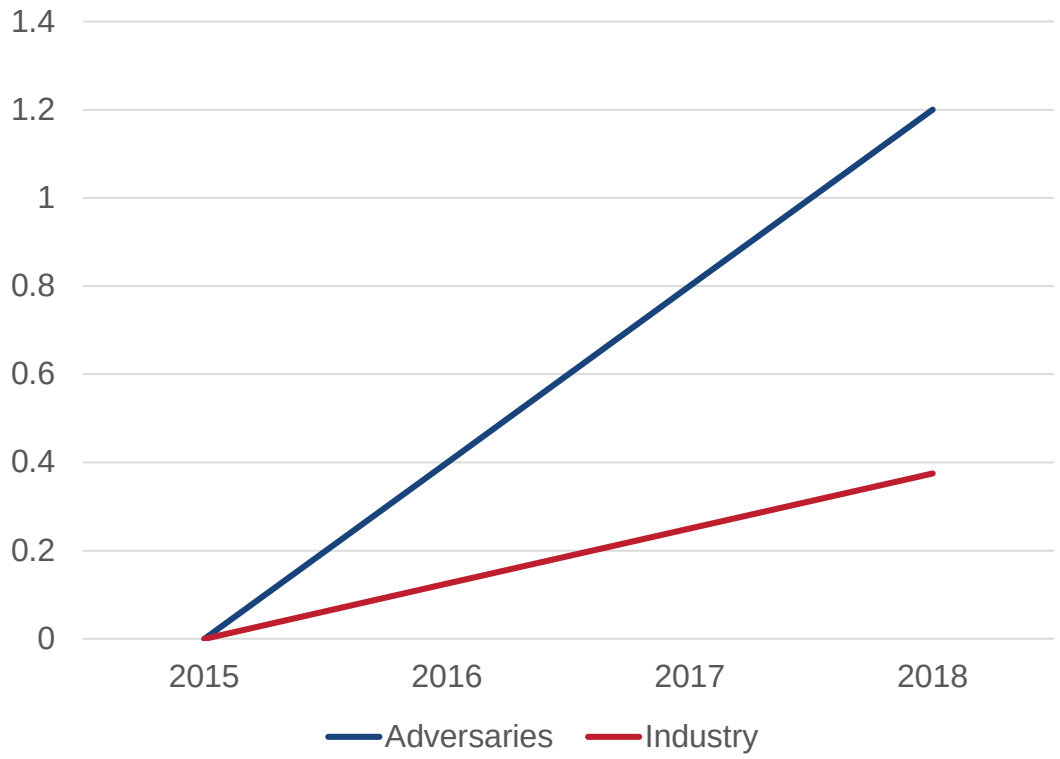
- Reducing the attack surface
- Fixing human behavior
- Applying funding in the right places
- Empowering our workforce to understand the issues



