Public Power Cybersecurity Roadmap

Western Regional Municipal Cybersecurity Summit

August 22, 2019

Christopher Kelley, PMP

ckelley@beamreachgroup.com

BEAM REACH
CONSULTING GROUP
Make the most of your resources.

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.

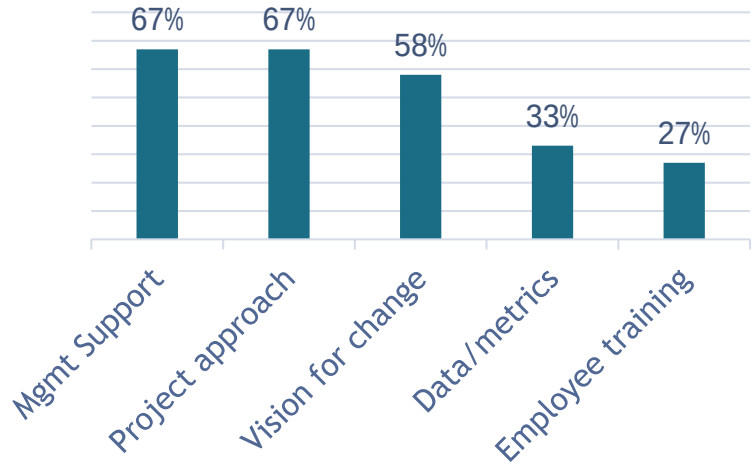
Overview

- About the Cybersecurity Roadmap Advisory Council
- Initial findings from the CRAC team
- Introduction to the Public Power Cybersecurity Roadmap
- Next Steps

Public Power Cybersecurity Roadmap Advisory Council

Designed approach to cybersecurity maturity implementation

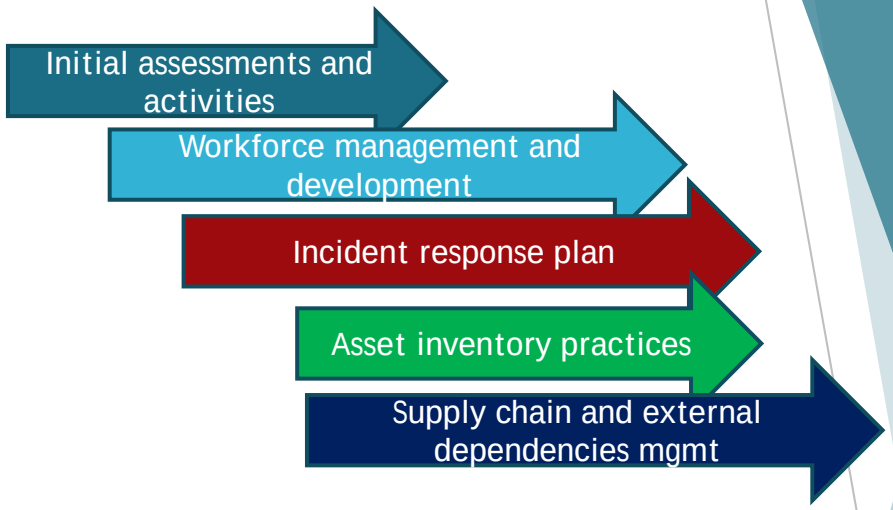
- Establish management buy-in
  - Security program
  - Budget and resources
- Assess the need and set the vision



- 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

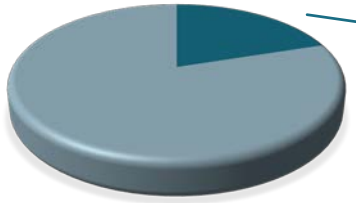
Outreach and Partnerships

- 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)



