USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

HOW TO DEVELOP AN INCIDENT RESPONSE PLAN

Michael Martin
Chelan County Public Utility District

CHELAN COUNTY PUBLIC UTILITY DISTRICT

ROCKY REACH DAM

5 MILLION megawatt hours generated in 2023
11 generators
2022 production cost $13.4/MWh

ROCK ISLAND DAM

2.1 MILLION megawatt hours generated in 2023
2 powerhouses – 19 generators
2022 production cost $34.4/MWh

LAKE CHELAN DAM

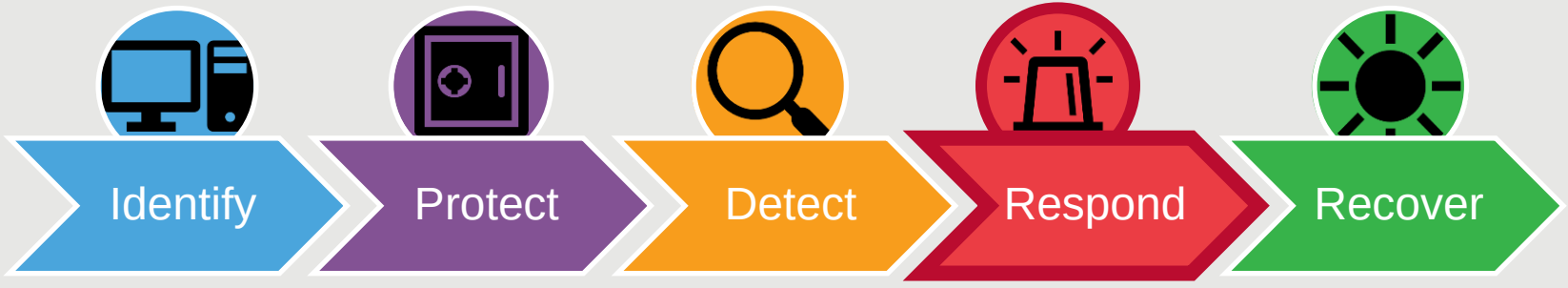
0.3 MILLION megawatt hours generated in 2023
2 generators
2022 production cost $19.5/MWh

USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

P.U.D. CHELAN COUNTY

NIST Cybersecurity Framework: RESPOND

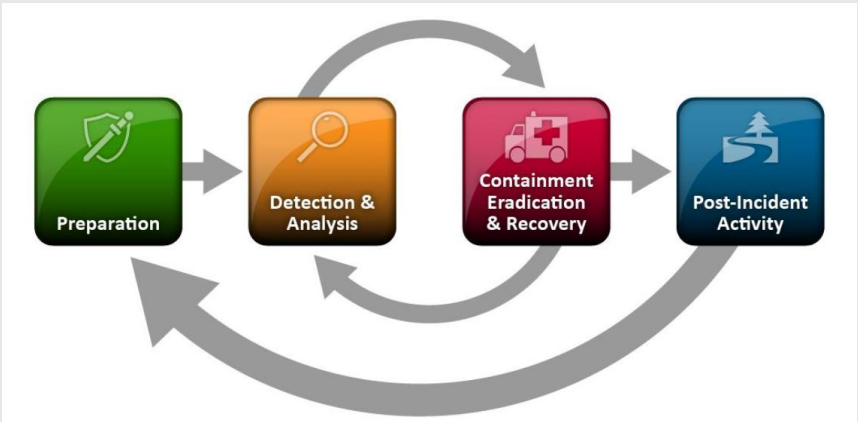


Example Outcomes:

- Ensuring response planning processes are executed during and after an incident
- Managing communications during and after an event
- Analyzing effectiveness of response activities

OUR INCIDENT RESPONSE PLAN JOURNEY

- Overhauled incident response plan in 2016 to comply with U.S. North American Electric Reliability Corp. (NERC) Critical Infrastructure Protection (CIP) version 5 regulations
- Adopted the NIST Model
- Referenced documents to develop plan:
  - *Computer Security Incident Handling Guide*, NIST Special Publication 800-61 Revision 2 (2012)
  - *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, Department of Homeland Security (2009)