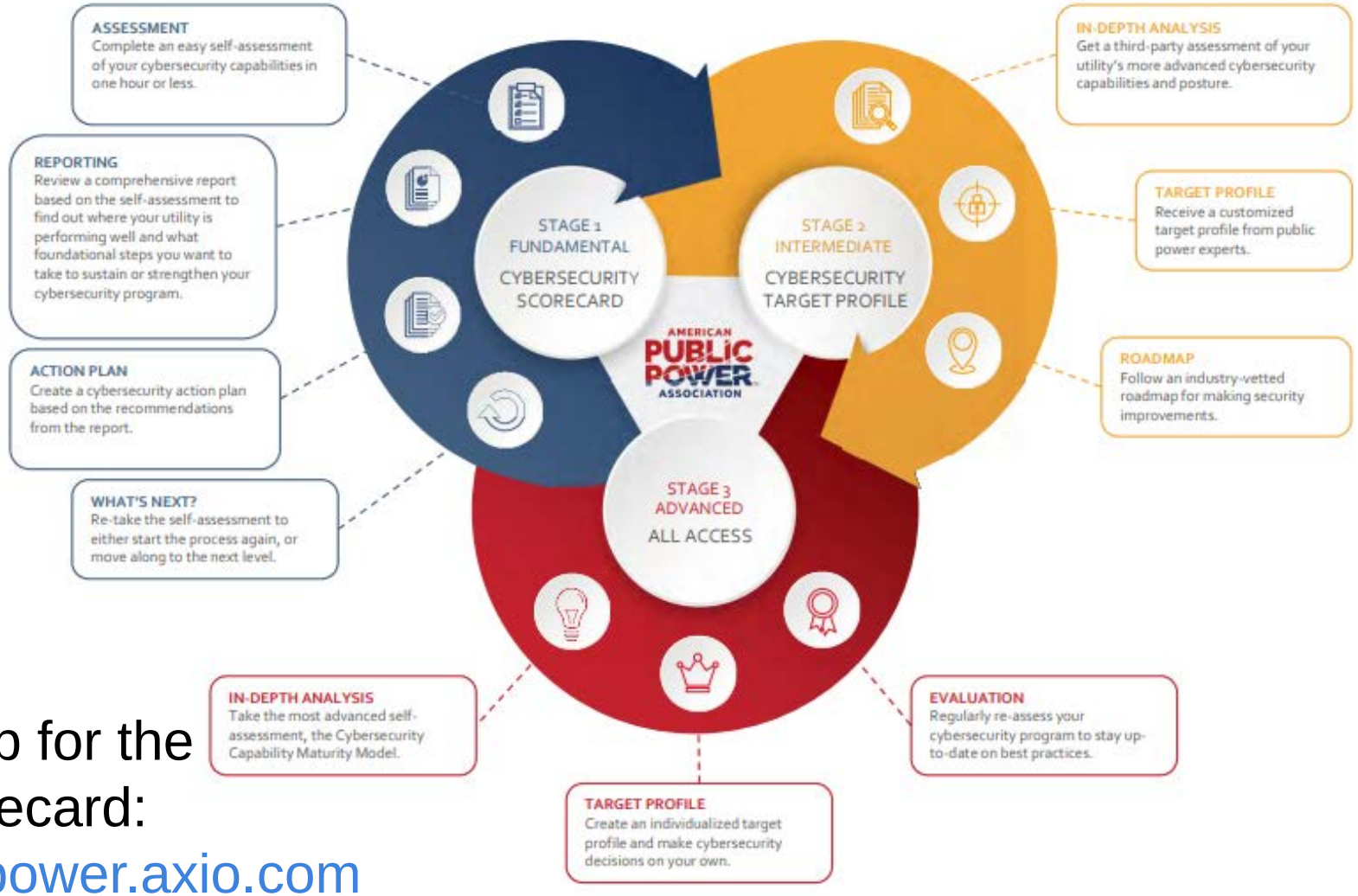
Bruce Schneier

What's the concern?

- Our cybersecurity efforts are just barely keeping up
- As we spend money, we're not improving our overall hygiene
- Adversaries are putting more time and developing skills at a much faster rate
- Bottom line – we have to change our attitudes and capabilities



Scorecard Basics



Sign up for the Scorecard:
https://publicpower.axio.com

Scorecard Basics

- How long is this “easy test” going to take me?
  - 14 Questions, most will have multiple responses
  - Answers are easy to understand and often have examples to help explain the choice
  - Questions like:
    - Do you have a risk management strategy?
    - Do you receive external threat data?
    - Have you performed a recent vulnerability analysis?
  - Average completion time ~ 45 minutes

Scorecard Basics

- I took the assessment… now what?
  - Take notes for each practice
  - Assign tasks to individuals
  - Use built in help to understand key concepts or describe them to your peers
  - Generate reports for management
  - Import previous C2M2 assessments
  - Expand to the advanced assessment if you're doing well
  - Compare results to other targets, such as CIP low/medium/high requirements

How can it help me?

- Scorecard gives you a point-in-time snapshot of how you're doing
- Generates reports that can show progress towards goals
- Allows you to compare your utility to your peers, standards or your own expectations

How can it help me?