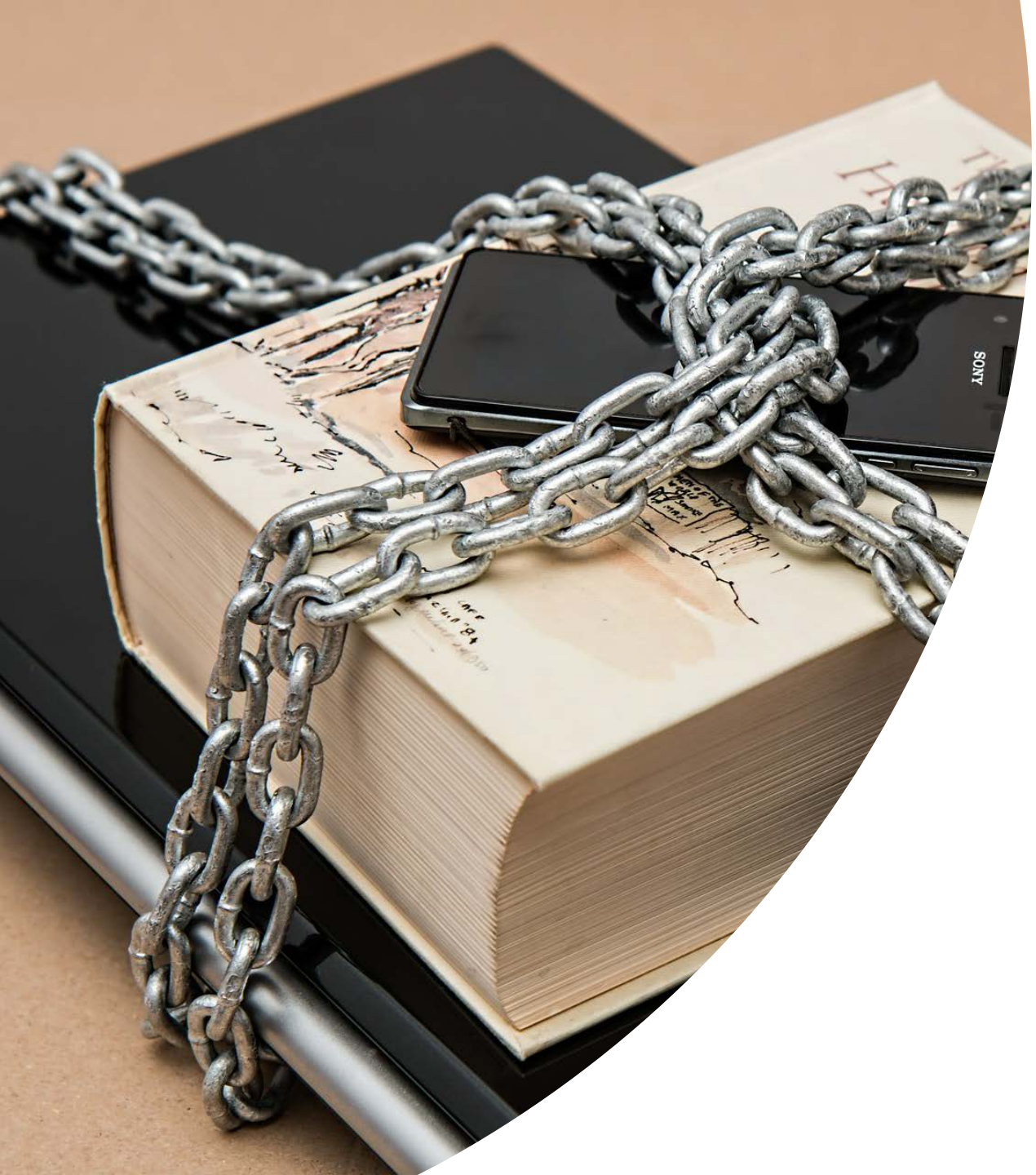
20% of employees willing to sell passwords to a third party*

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)



