# CYBERSECURITY

## An Overview

January 3, 2017

P.U.D.
CHELAN COUNTY
www.chelanpud.org

# Today's Presentation

- Where we are today
- Industry cybersecurity principles and guidance
- Key 2017 cybersecurity projects
- Take-away points

# Summary of Where We Are Today

- Focused on protecting the District and our customers from a cyber breach (attack)
- Strong “defense in depth” approach
- Employees are key to our success
- Emphasis on training and doing even more

# Overview

**Our goal:**

Relentlessly protect customers and District assets against cybersecurity risks

**Our reality:**

It’s not easy to do – a simple click on the wrong link can make us vulnerable

# Our Approach

- Defense in depth
  - Deploy many techniques simultaneously
- Active in industry groups
  - Gain knowledge of current best practices
- Trained users
  - Employee cyber awareness training

# Categories of Focus

1. Protecting:

- Control systems for reliability
- Business systems to ensure ability to operate
- Customer and employee data against compromise

2. Employing industry guidance to advance our abilities

# Industry Principles

1. Executive management must champion cybersecurity efforts
2. Cybersecurity programs and policies need to be documented and maintained
3. Enterprise, not just departmental, cybersecurity programs are essential
4. Have a plan to respond to cybersecurity incidents before they happen

# Industry Principles

5. Communicate policies and risks to Board and executive management
6. Develop and maintain an effective cybersecurity staff
7. Build public-private partnerships for information sharing

# Industry Principles

8. Implement a cybersecurity awareness, communication and education strategy
9. Use external resources to periodically assess the cybersecurity program and risks
10. Develop and maintain secure systems & design processes

# Additional Industry Guidance

- North American Electric Reliability Corporation (NERC) Standards
  - Critical Infrastructure Protection (CIP) Standards
  - Cybersecurity requirements for the District's critical infrastructure
  - Physical security for the District's critical infrastructure
- 20 Critical Security Controls
  - Threat based methodology developed by industry and government consortium

# Examples of How We Apply the Principles and Guidance

- General Manager “All Employee” communication emphasizing importance and every employee’s responsibility for cybersecurity
- Employee awareness training and phishing exercises
- Separation of business and operations systems – “air gap”
- Insurance protection against loss of customer information

# Examples of How We Apply the Principles and Guidance

- Compliance program for NERC and CIP cybersecurity standards
- Eight District-wide policies that include cybersecurity requirements
- Established authority for IT Manager to shut down system if there is a sign of attack
- Cross-functional cybersecurity working group meets monthly

