AMERICAN PUBLIC POWER ASSOCIATION™
Powering Strong Communities

axio

Cyber Readiness: What’s the Score?

Utilizing small batch, artisanal data to bring powerful insights

JASON D. CHRISTOPHER

CTO, Axio // ICS Security Lead

@jdchristopher
linkedin.com/in/jdchristopher

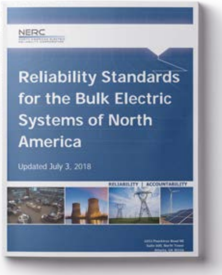
- Leads critical infrastructure strategy at Axio; actively involved in platform development
- SANS Instructor for ICS456
- Frequent speaker at conference and client events
- Federal energy lead for several industry standards and guidelines, including NERC CIPv5, NIST CSF, and the C2M2
- Incident response and risk management lead for DOE
- Security metrics development across EPRI and other research organizations
- Began career building control systems at a utility
- MS, Electrical Engineering, Cornell
- Based in Atlanta, GA

ELECTRICITY CYBERSECU

OIL AND NA CYBERSECUR

CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

Version 1.1
February 2014



NERC

Reliability Standards for the Bulk Electric Systems of North America

Updated July 3, 2018

RELIABILITY | ACCOUNTABILITY

Incentivizing Cyber Security: A Case for Cyber Insurance

Written by
Jason D. Christopher

June 2017

SANS

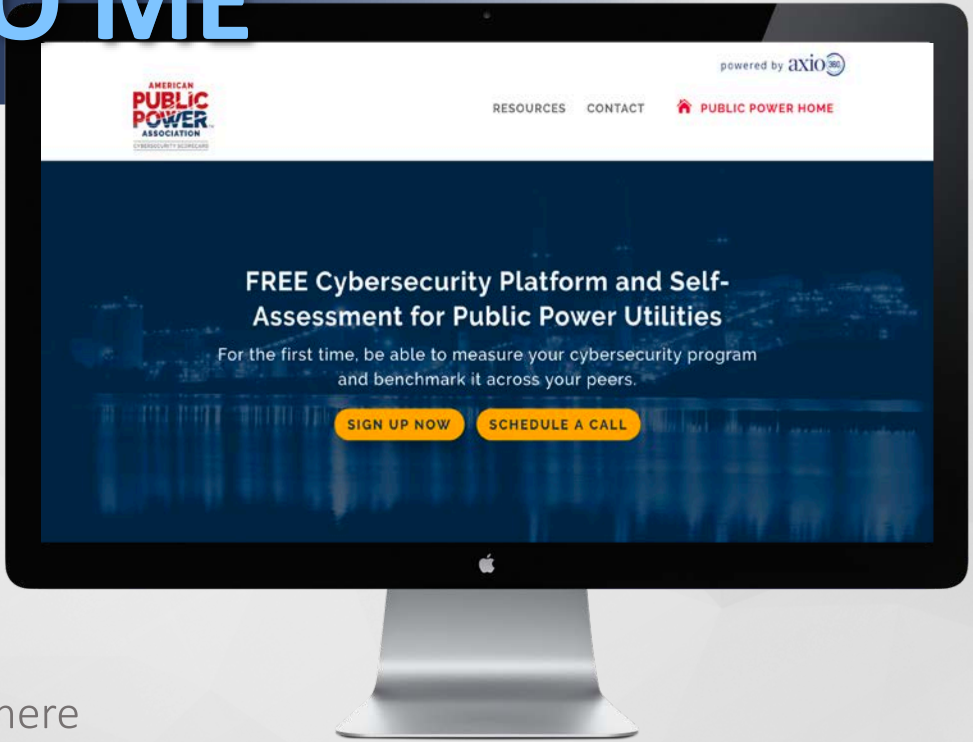
EPRI ELECTRIC POWER RESEARCH INSTITUTE

unlike most speakers
DON'T LISTEN TO ME

Be distracted, look things up!

Listen to your peers

- Over 250 public power utilities online
- 400+ active users
- Use cases from actual practitioners
- I'm just another pretty beard.



powered by axio360

AMERICAN PUBLIC POWER ASSOCIATION CYBERSECURITY SCORECARD

RESOURCES CONTACT PUBLIC POWER HOME

FREE Cybersecurity Platform and Self-Assessment for Public Power Utilities

For the first time, be able to measure your cybersecurity program and benchmark it across your peers.

SIGN UP NOW SCHEDULE A CALL

Visit: http://scorecard.axio.com while I'm here

myth #1

GETTING DATA IS HARD ☹

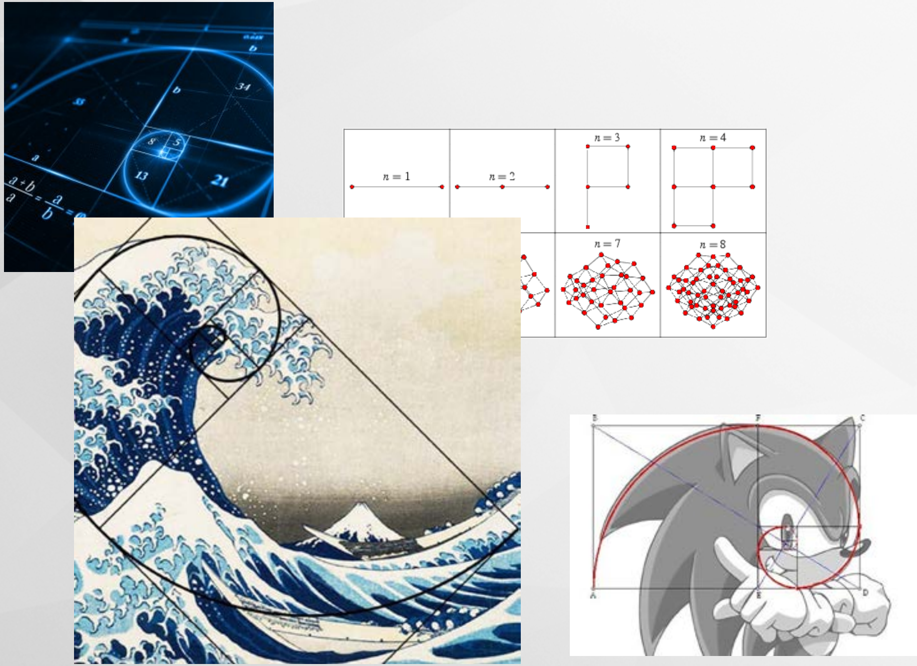
Then you're doing this wrong

- **You really mean "I need the right starting point"**
  - What *can* you measure? Start somewhere
  - Understand that metrics improve with time (only barbarians measure in "stones" and "feet")
  - Resources may be constrained at first
    - But if you don't try, it won't get better

Literally, just do *something*.

myth #2

SECURITY IS AN ART



Really bad argument here…

- **There's measurement in almost everything**
  - Can you document something?
  - Can you count something?
  - Observe the trends where you can

Literally, just do *anything*.

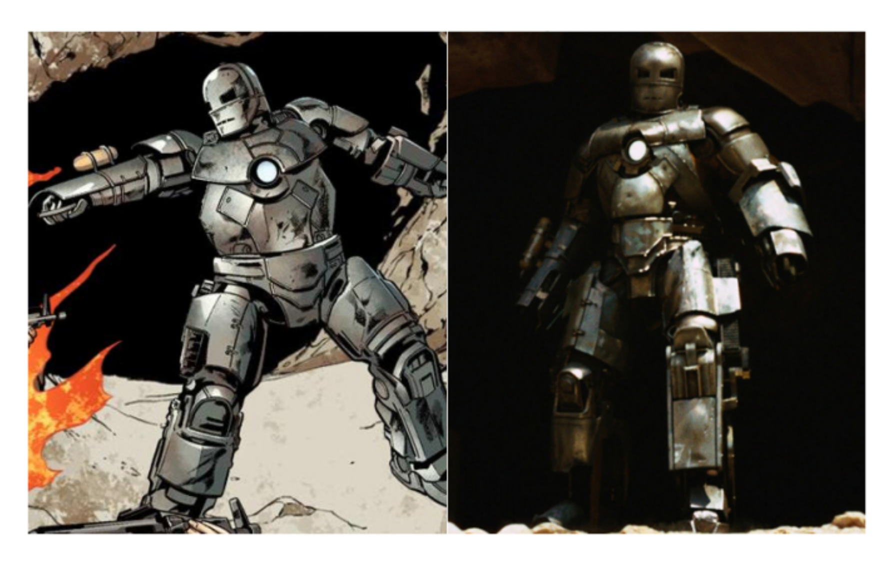
myth #3

THIS TAKES TOO MUCH TIME

Engineering 101: “Optimize within your constraints.”

- **Size your efforts to your team**
  - Team of 1? That still works (more on this later)
  - Don’t boil the ocean and don’t build a team to “admire the problem.”
  - Anything worth doing takes time and effort!