Measuring cybersecurity is tough…

- Proving the negative
- If you weren't attacked, is it because you're doing everything right or you weren't targeted?
- If you were targeted, would you know?
- What is your observable measurement?
- It doesn't have to just be after the fact
  - How long were we down for?
  - How much did that project cost?
- Measuring a reduction, and not necessarily an elimination, is good enough for a risk reduction

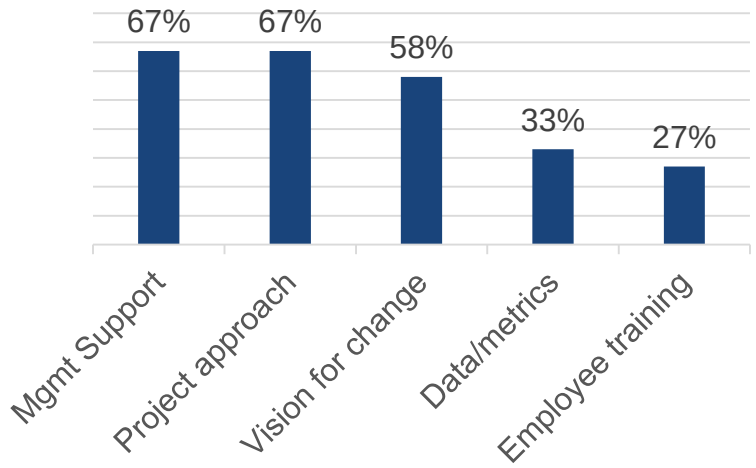
Public Power Cybersecurity Scorecard - EOY 2018

- 177 completed Scorecards
- 83 completed full C2M2 evaluations (converted from Scorecard)
- 305 total self-assessments
- 180 utilities have participated
- 272 total registered users

Public Power Cybersecurity Roadmap Advisory Council

Designed approach to cybersecurity maturity implementation

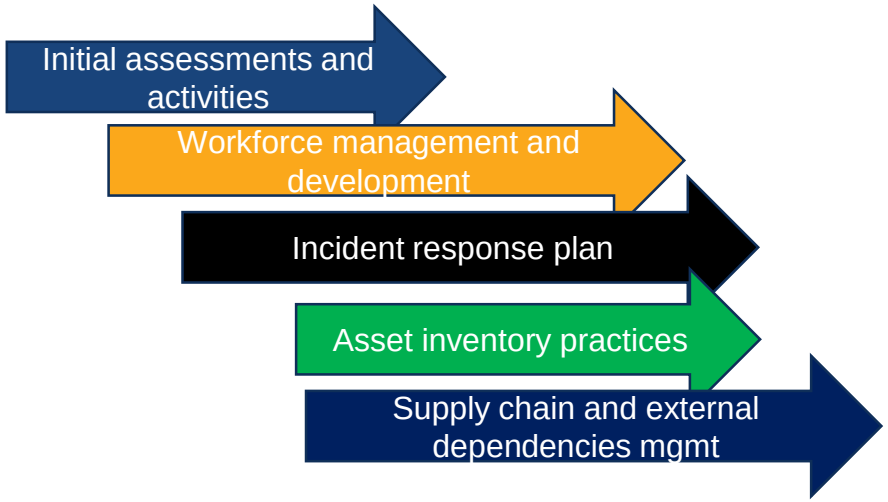
- Establish management buy-in
  - Security program
  - Budget and resources
- Assess the need and set the vision



- 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



- 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

Workforce management and development

Developing a culture of awareness and building knowledge

Assess

- ID weak knowledge areas
- Consider independent assessments

Policies

- Data classification
- Incident response
- Password mgmt
- Enforcement strategies

Organizational Design

- Cybersecurity lead with appropriate org purview
- Create clear roles and responsibilities for sercurity

Training

- Security training strategy
- Incentives for staff
- Educate board/leadership via workshop or dedicated training

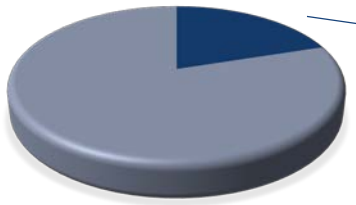
Outreach and Partnerships

- Regular staff and key stakeholder communication
- Real examples, creative messaging
- Contacts with cyber groups and law enforcement
- Education/training partnership with local educational institutions

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

Focus on technology > Impact on people?