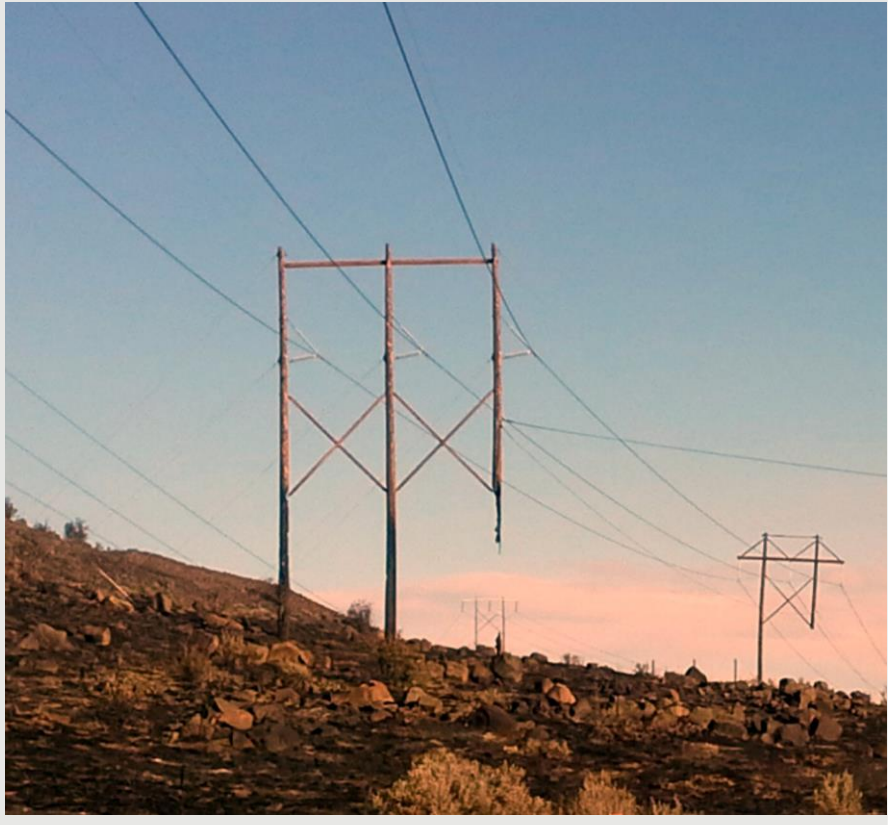
Source: U.S. National Institute of Standards and Technology (NIST)

PREPARATION: Identifying Critical Utility Assets

- All U.S. power utilities apply NERC Critical Infrastructure Protection (CIP) industry-standard classification criteria to identify critical and supporting systems with *high*, *medium*, *low*, or *no impact* to the greater interconnected power grid

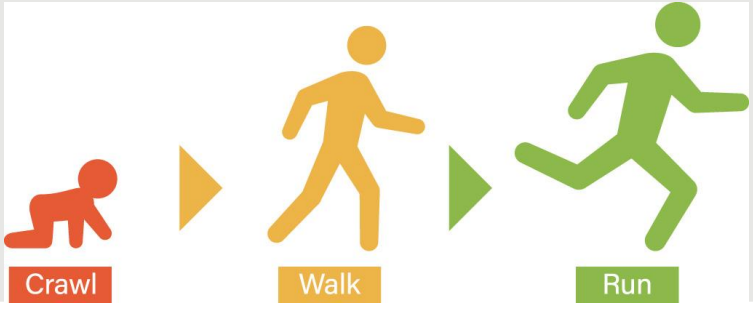
- Based on their impact, systems are protected by physical and cybersecurity controls to mitigate their risks

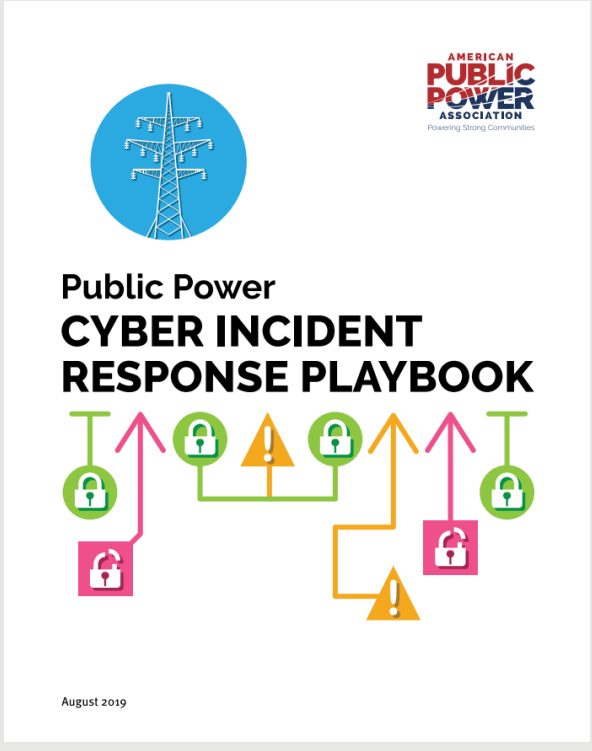
- Chelan uses **business impact risk assessment** to identify additional mitigations for these systems (such as insurance, support agreements, spare inventory, preventative maintenance, etc.)