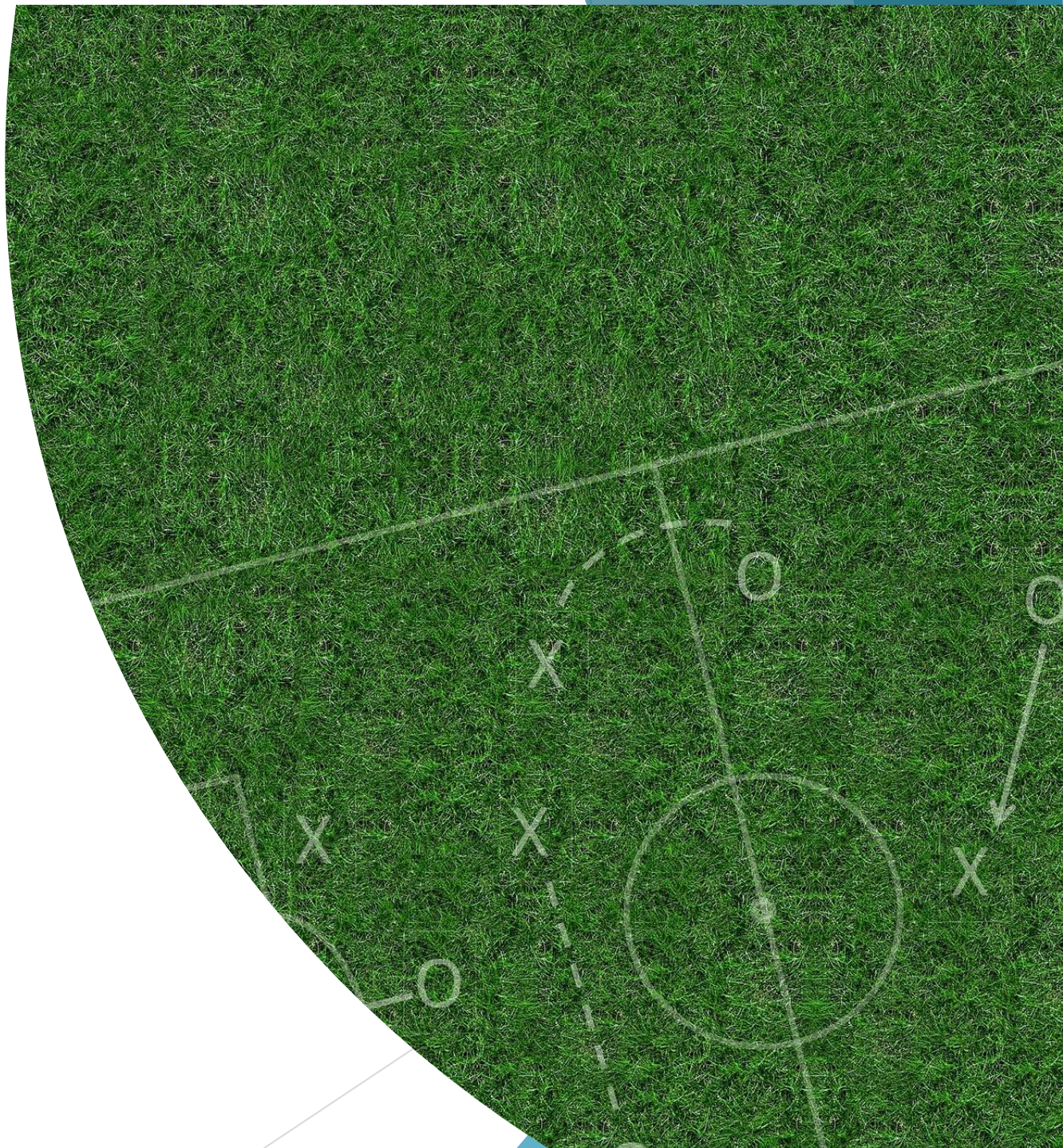
Change Management Challenges for Cybersecurity Adoption