People make your organization work (or fail)



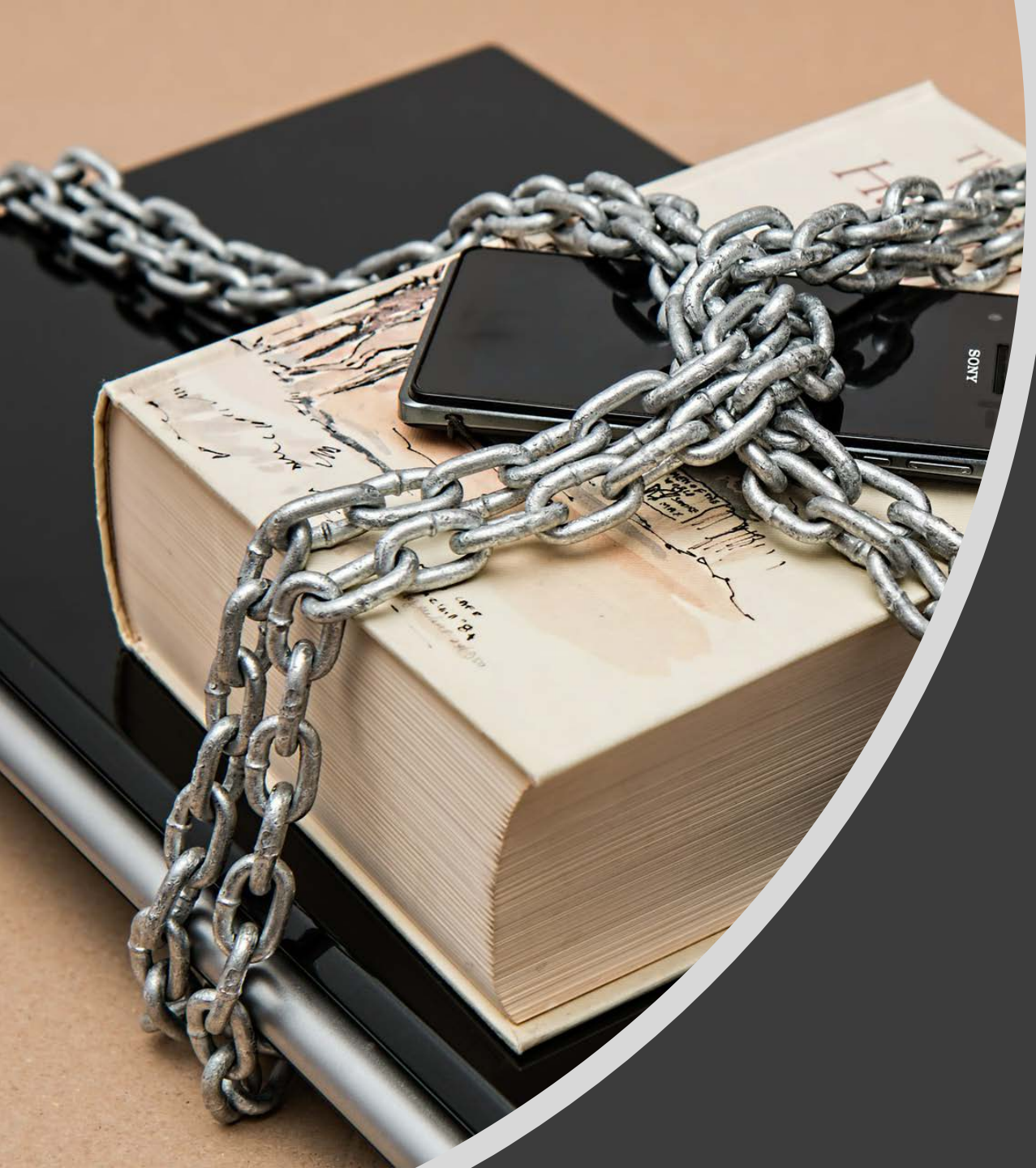
20% of employees willing to sell passwords to a third party*