WRITING YOUR INCIDENT RESPONSE PLAN

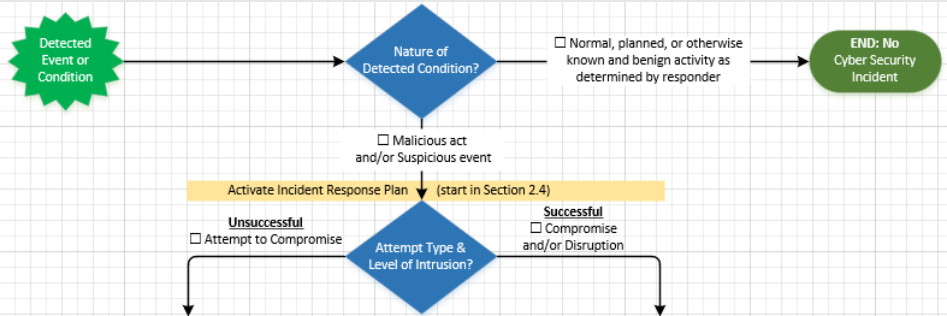
- Follow the *Public Power Cyber Incident Response Playbook* (2019) and its "Top 10 Steps to Develop a Cyber Incident Response Plan"
  - Helped our IT department develop its incident response plan
  - "Right size" your plan to your organization's size and resources
- Put together a plan
  - It won't be perfect and doesn't need to be

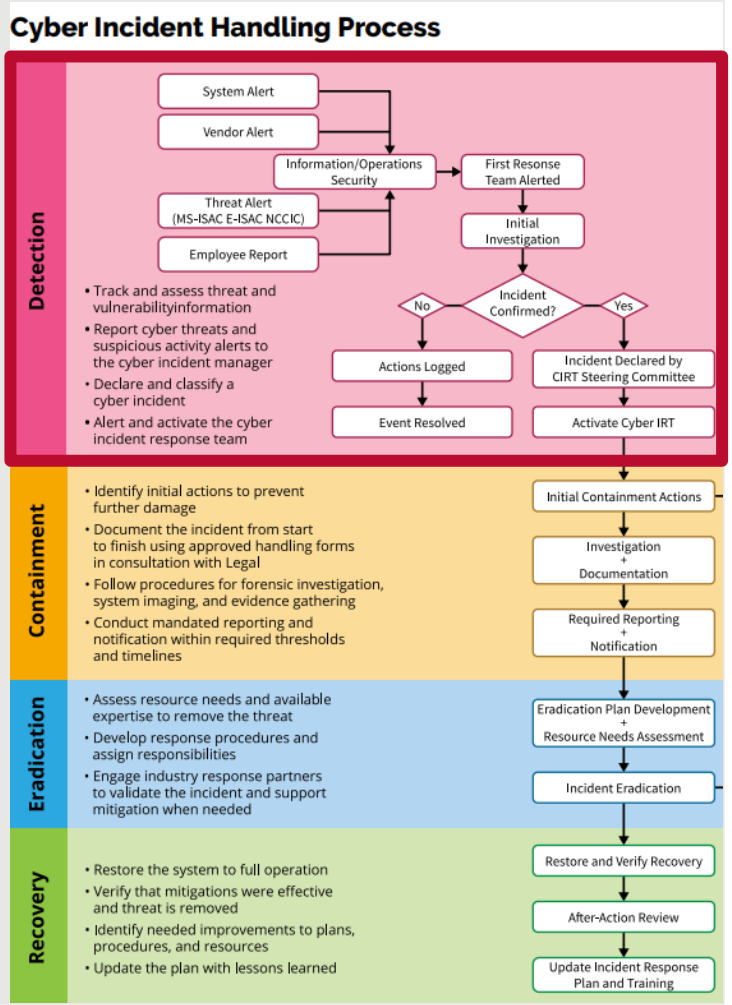




Cybersecurity Incident Response Plan
KEY ELEMENTS

- **Roles and responsibilities** – who does what
- **Detection** – distinguish incident from normal events
  - NERC: "malicious act or suspicious event"
  - Operators: NERC *Cyber Intrusion Guide for System Operators*
  - System Admins: NIST *Guide to Industrial Control Systems (ICS) Security*