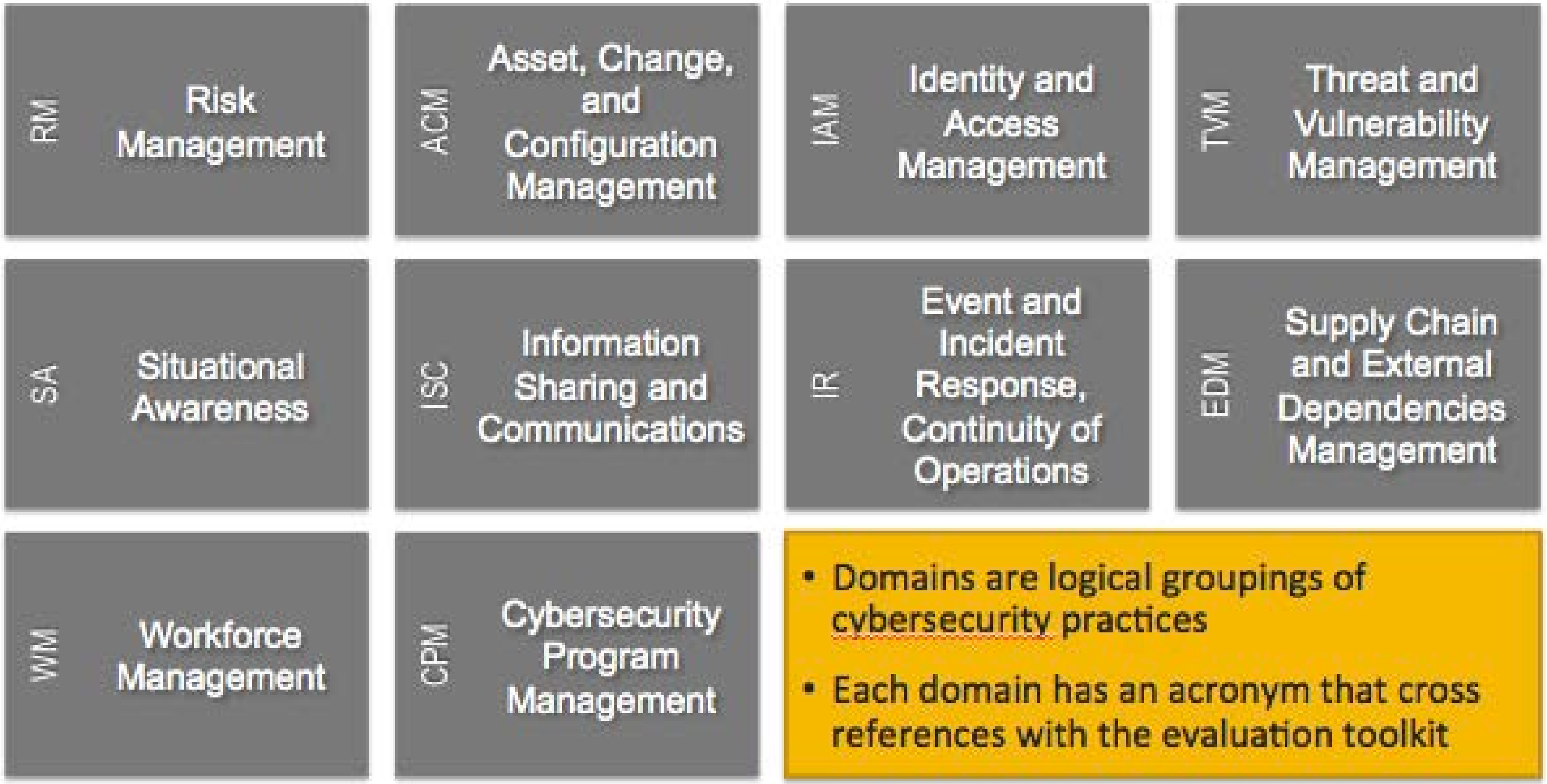
# Examples of How We Apply the Principles and Guidance

- Created industry expertise connections with Pacific Northwest National Laboratory (PNNL) and Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Conduct independent penetration testing
- Protect customer and employee data through encryption, “Red Flags” Committee, specific policies, etc.

# Key 2017 Project

- **Cybersecurity capability maturity model (C2M2)**
  - – Department of Energy sponsored program specific to the utility industry
  - – Pacific Northwest National Laboratories (PNNL) to assist in training and assessment
  - – Evaluation may identify future staffing and technology requirements

# C2M2



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 and Incident Response, Continuity of Operations

EDM Supply Chain and External Dependencies Management

WM Workforce Management

CPM Cybersecurity Program Management

- Domains are logical groupings of cybersecurity practices
- Each domain has an acronym that cross references with the evaluation toolkit

# Anticipated Areas for Maturity

## Internet traffic analysis tool

- Pilot study
- Automated collection and analysis of the District’s ***outgoing*** internet perimeter traffic
- 24x7 security event analysis & notifications

# Anticipated Areas for Maturity

## Network security response simulation

- Conduct with the Washington State Military Department (National Guard)
- District team will work to contain “attack”
- Debrief conducted with National Guard personnel to enhance District cyber resilience

# Take-Away Points

- Focused on protecting the District and our customers from a cyber attack
- Strong “defense in depth” approach
- Employees are key to our success
- Emphasis on training and doing even more
- Formal risk-based approach for 2017

## Questions?