“If you’re not keeping score, you’re just practicing” – Vince Lombardi



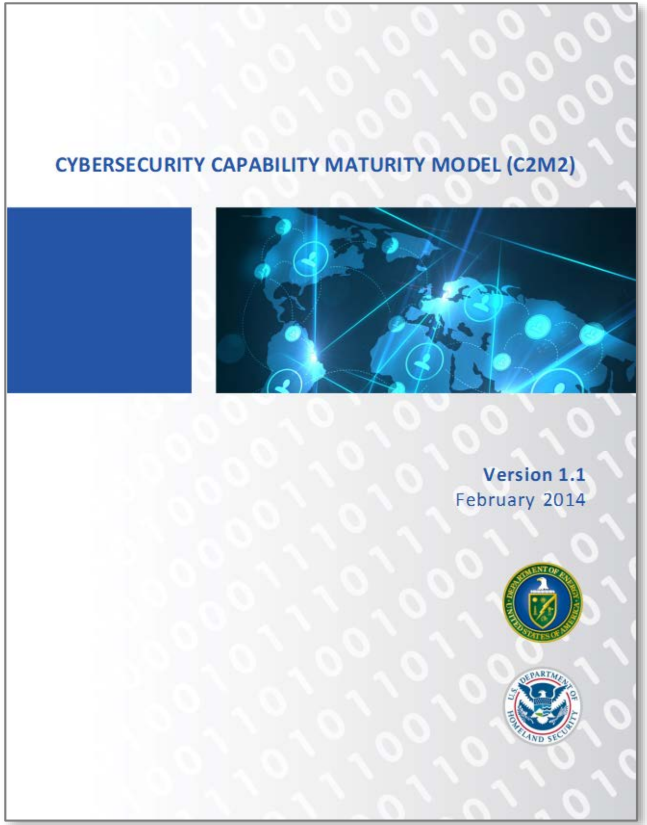
how did i

START?

ARE YOU #CyberReady?

The American Public Power Association is proud to present the all new Cybersecurity Scorecard. This robust platform is the result of a federally-funded cybersecurity improvement initiative that will be openly accessible to all Association members.

Cybersecurity Capability Maturity Model (C2M2) v1.1



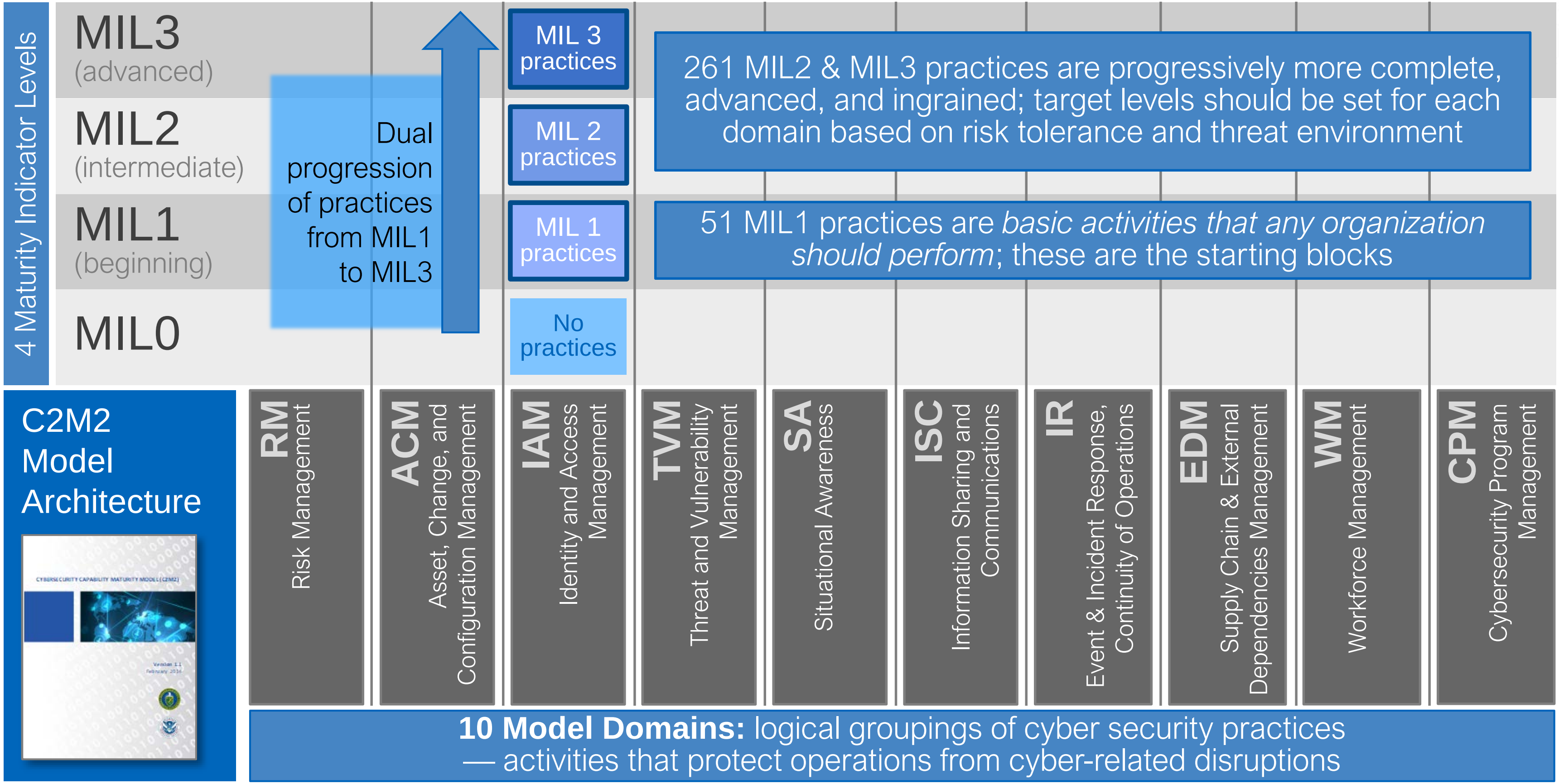
CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

Version 1.1
February 2014

A model and evaluation method to support ongoing evaluation and improvement of cybersecurity capabilities in IT and OT environments

Objectives

- Strengthen organizations’ cybersecurity capabilities
- Enable organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities
- Share knowledge, best practices, and relevant references as a means to improve cybersecurity capabilities.
- Enable organizations to prioritize actions and investments to improve cybersecurity



4 Maturity Indicator Levels

MIL3 (advanced)

MIL2 (intermediate)

MIL1 (beginning)

MIL0

Dual progression of practices from MIL1 to MIL3

MIL 3 practices

MIL 2 practices

MIL 1 practices

No practices

261 MIL2 & MIL3 practices are progressively more complete, advanced, and ingrained; target levels should be set for each domain based on risk tolerance and threat environment

