Ransomware and Today's Electric Grid

Tami Reynolds, NREL Cybersecurity Project Manager & Lead

CARILEC CEO's & Leadership Conference

May 2022

Photo from iStock-627281636

Presenter:

- National Renewable Energy Laboratory under the United States Department of Energy (DOE)
- 7 years cybersecurity research in the electric sector
- Expertise in cyber governance best practices, cybersecurity risk management, evaluation tools
- Technical lead on the Distributed Energy Resources Cybersecurity Framework (DER-CF)
- Conducts cyber-governance assessments in the electric utility sector based on DOE's C2M2 and the NIST Cybersecurity Framework

The USAID-NREL Partnership

USAID and NREL partner to deliver clean, reliable, and affordable power to the developing world. The USAID-NREL Partnership addresses critical aspects of deploying advanced energy systems in developing countries through:

- Policy, planning, and deployment support
- Global technical toolkits.

The Resilient Energy Platform provides expertly curated resources, training materials, tools, and technical assistance to enhance power sector resilience.

https://resilient-energy.org/cyber

The Cybersecurity Building Blocks are a starting point for utilities to promote a more rounded approach to cybersecurity for critical infrastructure.

https://resilient-energy.org/cybersecurity-resilience/building-blocks

iStock 022317350

What is Ransomware?

Ransomware is a type of malware that encrypts files on a device, rendering files unusable unless a ransom is paid.

Examples of a Ransomware Attack

January 2017: Guyana Water Incorporated disclosed that Information and Communication Technology (ICT) personnel found malware that compromised billing and collections for several days.

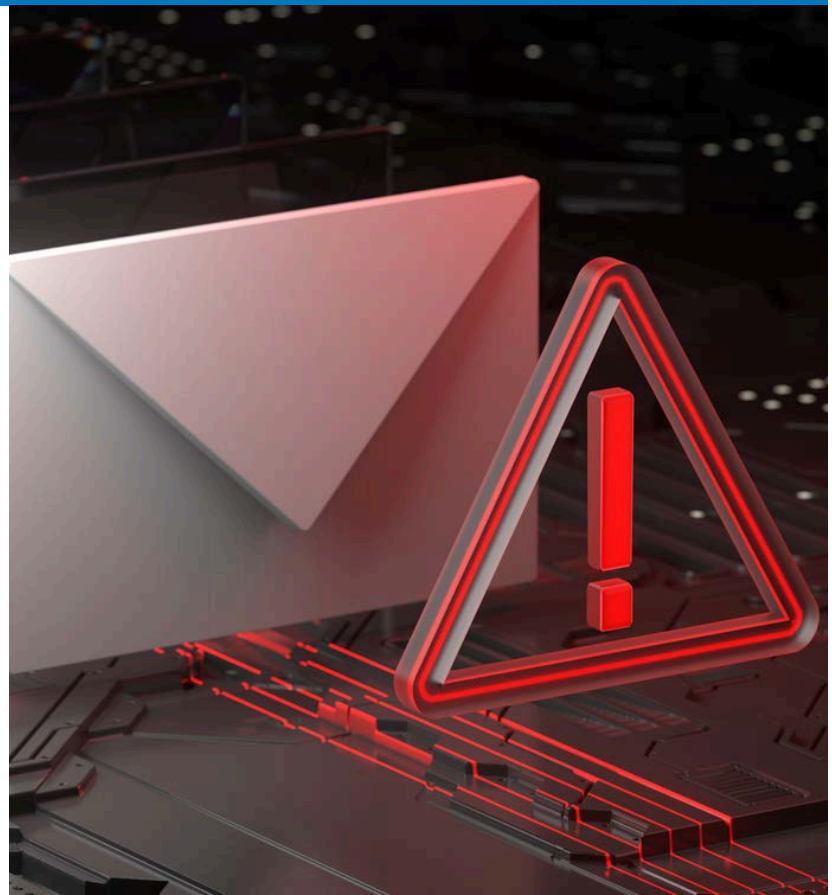
February 2019: Guyana Power and Light Inc. was able to quarantine an attack and did not pay the bitcoin ransom requested. The central offices were disrupted but customer services were maintained.

May 2021: Hackers breached the U.S. Colonial Pipeline with a compromised password, demanding ransom for $4.4 million and disrupting the delivery of fuel to much of the Southeastern United States. The Department of Justice recovered $2.3 million of what was paid.

