Photo from iStock-627281636

Cybersecurity Governance

Tami Reynolds, NREL Cybersecurity Project Manager & Lead

CARILEC CEO’s & Leadership Conference

May 2022

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

Examples of Recent Cyber Events

iStock 1317620668

December 2013: Target cyber breach hits 40 million payment cards at holiday peak

December 2015: Hackers compromised information systems of energy distribution companies in Ukraine, shutting off 30 substations and disrupting energy services to 230,000 customers

October 2019: Utah renewable energy developer hit by first-of-its-kind cyberattack

August 2020: Tesla Gigafactory employee reports to FBI of attempted ransomware attack

February 2021: Damage of SolarWinds attack is unveiled, reporting that up to 18,000 customers from federal agencies and private companies installed updates that left organizations vulnerable to hackers

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.

Consequences of a Cyberattack

ISTOCK 1144604245

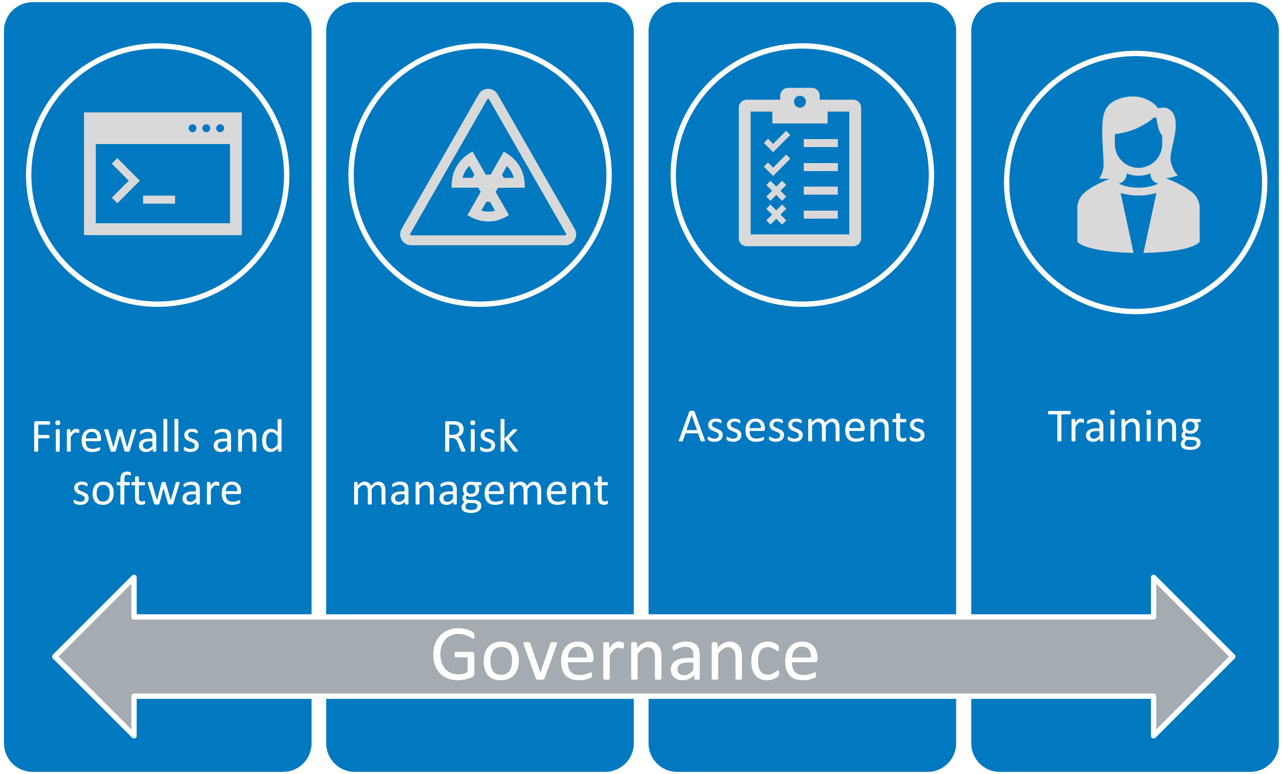
For all businesses:

- Deleted data: cost to restore
- Ransomware: cost to restore…or the ransom
- Theft of sensitive data (customer records, employee records, trade secrets), credit monitoring, fines, loss of revenue
- Reputational damage (consumers, regulators, investors)
- Loss of productivity

For utilities, all the above plus cyber-physical consequences:

- Safety concerns
- Interrupted service
- Damaged or destroyed physical assets and the cost to repair or replace

Common Cybersecurity Practices



Firewalls and software

Risk management

Assessments

Training

Governance

What is 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.”

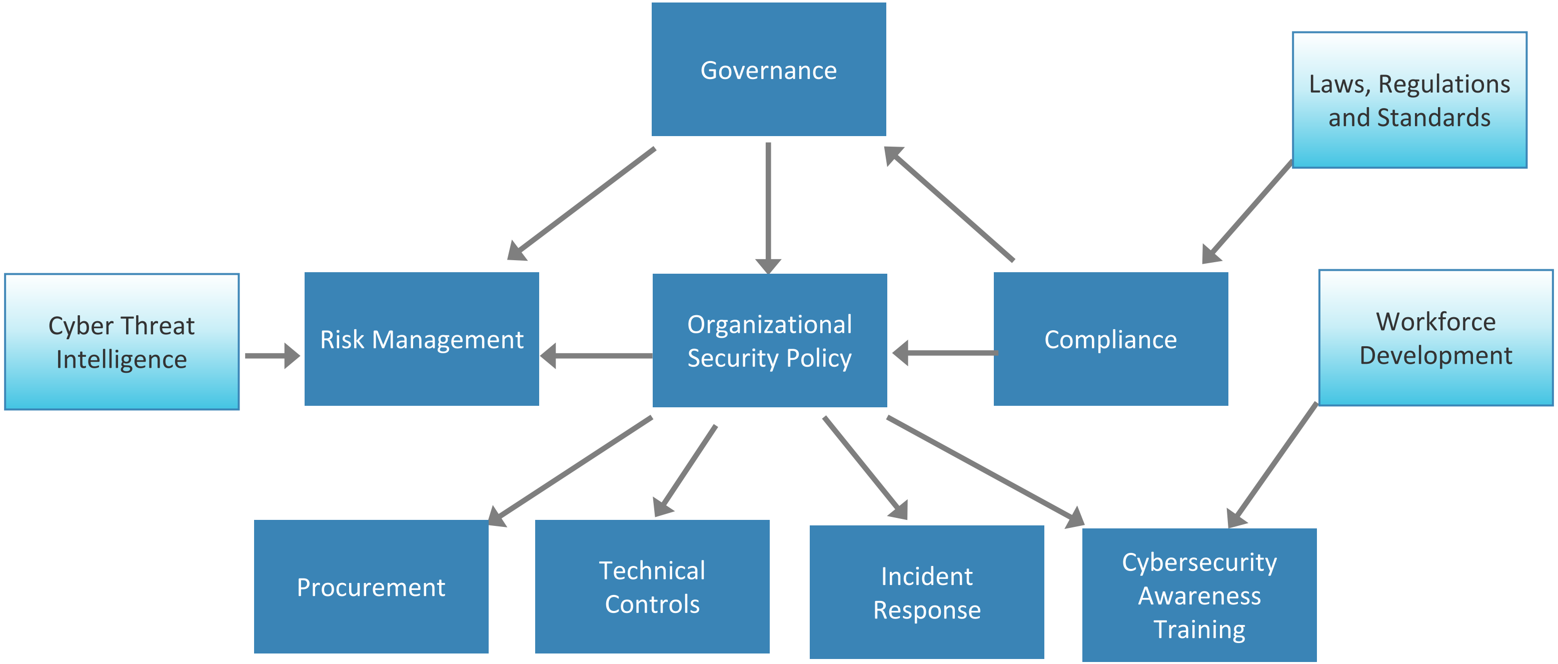
NIST *Framework for Improving Critical Infrastructure Cybersecurity*