51 MIL1 practices are *basic activities that any organization should perform*; these are the starting blocks

C2M2 Model Architecture

RM Risk Management

ACM Asset, Change, and Configuration Management

IAM Identity and Access Management

TVM Threat and Vulnerability Management

SA Situational Awareness

ISC Information Sharing and Communications

IR Event & Incident Response, Continuity of Operations

EDM Supply Chain & External Dependencies Management

WM Workforce Management

CPM Cybersecurity Program Management

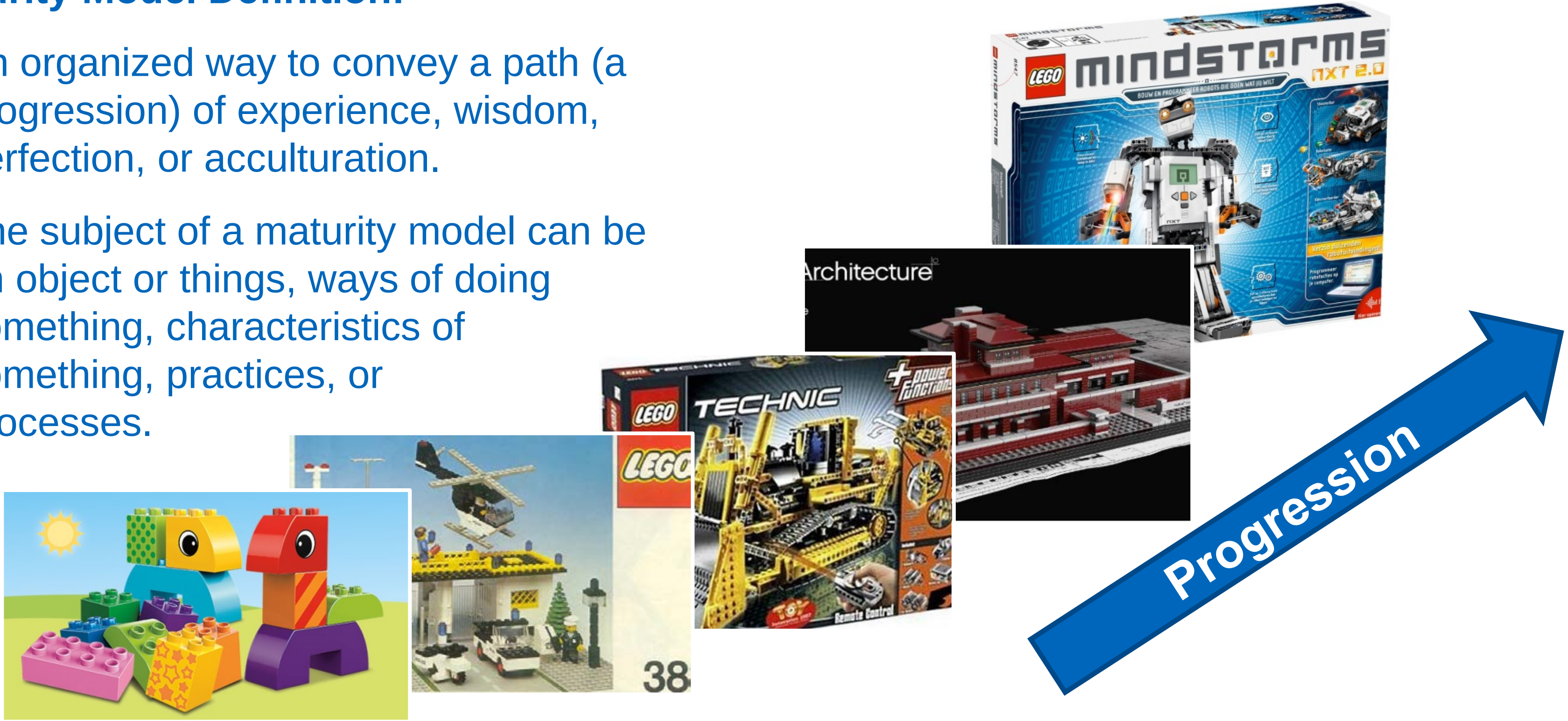
10 Model Domains: logical groupings of cyber security practices — activities that protect operations from cyber-related disruptions

Cybersecurity Capability

The Approach: Maturity Model

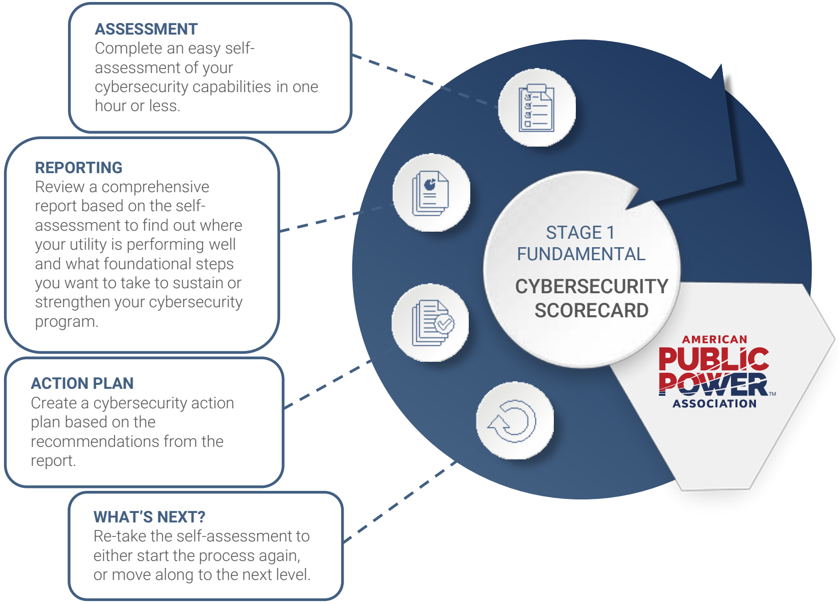
Maturity Model Definition:

- An organized way to convey a path (a progression) of experience, wisdom, perfection, or acculturation.
- The subject of a maturity model can be an object or things, ways of doing something, characteristics of something, practices, or processes.



CYBERSECURITY SCORECARD

APPA CYBERSECURITY SCORECARD



ASSESSMENT
Complete an easy self-assessment of your cybersecurity capabilities in one hour or less.

REPORTING
Review a comprehensive report based on the self-assessment to find out where your utility is performing well and what foundational steps you want to take to sustain or strengthen your cybersecurity program.

ACTION PLAN
Create a cybersecurity action plan based on the recommendations from the report.

WHAT'S NEXT?
Re-take the self-assessment to either start the process again, or move along to the next level.

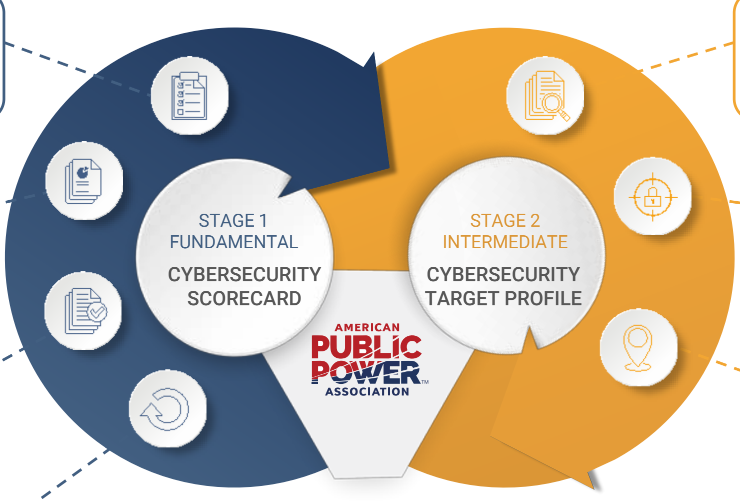
APPA CYBERSECURITY SCORECARD

ASSESSMENT
Complete an easy self-assessment of your cybersecurity capabilities in one hour or less.

REPORTING
Review a comprehensive report based on the self-assessment to find out where your utility is performing well and what foundational steps you want to take to sustain or strengthen your cybersecurity program.

ACTION PLAN
Create a cybersecurity action plan based on the recommendations from the report.

WHAT'S NEXT?
Re-take the self-assessment to either start the process again, or move along to the next level.


STAGE 1
FUNDAMENTAL
CYBERSECURITY SCORECARD
STAGE 2
INTERMEDIATE
CYBERSECURITY TARGET PROFILE
AMERICAN PUBLIC POWER ASSOCIATION

IN-DEPTH ANALYSIS
Get a third-party assessment of your utility's more advanced cybersecurity capabilities and posture.

TARGET PROFILE
Receive a customized target profile from public power experts.

ROADMAP
Follow an industry-vetted roadmap for making security improvements.

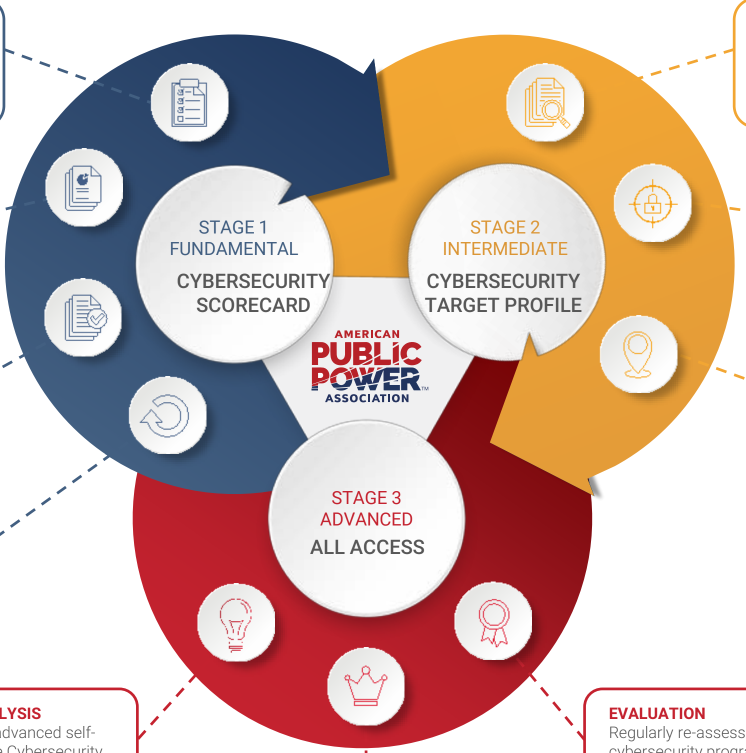
APPA CYBERSECURITY SCORECARD

ASSESSMENT
Complete an easy self-assessment of your cybersecurity capabilities in one hour or less.

REPORTING
Review a comprehensive report based on the self-assessment to find out where your utility is performing well and what foundational steps you want to take to sustain or strengthen your cybersecurity program.