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

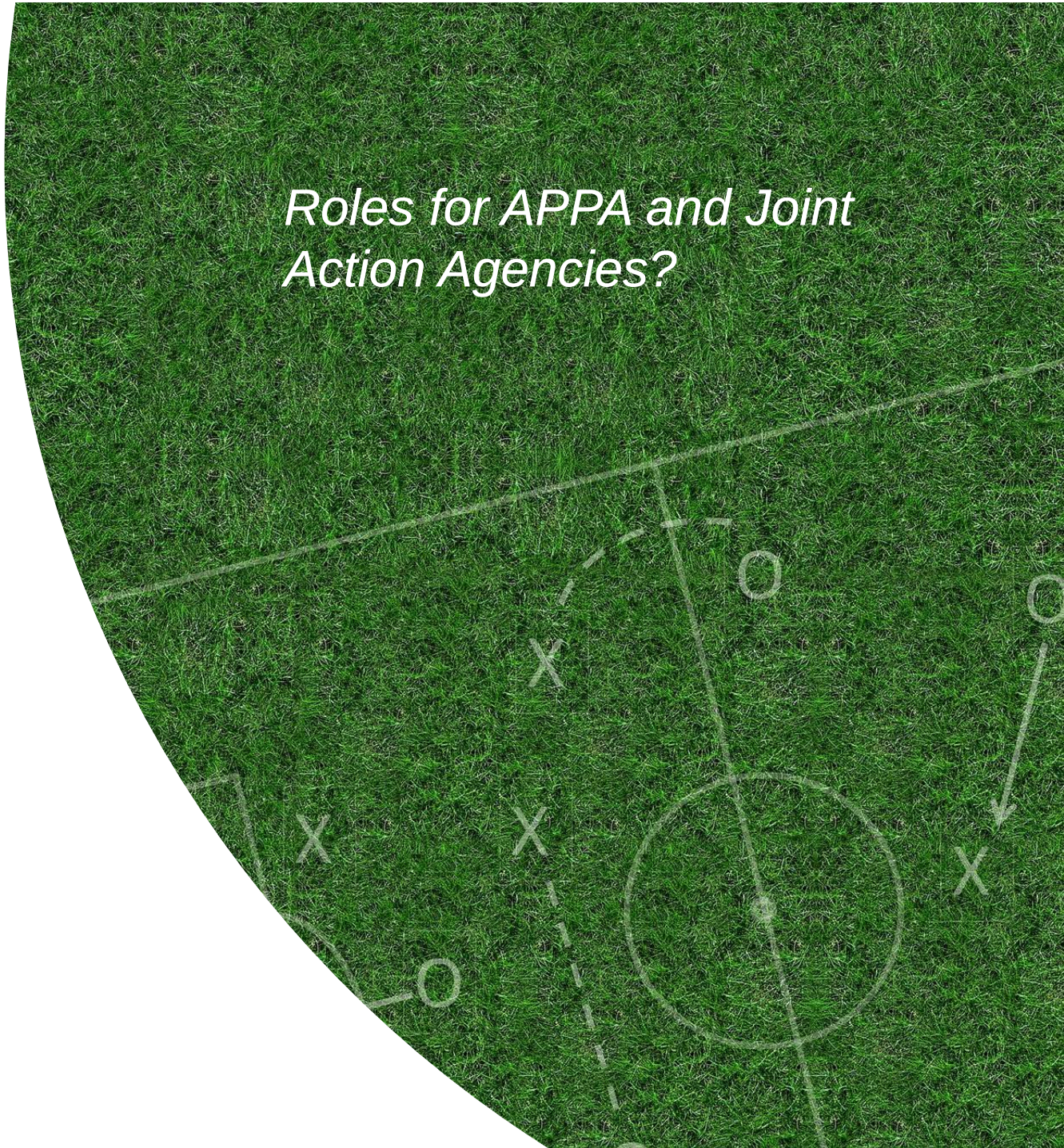
- Security is the enemy of productivity!
- Cybersecurity has never been an issue for us before.
- We are a small utility in a small town. We're not on the radar screen.
- We can't afford it!
- I already have 3 day jobs. How do I have time for one more?

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
  - o Cybersecurity 101
  - o Deeper dive training
- Regional Cybersecurity Summits (April-August 2019)
  - o Midwest location
  - o Northeast location
- Cybersecurity Roadmap Advisory Committee – Joint Action Agency
- GridEx V (November 13-14, 2019)
- National Cybersecurity Summit (Fall 2019)
  - o Pacific Northwest location

More info: cybersecurity@publicpower.org

So what's next?

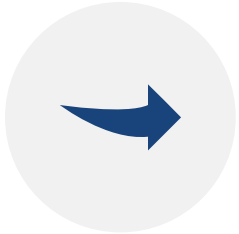
Assessment is step one
https://publicpower.axio.com

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

Think you're done?



MOVE ONTO THE NEXT PHASE!

KEEP IMPROVING CRAWL, WALK, RUN

HELP YOUR PEERS!

SHARE SUCCESS STORIES

WATCH OUT FOR NEW REQUIREMENTS

Questions and Discussion