Cars line up for gas during the Colonial Pipeline attack (iStock 1317620668)

How Ransomware Works

1. Attackers infect your system.
2. Receive a message saying your data is locked.
3. Attackers provide payment instructions.
4. Victim pays ransom and *may* receive decryption instructions.



iStock 1323226102

Defenses Against Ransomware

General cybersecurity best practices are the best defense against ransomware:

- Data backups
- Comprehensive incident response plan
- Strong network defenses
- Email scanning
- Workforce training

No one delivery system for ransomware

No one defense

Preparing for Ransomware

Back up Your Data

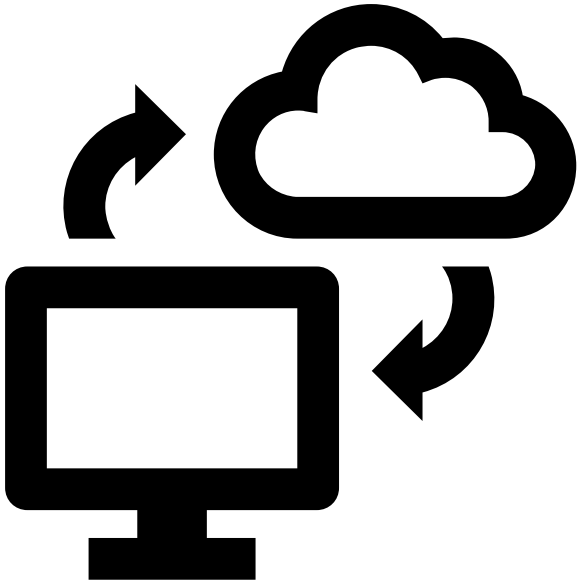
- Determine how often you should back up all your data.
- Determine where to store your backed up data.

Have an Incident Response Plan

- A plan that is well understood and comprehensive will allow staff to react quickly and minimize the impact.

Segment Your Network

- Limits how far an attack could spread



Ransomware isn't going away…

- **Critical infrastructure** services such as energy, hospitals, and food supply chains are a popular target.
- At least **140 ransomware strains** collected payments at in 2021, compared to 119 in 2020, and 79 in 2019.
- Average **payment size was over $118,000** in 2021, up from $88,000 in 2020 and $25,000 in 2019.
- By 2031 a ransomware attack will **take place every 2 seconds,** up from every 14 seconds in 2019, estimates the firm Cybersecurity Ventures.

But there are precautions you can take, with benefits beyond being prepared for ransomware:

- Better backups in the event of system failures and natural disasters
- Better overall cybersecurity protection

Sources: https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware (Feb. 2022)
https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025 (Dec. 2021)
https://www.securityweek.com/securityweek-cyber-insights-2022-ransomware (Jan 2022)