ACTION PLAN
Create a cybersecurity action plan based on the recommendations from the report.

WHAT'S NEXT?
Re-take the self-assessment to either start the process again, or move along to the next level.



STAGE 1
FUNDAMENTAL
CYBERSECURITY SCORECARD

STAGE 2
INTERMEDIATE
CYBERSECURITY TARGET PROFILE

STAGE 3
ADVANCED
ALL ACCESS

IN-DEPTH ANALYSIS
Get a third-party assessment of your utility's more advanced cybersecurity capabilities and posture.

TARGET PROFILE
Receive a customized target profile from public power experts.

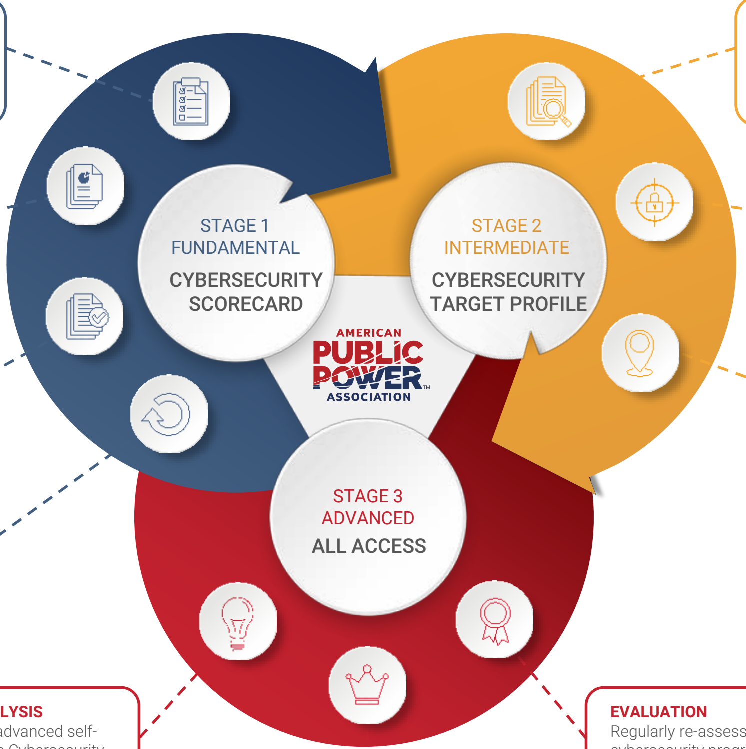
ROADMAP
Follow an industry-vetted roadmap for making security improvements.

IN-DEPTH ANALYSIS
Take the most advanced self-assessment, the Cybersecurity Capability Maturity Model.

TARGET PROFILE
Create an individualized target profile and make cybersecurity decisions on your own.

EVALUATION
Regularly re-assess your cybersecurity program to stay up-to-date on best practices.

APPA CYBERSECURITY SCORECARD



ASSESSMENT
Complete an easy self-assessment of your cybersecurity capabilities in one hour or less.

REPORTING
Review a comprehensive report based on the self-assessment to find out where your utility is performing well and what foundational steps you want to take to sustain or strengthen your cybersecurity program.

ACTION PLAN
Create a cybersecurity action plan based on the recommendations from the report.

WHAT'S NEXT?
Re-take the self-assessment to either start the process again, or move along to the next level.

IN-DEPTH ANALYSIS
Get a third-party assessment of your utility's more advanced cybersecurity capabilities and posture.

TARGET PROFILE
Receive a customized target profile from public power experts.

ROADMAP
Follow an industry-vetted roadmap for making security improvements.

IN-DEPTH ANALYSIS
Take the most advanced self-assessment, the Cybersecurity Capability Maturity Model.

TARGET PROFILE
Create an individualized target profile and make cybersecurity decisions on your own.

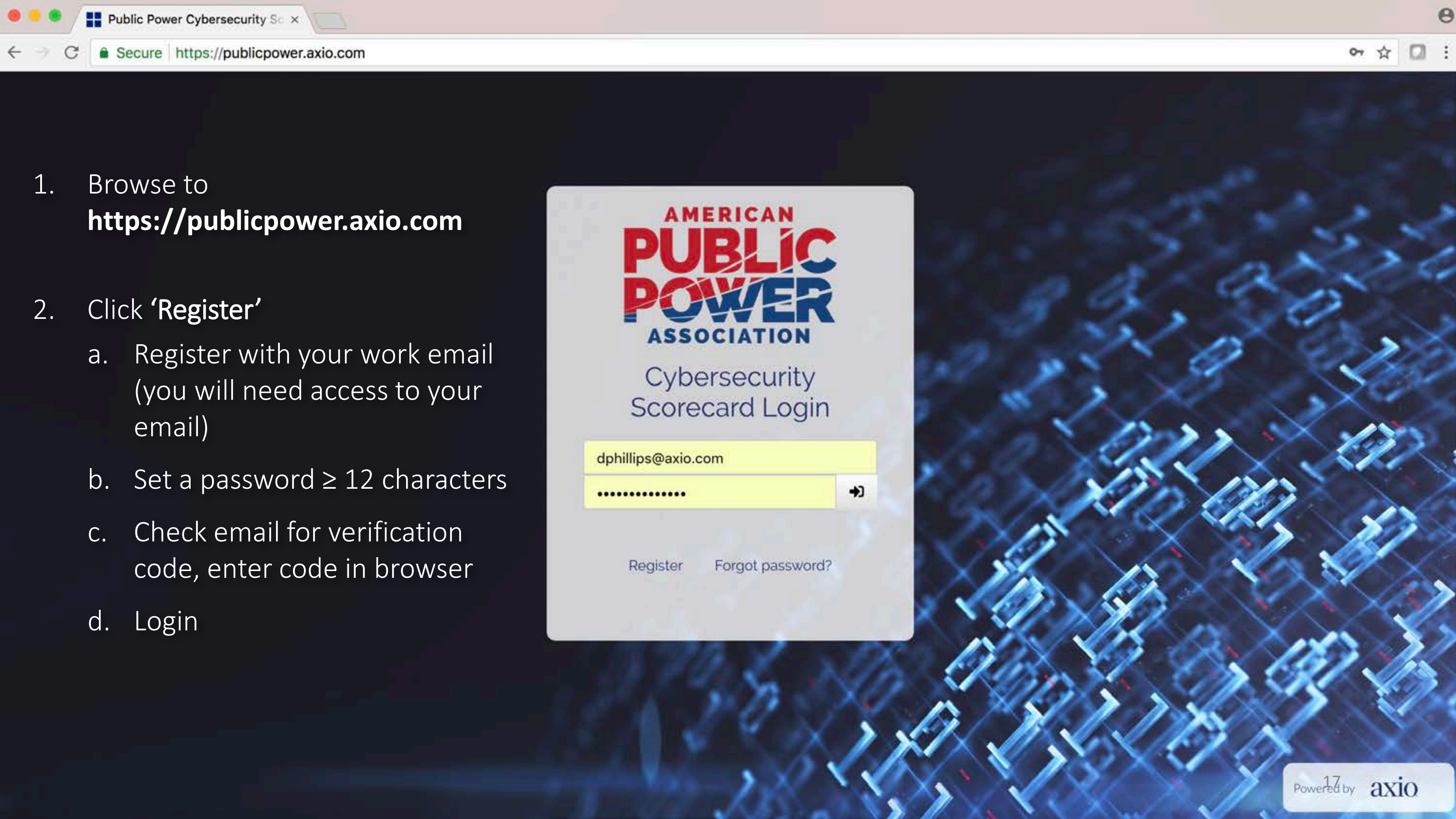
EVALUATION
Regularly re-assess your cybersecurity program to stay up-to-date on best practices.

ONLINE PORTAL FEATURES

- Take notes for each practice within the platform.
- Assign tasks to individuals with deadlines.
- Help text in each section including definitions and concepts.
- User dashboard showcasing each assessment and various statistics in real time.
- Ability to do multiple internal assessments and benchmarking.
- Improvement toolkit including document templates, policies and example policies.
- Regional workshops to provide additional help and guidance.
- Suggestions for cybersecurity training.
- Expert coaching
- Ability to tie to other association projects, such as technology deployments and vulnerability assessments.
- Each level is capable of being a fully sustainable cybersecurity program and can be reassessed on a regular basis to track improvements.