- 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

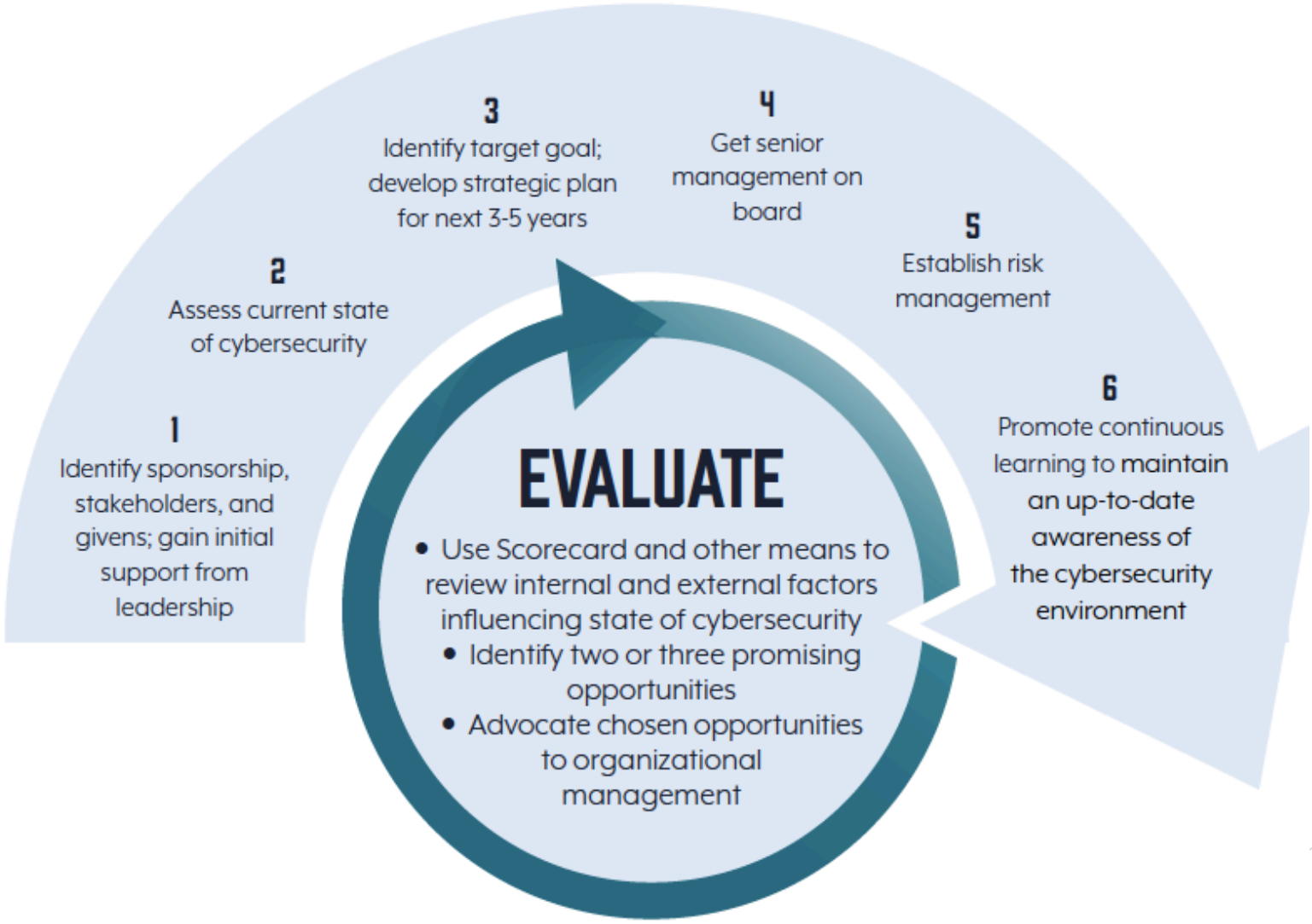
Incident response plan

- 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

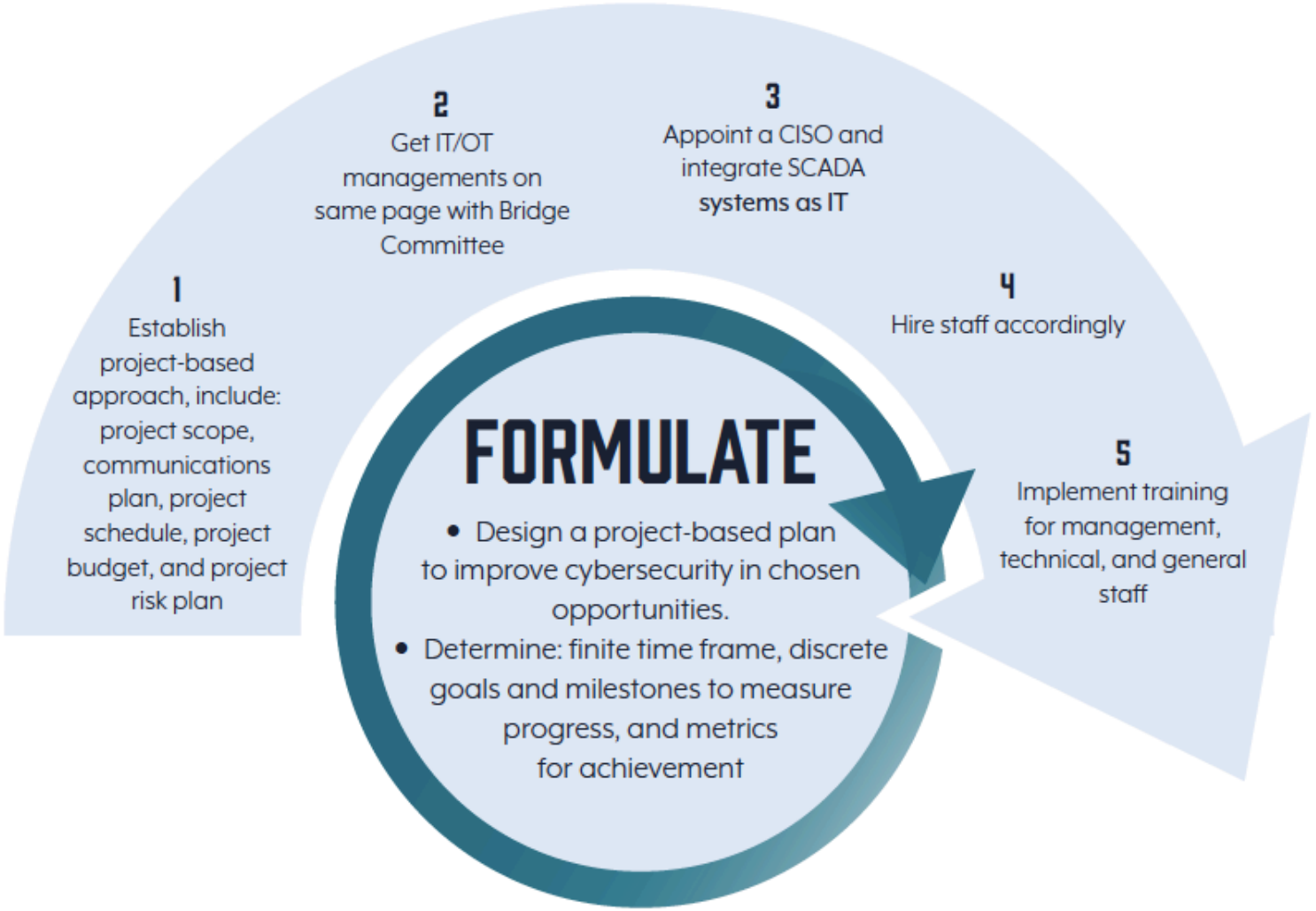



Evaluate
• Use Scorecard and other means to review internal and external factors influencing state of cybersecurity
• Identify two or three promising opportunities
• Advocate chosen opportunities to organizational management
Formulate
• Design a project-based plan to improve cybersecurity in chosen opportunities.
• Determine: finite time frame, discrete goals and milestones to measure progress, and metrics for achievement
AMERICAN PUBLIC POWER ASSOCIATION
Integrate
• Implement practices defined by your plan into the operation of your organization
• Engage employees and embed the organizational change into the company culture to ensure these cybersecurity improvements last
Activate
• Put the plan into action
• Identify and obtain the resources needed (e.g. funds, expertise)
• Assign clear owners and inform leaders and staff of changes to come
• Perform regular status checks against defined goals and milestones