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.

iStock 1331137712

Project Spotlight:
The Power Sector Cybersecurity Building Blocks


Governance
Laws, Regulations and Standards
Cyber Threat Intelligence
Risk Management
Organizational Security Policy
Compliance
Workforce Development
Procurement
Technical Controls
Incident Response
Cybersecurity Awareness Training

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.**

Examples of Cybersecurity Governance

- Employee password policies
- Network access controls
- Required cybersecurity training
- Incident response policies
- Threat and vulnerability management
- Supply chain awareness
- Asset management

iStock 000075109659

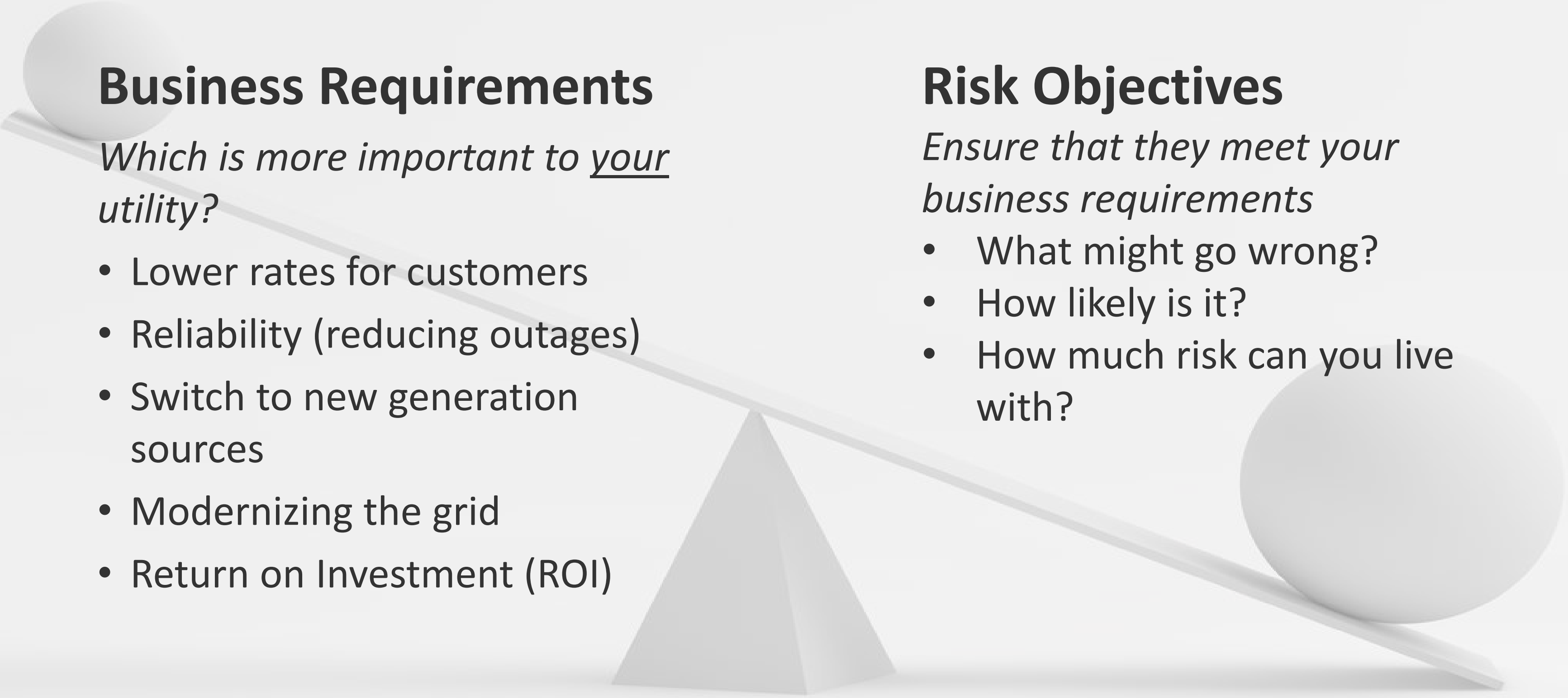
Getting Started

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?*

Prioritize Business Requirements and Risk Objectives



Business Requirements