1. Browse to **https://publicpower.axio.com**

2. Click **‘Register’**
   a. Register with your work email (you will need access to your email)
   b. Set a password ≥ 12 characters
   c. Check email for verification code, enter code in browser
   d. Login



Public Power Cybersecurity Sc

Secure https://publicpower.axio.com

Cybersecurity Scorecard Login

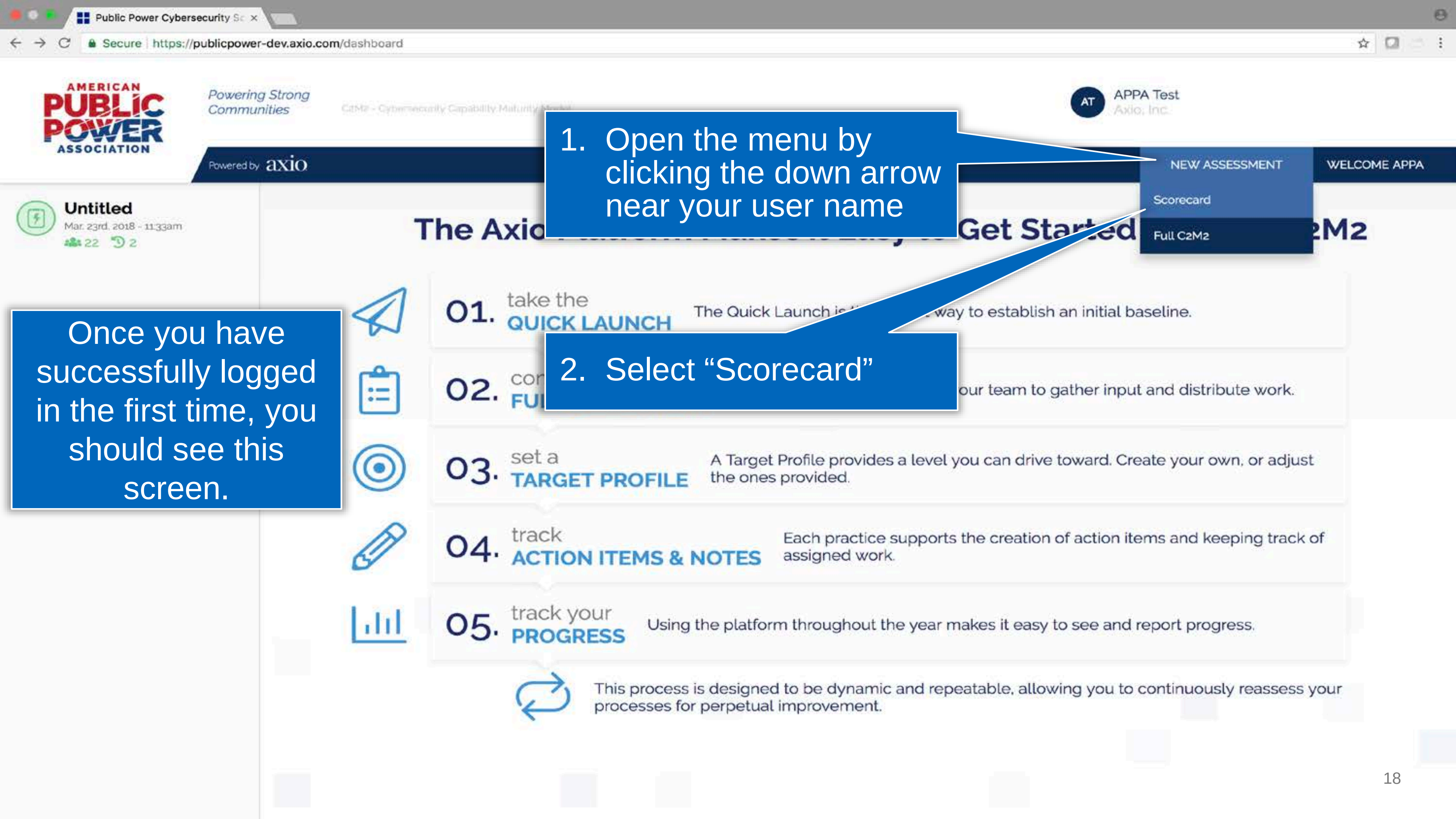
dphillips@axio.com

•••••••••••••••

Once you have successfully logged in the first time, you should see this screen.

1. Open the menu by clicking the down arrow near your user name

2. Select “Scorecard”


Public Power Cybersecurity Sc ×
Secure https://publicpower-dev.axio.com/dashboard
AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities
C2M2 - Cybersecurity Capability Maturity Model
AT
APPA Test
Axio, Inc.
Powered by axio
NEW ASSESSMENT
WELCOME APPA
Scorecard
Full C2M2
Untitled
Mar. 23rd, 2018 - 11:33am
22
2

The Axio ... Get Started ... 2M2

01. take the **QUICK LAUNCH** The Quick Launch is ... way to establish an initial baseline.

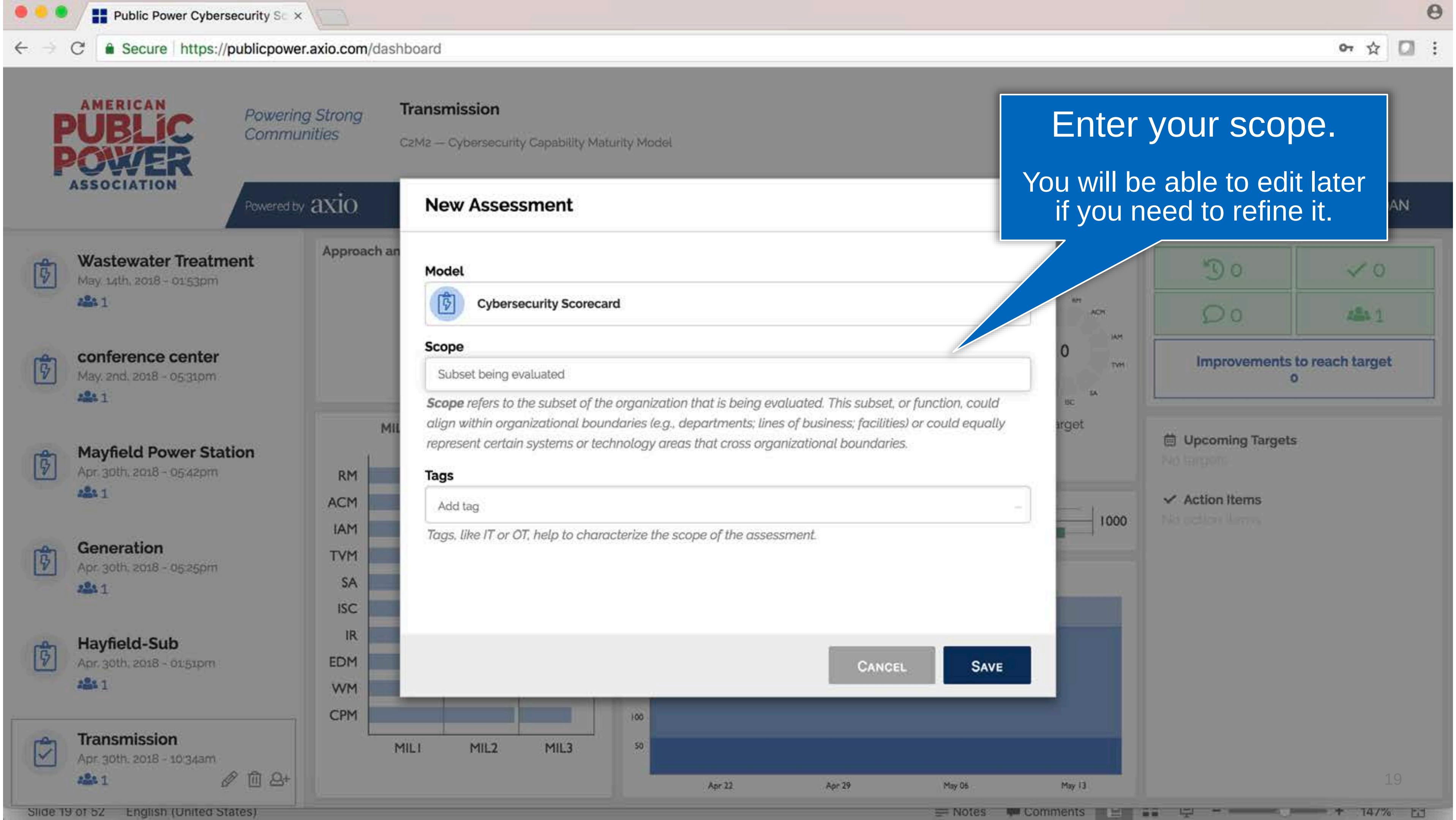
02. co... FU... ...our team to gather input and distribute work.

03. set a **TARGET PROFILE** A Target Profile provides a level you can drive toward. Create your own, or adjust the ones provided.

04. track **ACTION ITEMS & NOTES** Each practice supports the creation of action items and keeping track of assigned work.

05. track your **PROGRESS** Using the platform throughout the year makes it easy to see and report progress.

This process is designed to be dynamic and repeatable, allowing you to continuously reassess your processes for perpetual improvement.