Cybersecurity Governance

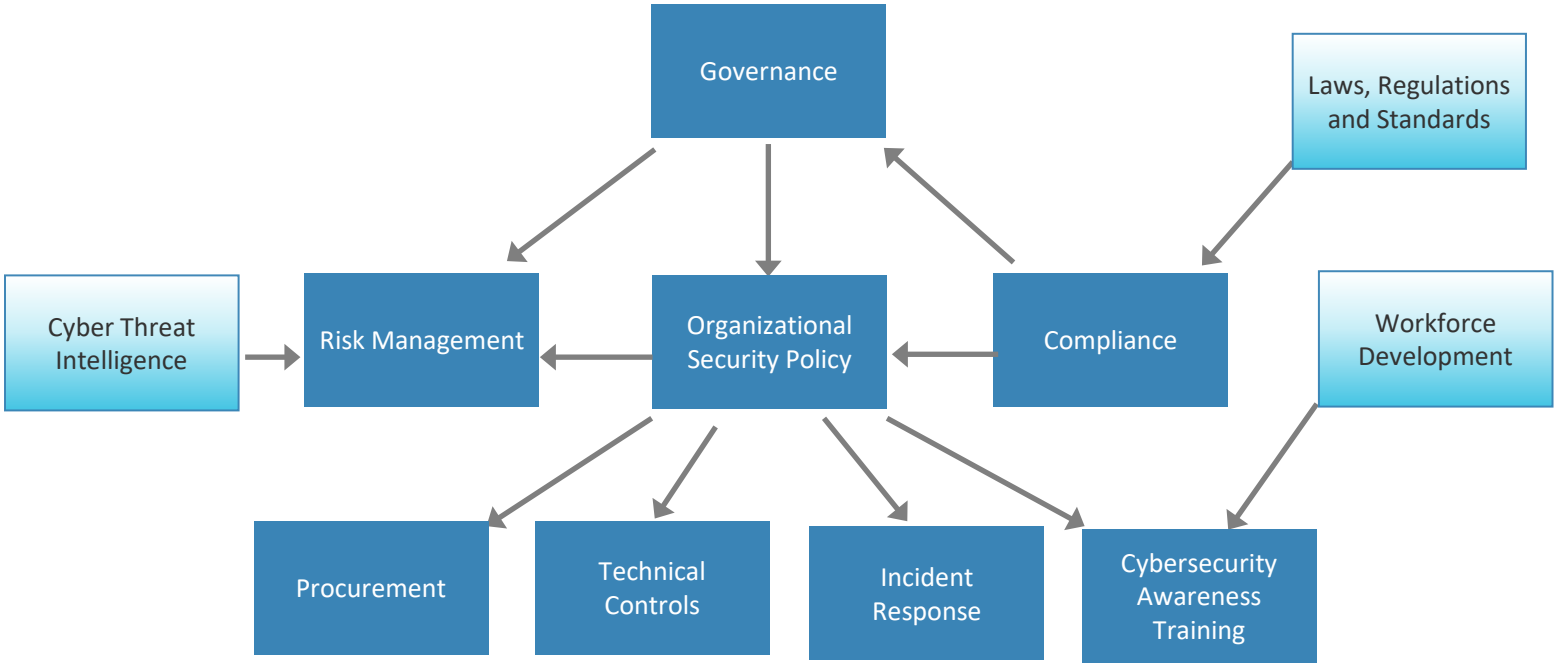
"The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk."

NIST *Framework for Improving Critical Infrastructure Cybersecurity*

Importance of Cybersecurity Governance

- Cybersecurity governance helps an organization detect, prevent, and respond to cyber incidents and mitigate risks.
- Proper governance reduces potentially costly risk exposure, provides a basis for informed decisions, and furnishes a comprehensive yet flexible framework for planning.
- It has been recognized by the U.S. Department of Homeland Security as a crucial component in protecting critical infrastructure.

Project Spotlight: The Power Sector Cybersecurity Building Blocks



The Power Sector Cybersecurity Building Blocks, developed through the U.S. Agency for International Development (USAID)-National Renewable Energy Laboratory (NREL) Partnership and the Partnership's Resilient Energy Platform, are **designed to help a variety of stakeholders improve security for the electrical grid.**

Getting Started

ISTOCK I 183325843

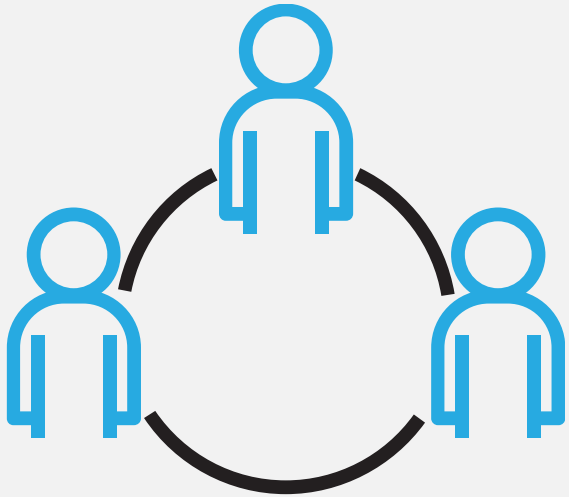
Review Your Organizational Security Policy:

- What is an organizational security policy and why is it important to have one?
  - *Who needs access to it?*
  - *What are your organization's executive directives on cybersecurity?*
  - *What is the specific guidance on implementing directives?*