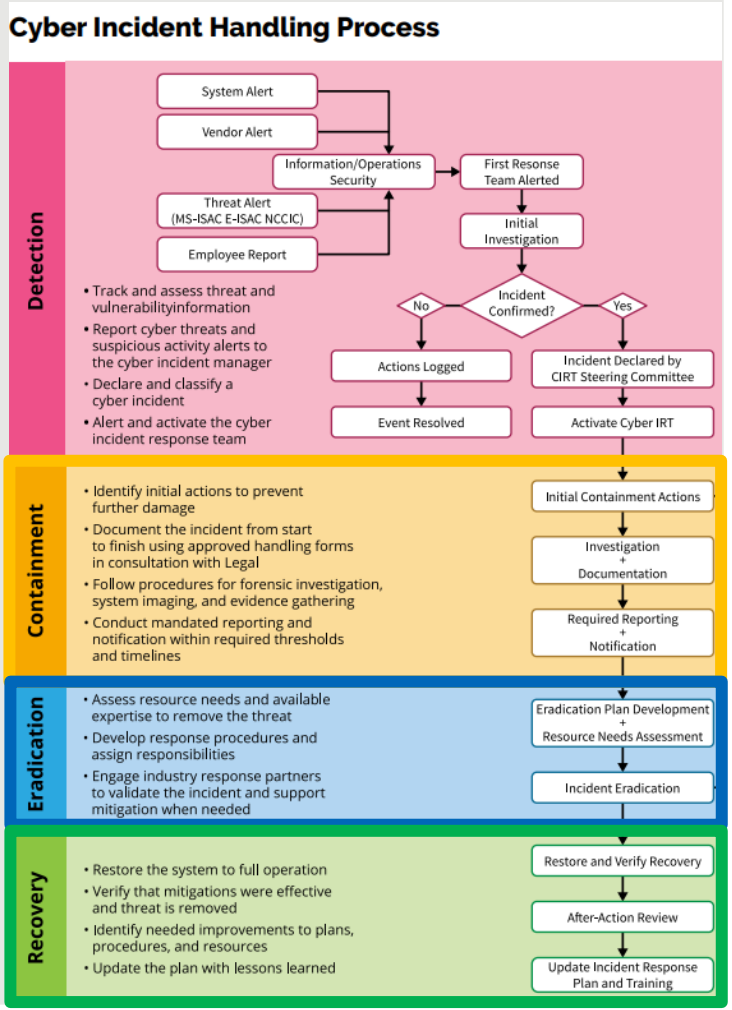




Source: Public Power Cyber Incident Response Playbook

Cybersecurity Incident Response Plan
KEY ELEMENTS

- **Containment** – prevent further damage
  - Document potential containment actions for common incident types that might be overlooked during the frenzy of an incident
- **Eradication** – remove the threat
- **Recovery** – restore the system to full operation
  - Spare hardware for computers, HMIs, PLCs, RTUs, switches, etc. (in case of supply chain delays)
  - Practice operational recoveries of different system types (HMI, firewall, switch, etc.)