Public Power Cybersecurity Sc
Secure
https://publicpower.axio.com/dashboard
AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities
Powered by axio
Transmission
C2M2 — Cybersecurity Capability Maturity Model
Wastewater Treatment
May. 14th, 2018 - 01:53pm
1
conference center
May. 2nd, 2018 - 05:31pm
1
Mayfield Power Station
Apr. 30th, 2018 - 05:42pm
1
Generation
Apr. 30th, 2018 - 05:25pm
1
Hayfield-Sub
Apr. 30th, 2018 - 01:51pm
1
Transmission
Apr. 30th, 2018 - 10:34am
1
Approach an
RM
ACM
IAM
TVM
SA
ISC
IR
EDM
WM
CPM
MIL1
MIL2
MIL3
1000
100
50
Apr 22
Apr 29
May 06
May 13
0
0
0
1
Improvements to reach target
0
Upcoming Targets
Action Items
Slide 19 of 52
English (United States)
Notes
Comments
147%

New Assessment

Model

Cybersecurity Scorecard

Scope

Subset being evaluated

__Scope__ refers to the subset of the organization that is being evaluated. This subset, or function, could align within organizational boundaries (e.g., departments; lines of business; facilities) or could equally represent certain systems or technology areas that cross organizational boundaries.

Tags

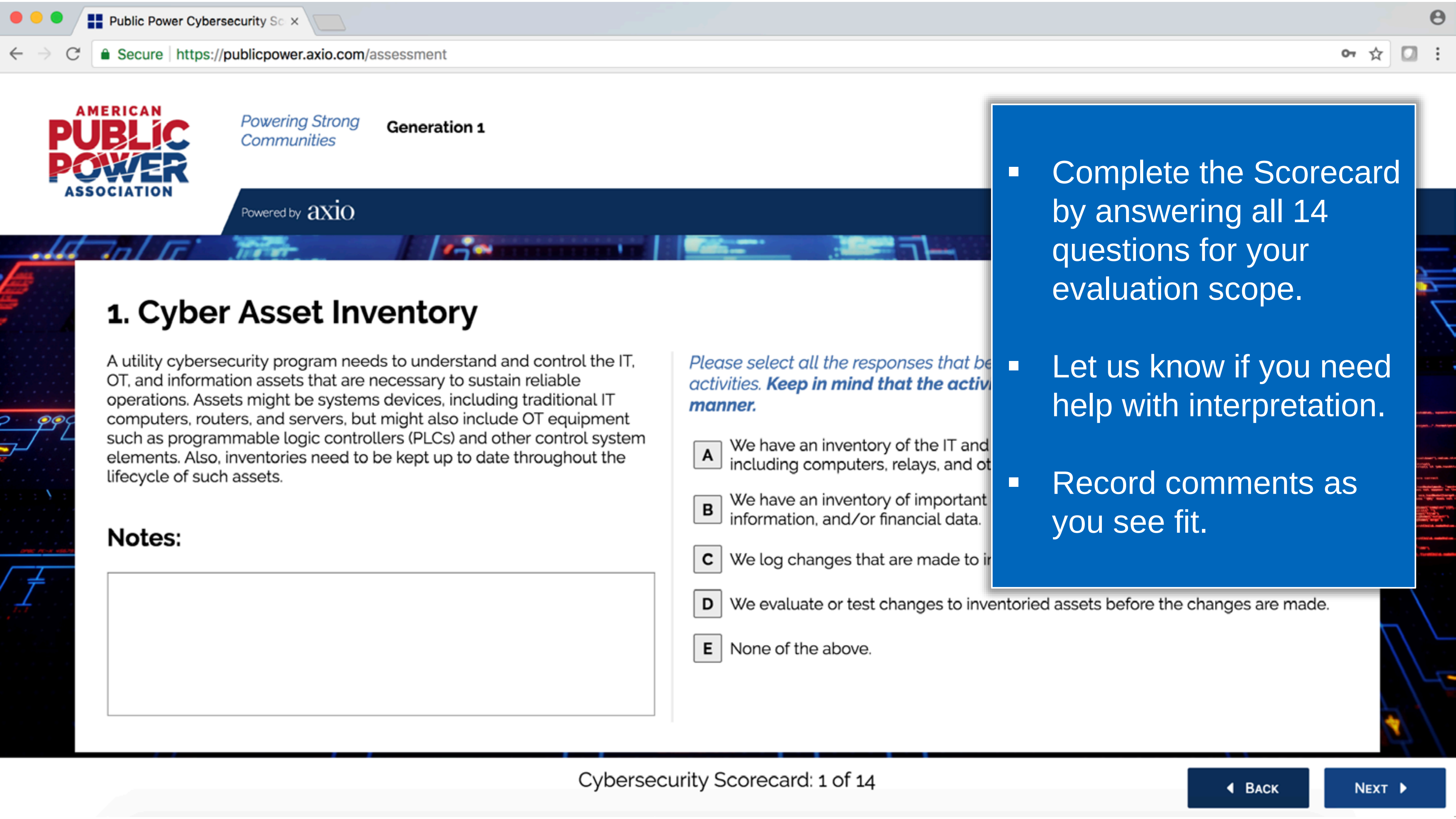
Add tag

Tags, like IT or OT, help to characterize the scope of the assessment.

CANCEL SAVE

Enter your scope.

You will be able to edit later if you need to refine it.


Public Power Cybersecurity Sc
Secure
https://publicpower.axio.com/assessment
AMERICAN PUBLIC POWER ASSOCIATION
Powered by axio
Back
Next

Powering Strong Communities

Generation 1

1. Cyber Asset Inventory

A utility cybersecurity program needs to understand and control the IT, OT, and information assets that are necessary to sustain reliable operations. Assets might be systems devices, including traditional IT computers, routers, and servers, but might also include OT equipment such as programmable logic controllers (PLCs) and other control system elements. Also, inventories need to be kept up to date throughout the lifecycle of such assets.

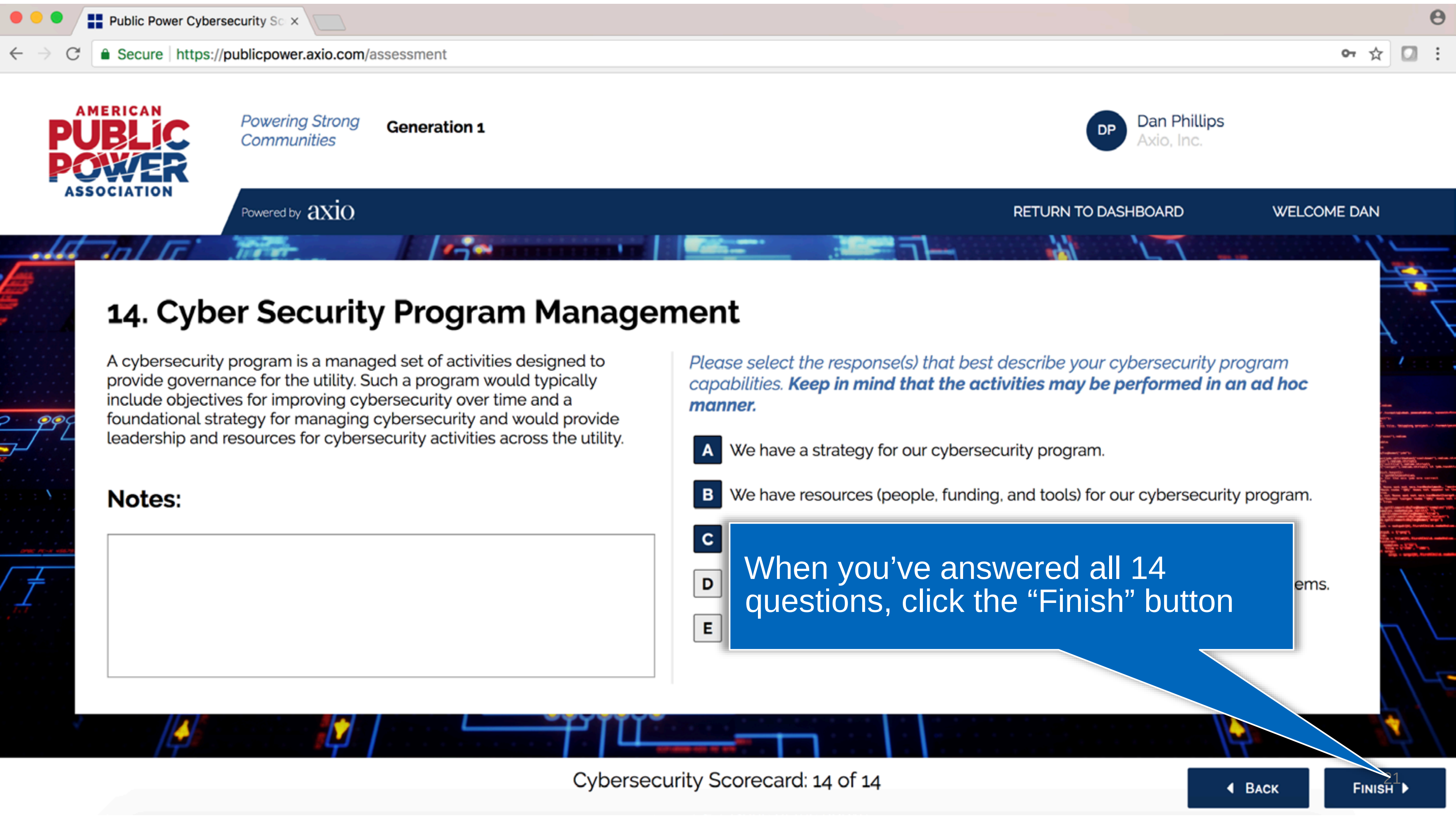
Notes:

*Please select all the responses that be activities. **Keep in mind that the activi manner.***

- A We have an inventory of the IT and including computers, relays, and ot
- B We have an inventory of important information, and/or financial data.
- C We log changes that are made to i
- D We evaluate or test changes to inventoried assets before the changes are made.
- E None of the above.