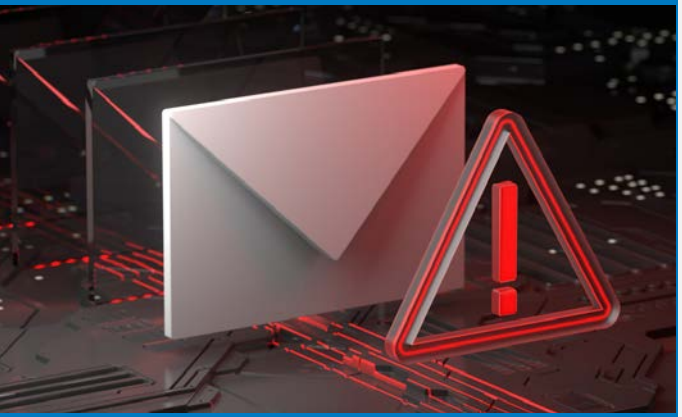
Assign Roles and Responsibilities

Resource Allocation

- Divide your cyber program into clusters of related activities
- Meet with stakeholders to discuss
  - Who has the skills to execute those activities?
  - Who has the bandwidth?



Educate on Cyber Responsibility



Does your staff understand why cybersecurity is important?

Do they understand their role in it?

"Human error" causes of a cyber breach:

- Opening an infected email attachment
- Visiting a malicious web site
- Connecting to an unsecure Wi-Fi network
- Plugging in an infected USB device
- Use of ineffective passwords
- Allowing others to use device

"25% [of cyberattacks] were due to negligent employees or contractors"

-- Ponemon Institute, 2017

iStock 1323226102

Create a Culture of Cybersecurity

- Provide regular training for all staff
- Communicate: Presentations, newsletters, internal marketing, etc.
- Lead by example
- Track (and celebrate!) successes
- Ensure staff feel safe reporting cyber incidents
- Provide incentives

Message:
***Everyone* has a role to play in cybersecurity.**

iStock 1320920010

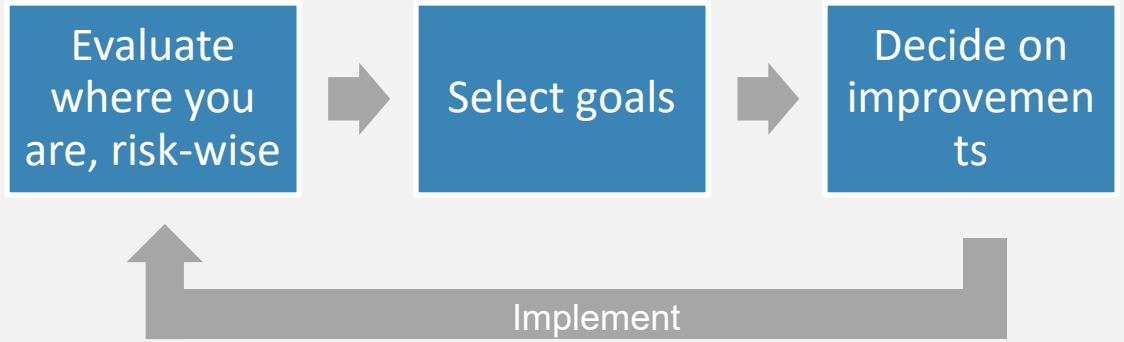
Track Metrics & Indicators

Monitor Progress of the Cybersecurity Program

The bad news: Nobody is 100% cybersecure.

The good news: If you're always improving your game, you just might stay ahead of the bad guys.

Strive for "continuous improvement"