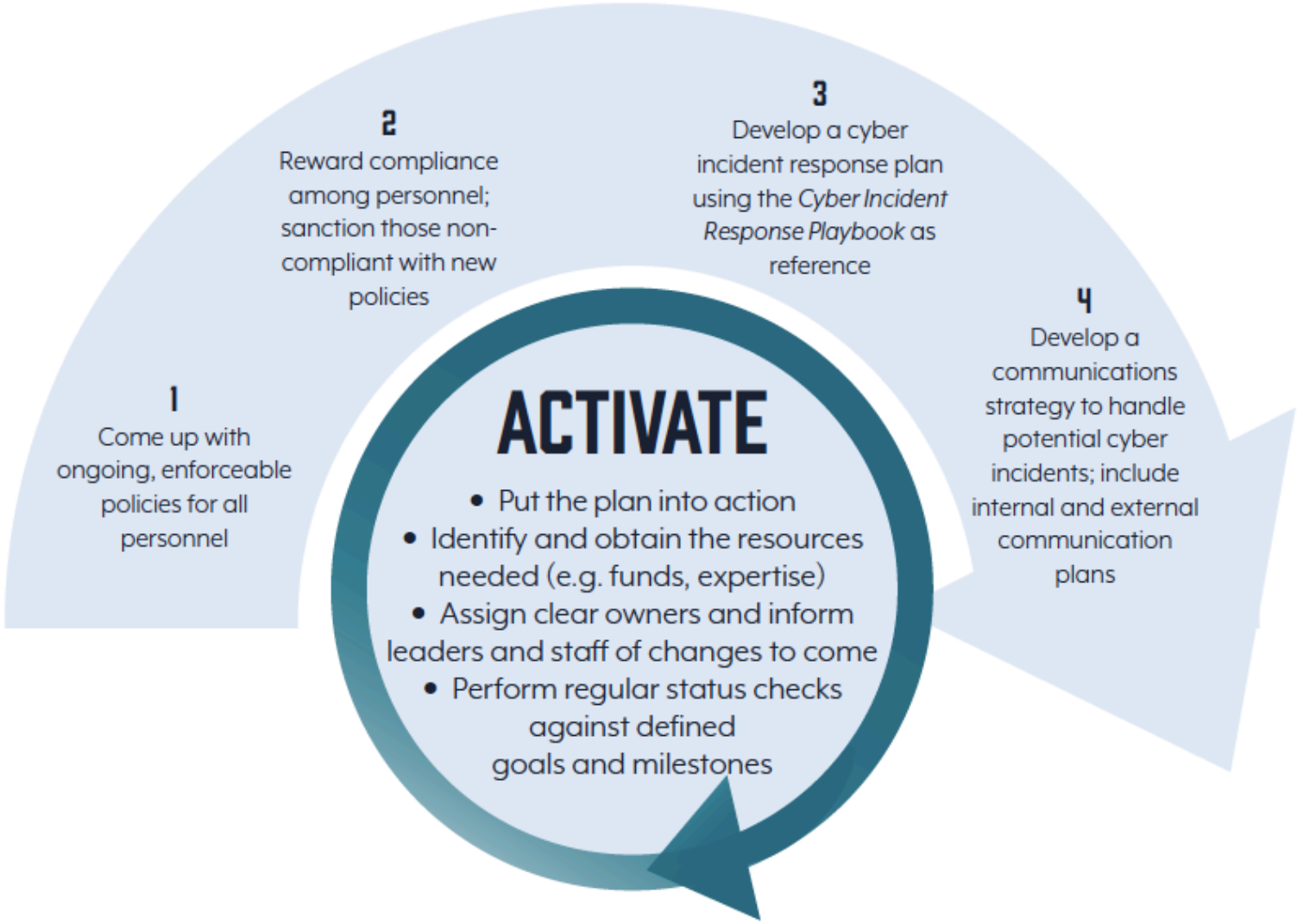
Stage 1: Evaluate



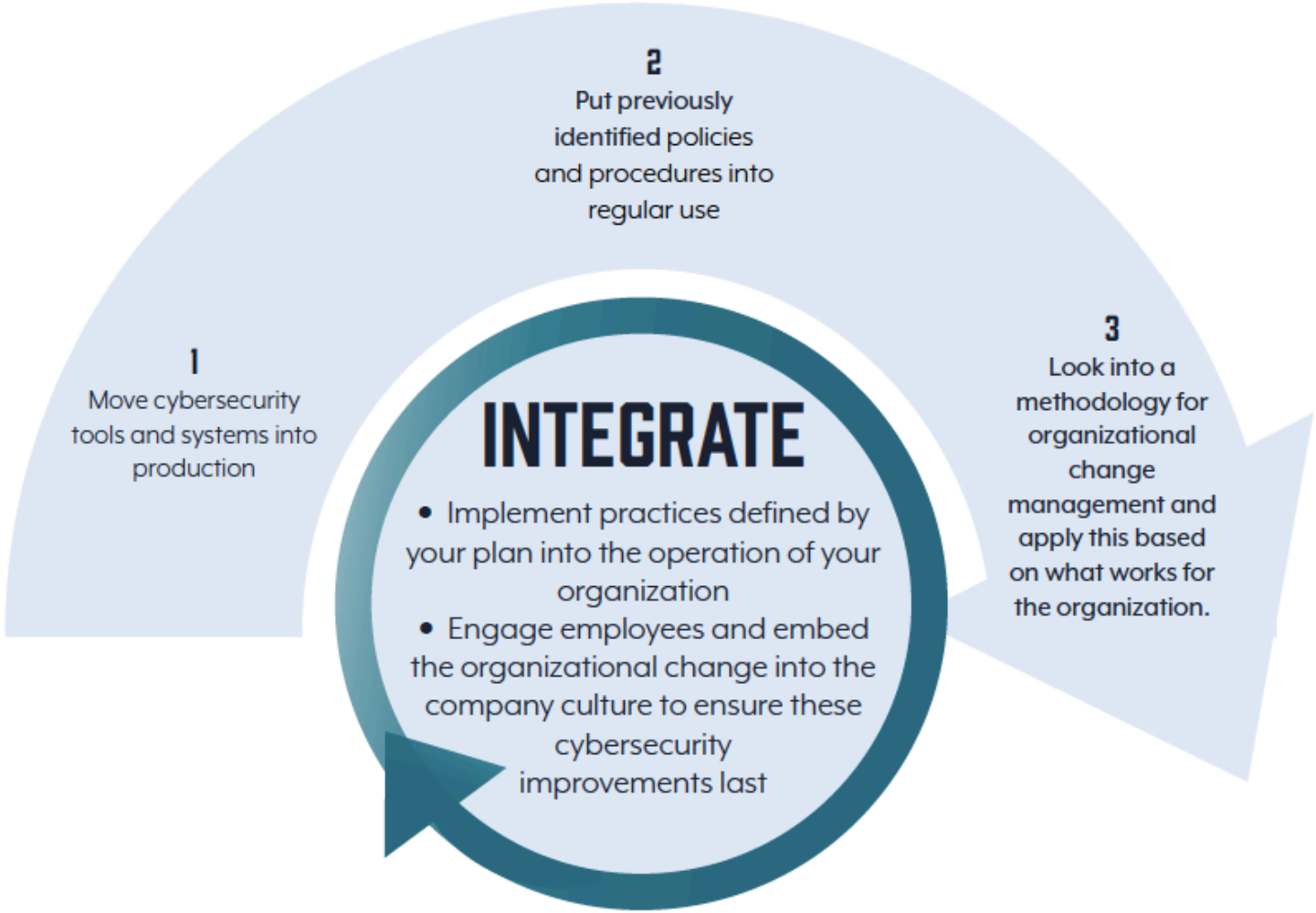
Stage 2: Formulate



Stage 3: Activate



Stage 4: Integrate



Next Steps

Next Steps

- The Roadmap serves as a guide
- Success of any project lies in its execution
  - The Roadmap should help chart a path to an improved state in the future.
- Communication among peers and collaboration with APPA and experienced subject matter experts may be necessary,
- Working together we can improve the cybersecurity of the entire public power sector

- Maintain a posture of continuous cybersecurity improvement, no matter the size of your public power utility.
- Take advantage of resources and tools available to public power utilities referenced in the Roadmap.
- For the latest recommendations visit APPA's website at: https://www.PublicPower.org or email Cybersecurity@PublicPower.org.

Questions?


I'M NOT AN ENGINEER, SO THIS MIGHT BE A DUMB QUESTION.
DILBERT.COM @SCOTTADAMSSAYS
BUT WHY CAN'T WE 3-D PRINT A BLOCKCHAIN AND HTML IT INTO A BITCOIN?
4-20-18 ©2018 Scott Adams, Inc./Dist. by Andrews McMeel
ALICE CAN ANSWER THAT.
I QUIT.