Cybersecurity Scorecard: 1 of 14

- Complete the Scorecard by answering all 14 questions for your evaluation scope.
- Let us know if you need help with interpretation.
- Record comments as you see fit.


Public Power Cybersecurity Sc
Secure https://publicpower.axio.com/assessment
AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities
Generation 1
DP
Dan Phillips
Axio, Inc.
Powered by axio
RETURN TO DASHBOARD
WELCOME DAN
BACK
FINISH

14. Cyber Security Program Management

A cybersecurity program is a managed set of activities designed to provide governance for the utility. Such a program would typically include objectives for improving cybersecurity over time and a foundational strategy for managing cybersecurity and would provide leadership and resources for cybersecurity activities across the utility.

Notes:

Please select the response(s) that best describe your cybersecurity program capabilities. ***Keep in mind that the activities may be performed in an ad hoc manner.***

A We have a strategy for our cybersecurity program.

B We have resources (people, funding, and tools) for our cybersecurity program.

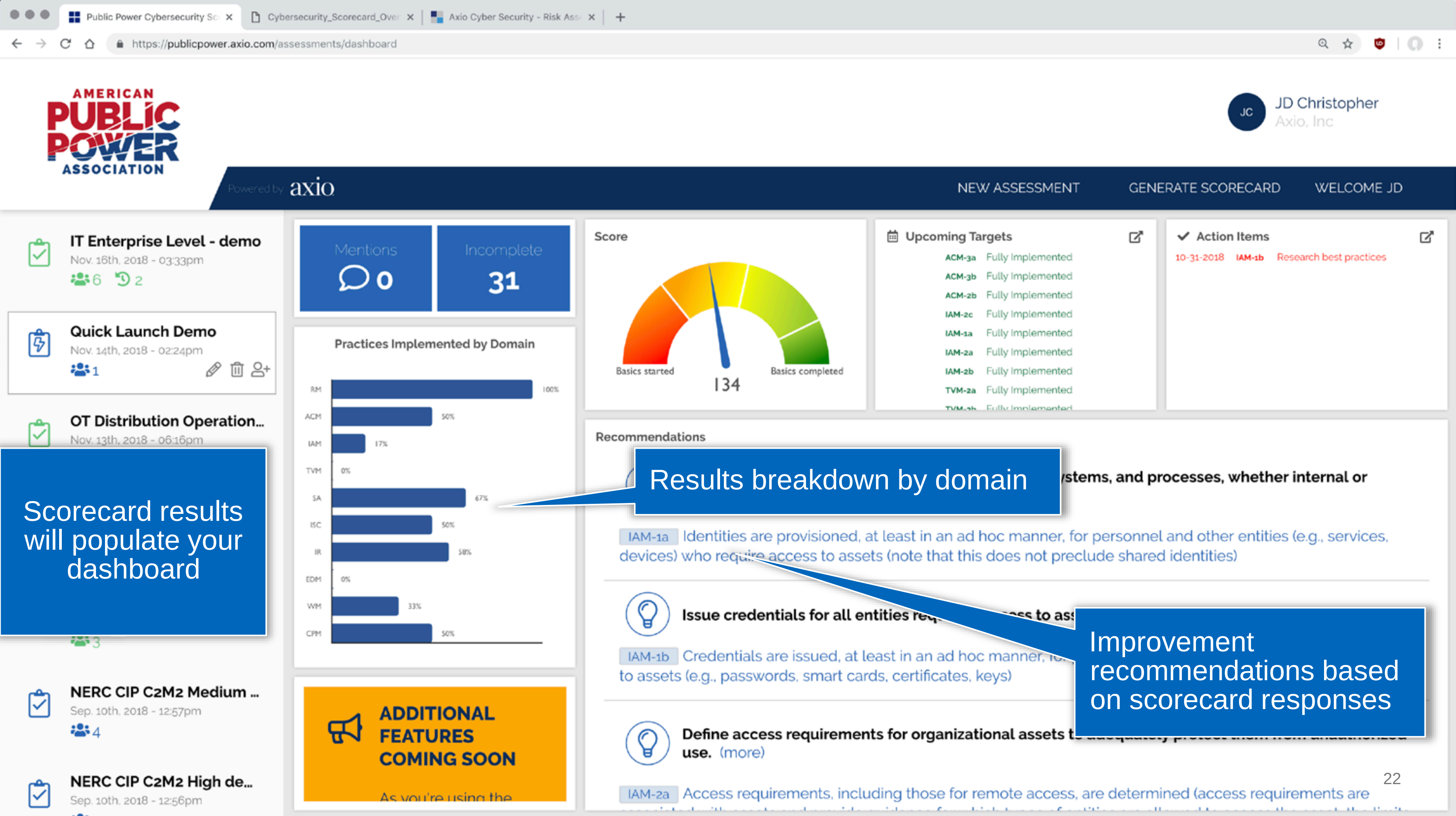
C

D ems.

E

Cybersecurity Scorecard: 14 of 14

When you’ve answered all 14 questions, click the “Finish” button


Public Power Cybersecurity Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
https://publicpower.axio.com/assessments/dashboard
AMERICAN PUBLIC POWER ASSOCIATION
Powered by axio
NEW ASSESSMENT
GENERATE SCORECARD
WELCOME JD
JC
JD Christopher
Axio, Inc

IT Enterprise Level - demo
Nov. 16th, 2018 - 03:33pm
6 2

Quick Launch Demo
Nov. 14th, 2018 - 02:24pm
1

OT Distribution Operation...
Nov. 13th, 2018 - 06:16pm
3

NERC CIP C2M2 Medium ...
Sep. 10th, 2018 - 12:57pm
4

NERC CIP C2M2 High de...
Sep. 10th, 2018 - 12:56pm

Mentions 0

Incomplete 31

Practices Implemented by Domain

ADDITIONAL FEATURES COMING SOON

As you're using the

Score

Upcoming Targets

ACM-3a	Fully Implemented
ACM-3b	Fully Implemented
ACM-2b	Fully Implemented
IAM-2c	Fully Implemented
IAM-1a	Fully Implemented
IAM-2a	Fully Implemented
IAM-2b	Fully Implemented
TVM-2a	Fully Implemented
TVM-2b	Fully Implemented

Action Items

10-31-2018 IAM-1b Research best practices

Recommendations

ystems, and processes, whether internal or

IAM-1a Identities are provisioned, at least in an ad hoc manner, for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities)

Issue credentials for all entities req ss to as

IAM-1b Credentials are issued, at least in an ad hoc manner, fo to assets (e.g., passwords, smart cards, certificates, keys)

Define access requirements for organizational assets t use. (more)

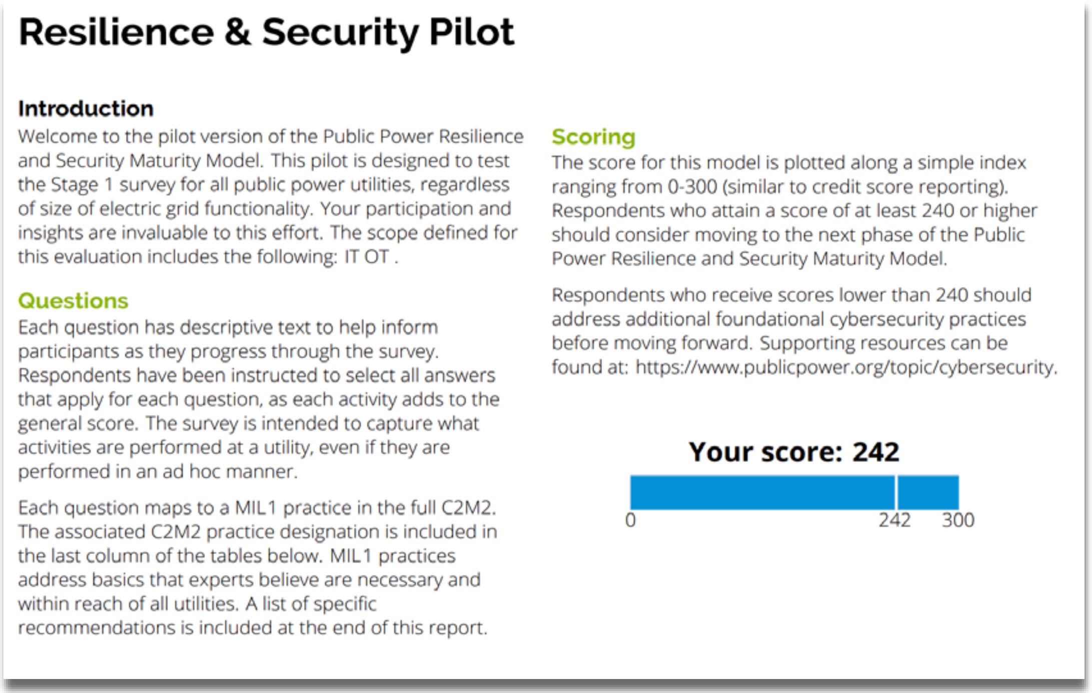
IAM-2a Access requirements, including those for remote access, are determined (access requirements are