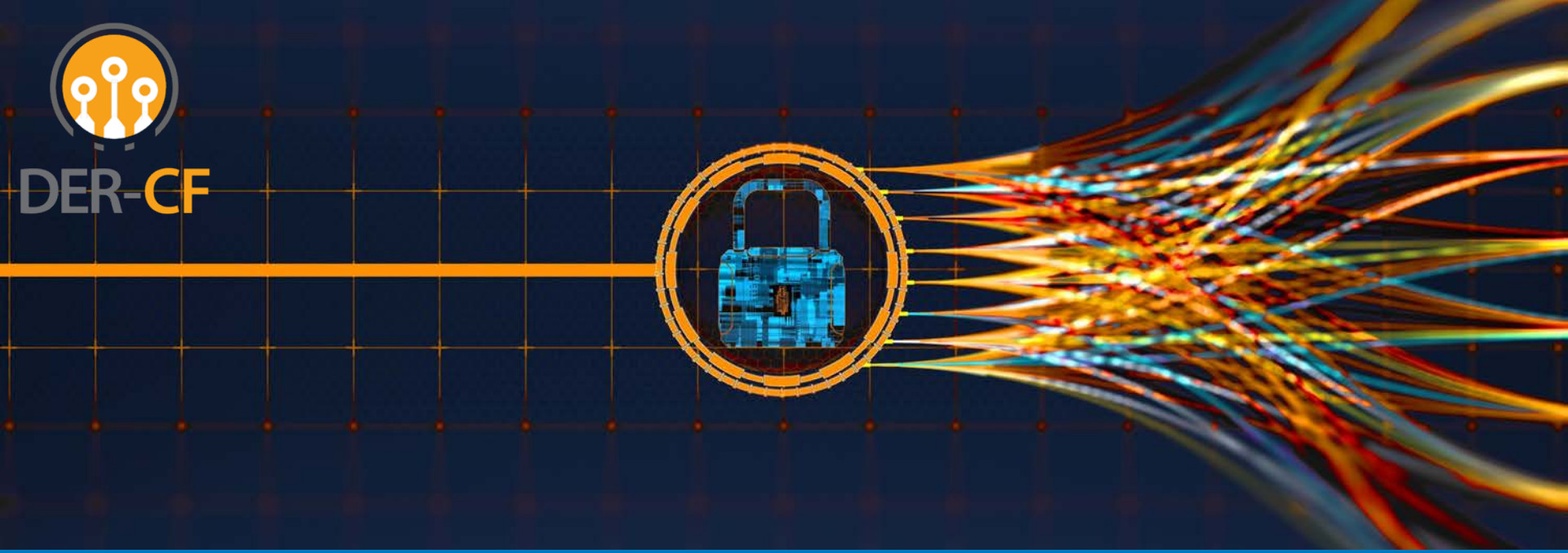


Or as W. Edwards Deming would say: "check, act, plan, do"

How to monitor improvement?

Perform regular cybersecurity assessments

- **Choose an assessment platform**
  - Self-assessment
  - Third-party
- **First assessment establishes a baseline**
  - Provides insight on areas that need immediate attention
  - Gives executive management key focus areas where to invest time and resources
- **Follow-up with reassessments and track progress**
  - Allows for comparative analysis



The Distributed Energy Resource Cybersecurity Framework (DER-CF) was developed to help federal agencies mitigate gaps in their cybersecurity posture for distributed energy systems.

Cybersecurity for Distributed Energy Resources

Modern energy systems are increasingly reliant on smaller decentralized generation sources, i.e., **distributed energy resources (DERs)** such as solar, wind, and storage.

iStock 1181551812

- DERs are equipped with complex, data-driven communications networks to connect with the energy grid.
- This growing number of smart devices that support DERs can increase the number of access points outside a utility's administrative domain, which can increase the potential for cyberattack.

Cyber Governance Security Assessment

Domains

- Risk Management
- Asset, Change, and Configuration
- Identity and Access Management
- Threat and Vulnerability Management
- Situational Awareness
- Information Sharing and Communication Management
- Incident Response
- External Dependency Management
- Cybersecurity Program Management

Cyber-Physical Technical Management Security Assessment

Domains

- Account Management
  - Authentication, authorization, and accounting
  - Role-based access control
  - Remote access
  - Monitoring and logging
- Configuration Management
  - Change management
  - Access control
  - System settings
  - Cloud security
- Systems/Device Management
  - Software integrity
  - Cryptography
  - System protections

Physical Security Assessment

Domains

- Administration Controls
  - Audits
  - Awareness training
  - System security testing
  - Operational management
  - Security plan
  - Secure data
- Physical Access Controls
  - Perimeter security
  - Building security
  - Lighting
  - Signage
  - Intrusion alarm/motion detector
- Technical Controls
  - Intrusion Detection/prevention assets
  - Smart card/keying/badges
  - Sensor system/proximity reader/radio-frequency identification
  - Communication system
  - Closed-circuit television

DER-CF Tool: Overview

- Publicly available interactive version of the DER-CF framework
- User-focused assessment
- Detailed results and action items
- Userbase: Site operations, energy managers, executive managers
- Tailored assessment to individual site

Hosted by NREL at www.dercf.nrel.gov

Unique from Any Other Assessment Tool

The tool expands to DERs, specifically:

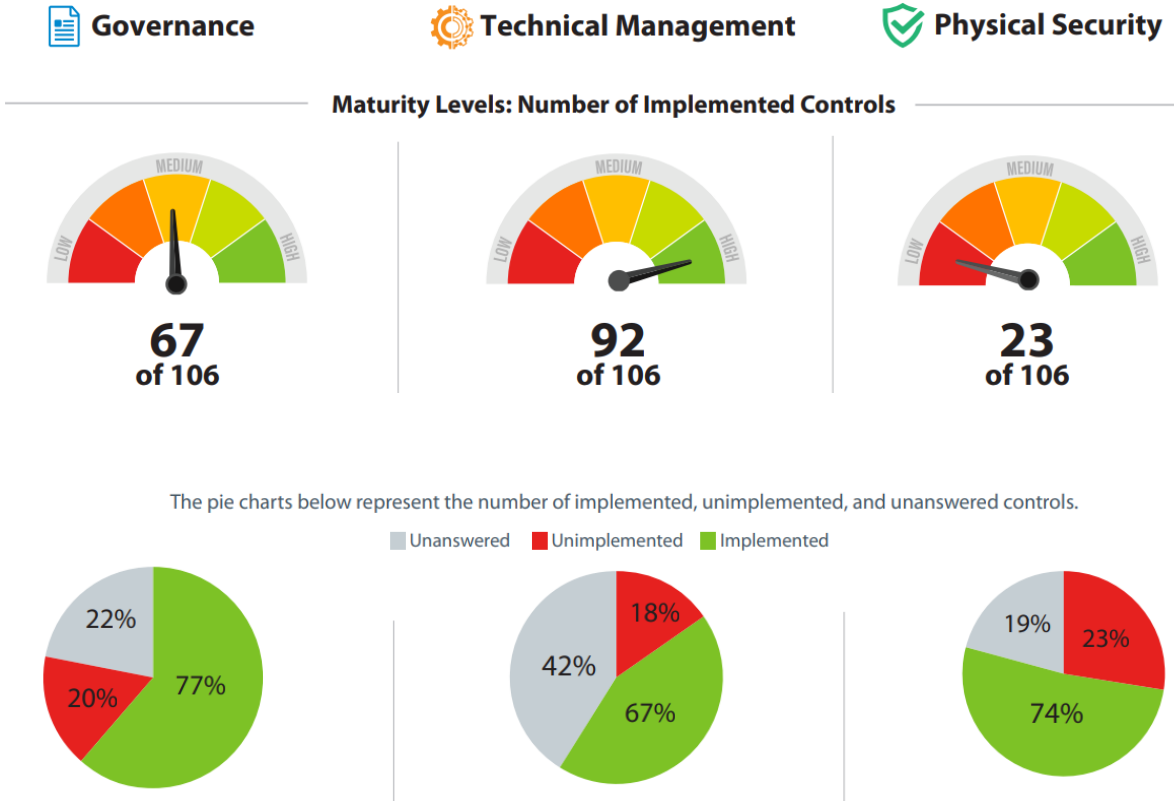
- Solar
- Wind
- Electric vehicles (charging stations)
- Buildings
- Storage

The DER-CF uses the following standards and/or frameworks:

- DOE Cyber Security Capability Maturity Model (C2M2)
- NIST 800-53, 800-30,800-82, CSF
- DHS Cyber Assessments of ICS
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- International Electrotechnical Commission (IEC) 62351
- Executive Order 13800

Other Unique Features

- Dynamic content-driven approach
- Internal-facing application to aid researchers based on user behavior
- User experience focused application, encourages re-use
- Data secured to meet FIPS-199 medium standards



Summary

- Utilities are a target of ransomware attacks and must plan accordingly.
- General cybersecurity best practices are the best defense against ransomware.
- Back up data and know how to pay the ransom in cryptocurrency, if needed.
- Cybersecurity governance helps an organization detect, prevent, and respond to cyber incidents and mitigate risks.
- Effective cybersecurity policies require participation from all team members.
- Tracking metrics and monitoring progress will help you improve your game—and you might just stay ahead of the bad guys.
- Cybersecurity assessments, like NREL's DER-CF, can help you monitor progress and identify gaps in cybersecurity posture.

www.nrel.gov

NREL/PR-5R00-82815

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Federal Energy Management Program. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

NREL
Transforming ENERGY