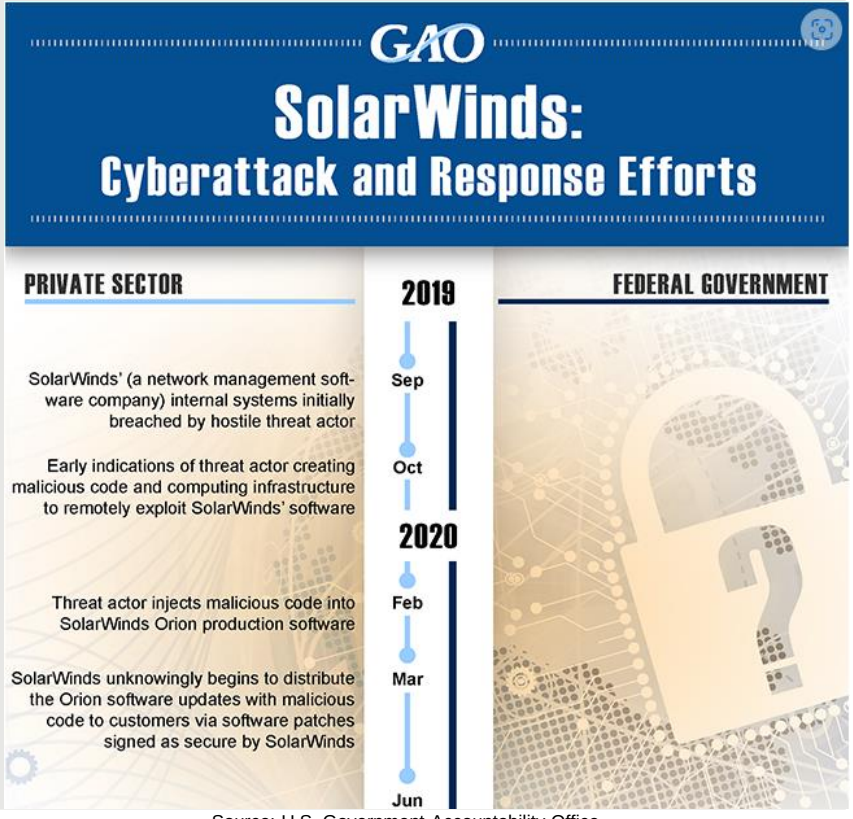
Source: Public Power Cyber Incident Response Playbook

Cybersecurity Incident Response Plan
KEY ELEMENTS

- **Communication plans**
  - Methods – cell phones, Slack, Teams, WhatsApp, Zoom, etc.
  - Technical response teams
  - Communication between groups or departments
  - External communications – law enforcement, public, partners, neighboring utilities

EXERCISE YOUR INCIDENT RESPONSE PLAN

- Practice the plan with a tabletop drill
  - Once a year seems reasonable
- Consider testing recent scenarios in the news
  - Supply chain watering hole attack
  - Insider threat: Stolen two-factor fob and USB key logger enables unauthorized computer use
  - Ransomware
- USE the plan during the exercise
- Train responders



Source: U.S. Government Accountability Office

Cybersecurity Incident Response Plan
LESSONS LEARNED MEETING

After testing your plan, hold a lessons learned meeting to improve the process and be better prepared for future incidents.

- How well did we perform?
- What information was needed sooner?
- What should we do differently next time?
- How could information sharing be improved?
- Can corrective actions be implemented?
- Did any steps inhibit recovery?
- Are additional tools or resources needed?
- Could this incident have been prevented?

Cybersecurity Incident Response Plan
LESSONS LEARNED FEEDBACK

- Plan was too long
  - Users wanted shorter plan or decision tree/checklist
- Communication plan didn't reflect reality
  - In early tests with just a few departments, participants met in a conference room to discuss scenarios
  - Later exercises (like nationwide GridEx) involved more departments, and participants worked at their desks to simulate a real event—identifying many communication challenges

Cybersecurity Incident Response Plan
LESSONS LEARNED IMPROVEMENTS

- Application architecture improvements
- Additional security cameras
- Penetration tests of specific networks
- Enhanced event notifications (e.g., after-hours alerts)
- Tools – network monitoring solution to store packet data for operational troubleshooting and forensic analysis

Cybersecurity Incident Response Plan
SUGGESTIONS

- Print response plans and related information (contact list, vendor information)
- Put the plan revision date in a header/footer on each page to identify the current version
- Establish delegates or backups for each role, so incident response isn't slowed when someone is not available
- Empower people to make decisions to facilitate efficient response (e.g., can a manager make the decision instead of a director?)
- Document incident response resources in your plan (contracted incident response service, government resources, insurance, etc.)

RESOURCES

- Public Power Cyber Incident Response Playbook (2019)
- NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide (2012)
- NIST SP 800-82 Revision 3, Guide to Operational Technology (OT) Security (2023)
- NIST SP 800-83 Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops (2013)
- NERC Cyber Intrusion Guide for System Operators (2023)
- CISA #StopRansomware Guide (2023)

Michael Martin
CIP Standard Owner and Control Systems Engineer
Chelan County Public Utility District