Scorecard results will populate your dashboard

Results breakdown by domain

Improvement recommendations based on scorecard responses

Results: Scorecard



Resilience & Security Pilot

Introduction

Welcome to the pilot version of the Public Power Resilience and Security Maturity Model. This pilot is designed to test the Stage 1 survey for all public power utilities, regardless of size of electric grid functionality. Your participation and insights are invaluable to this effort. The scope defined for this evaluation includes the following: IT OT .

Questions

Each question has descriptive text to help inform participants as they progress through the survey. Respondents have been instructed to select all answers that apply for each question, as each activity adds to the general score. The survey is intended to capture what activities are performed at a utility, even if they are performed in an ad hoc manner.

Each question maps to a MIL1 practice in the full C2M2. The associated C2M2 practice designation is included in the last column of the tables below. MIL1 practices address basics that experts believe are necessary and within reach of all utilities. A list of specific recommendations is included at the end of this report.

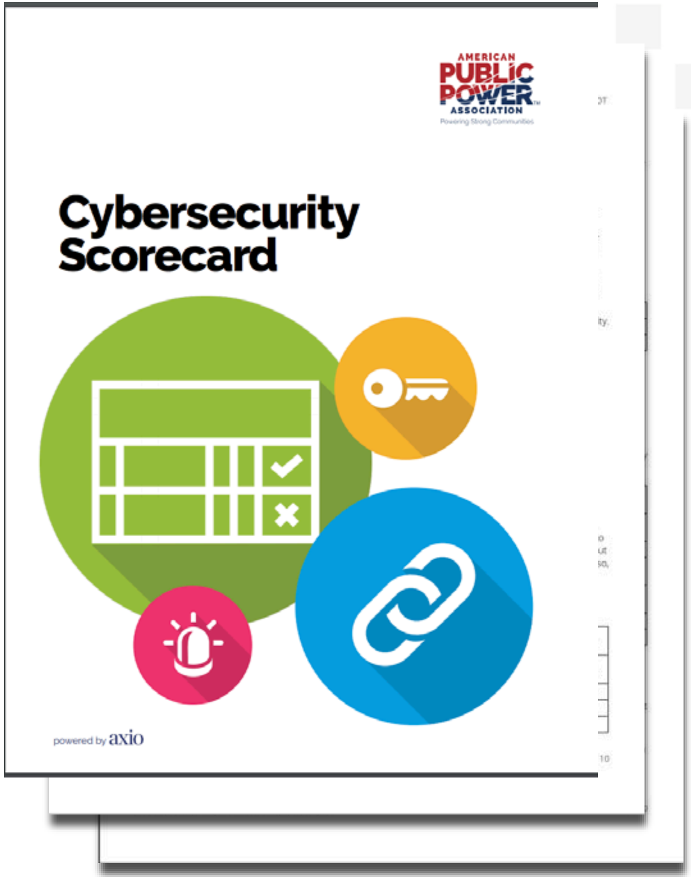
Scoring

The score for this model is plotted along a simple index ranging from 0-300 (similar to credit score reporting). Respondents who attain a score of at least 240 or higher should consider moving to the next phase of the Public Power Resilience and Security Maturity Model.

Respondents who receive scores lower than 240 should address additional foundational cybersecurity practices before moving forward. Supporting resources can be found at: https://www.publicpower.org/topic/cybersecurity.

Your score: 242

0 242 300



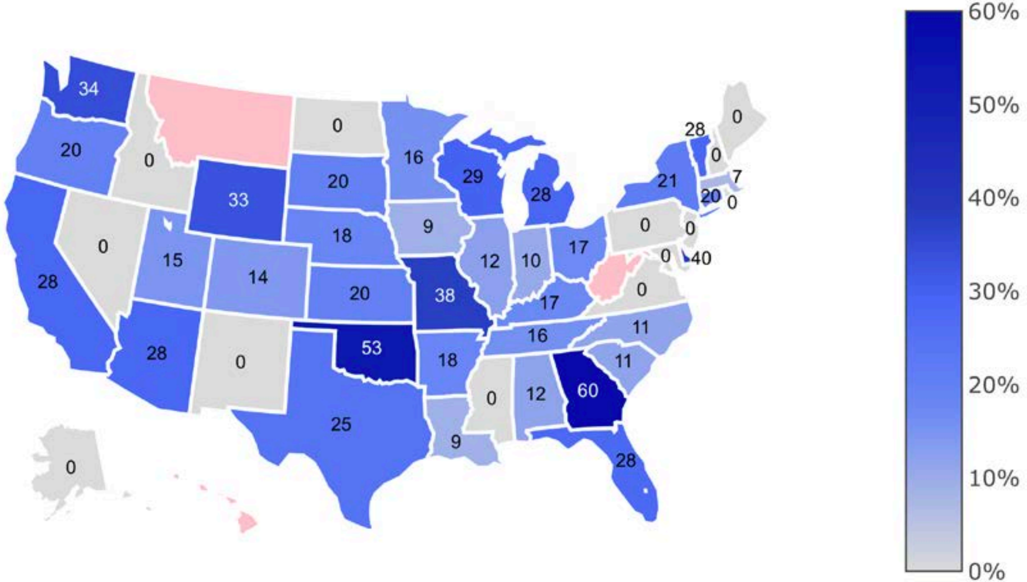
AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

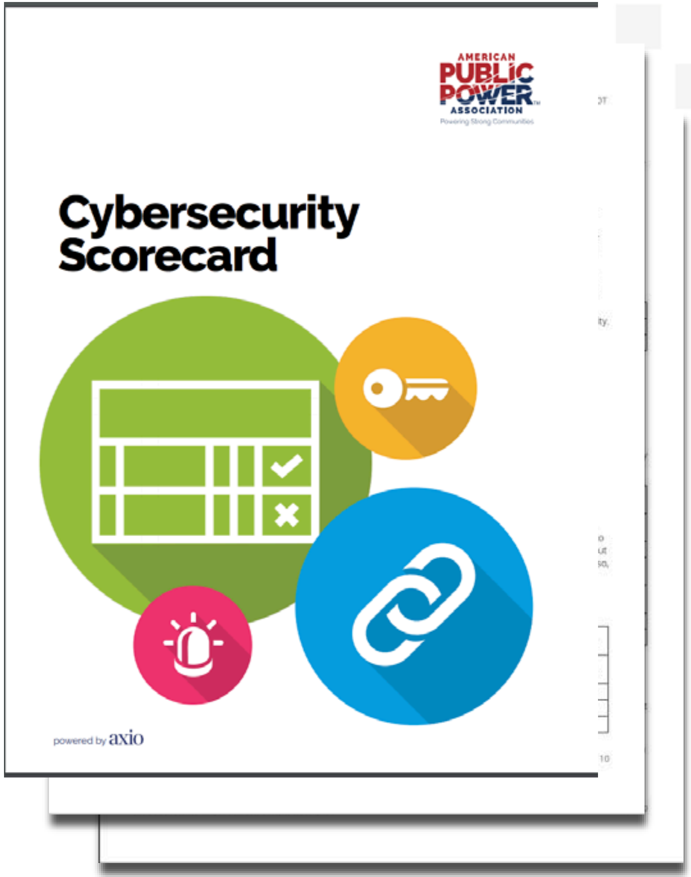
Cybersecurity Scorecard

powered by axio

Cybersecurity Scorecard Today

Platform Users as Percent of all Medium and Large Municipal Utilities




AMERICAN PUBLIC POWER ASSOCIATION

Powering Strong Communities

Cybersecurity Scorecard

powered by axio

Again, don’t listen to me…

LET’S ASK USERS

axio®

THANK YOU

Jason Christopher
Chief Technology Officer
jchristopher@axio.com
@jdchristopher
linkedin.com/in/jdchristopher