Which is more important to your utility?

- Lower rates for customers
- Reliability (reducing outages)
- Switch to new generation sources
- Modernizing the grid
- Return on Investment (ROI)

Risk Objectives

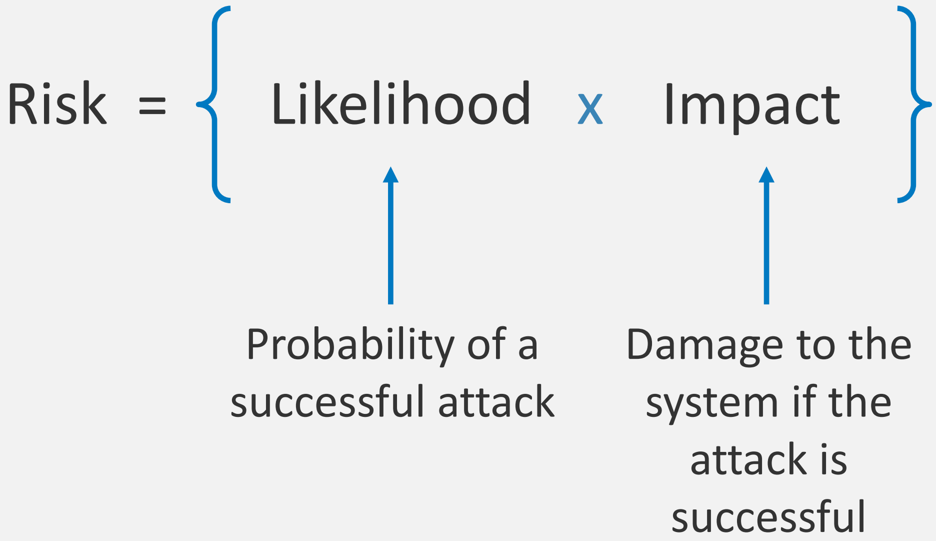
Ensure that they meet your business requirements

- What might go wrong?
- How likely is it?
- How much risk can you live with?

Photo credit to come

Cyber Risk

One definition…



Risk = { Likelihood x Impact }

Probability of a successful attack

Damage to the system if the attack is successful

iStock 1290692464

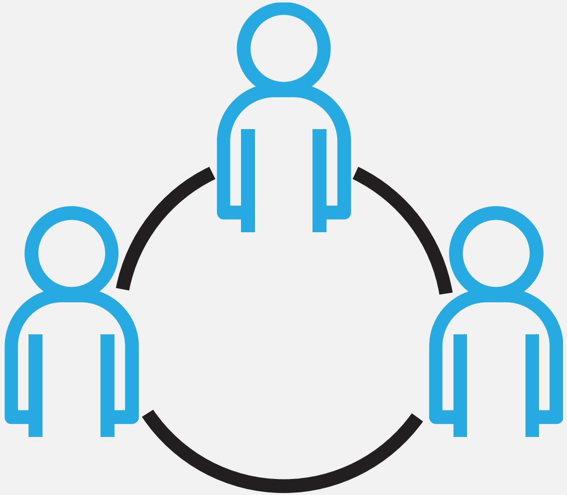
Ensure Participation from All

Although decisions and documentation of procedures are primarily the responsibility of energy systems managers and system administrators, effective implementation of strong cybersecurity policies requires participation **from all team members**, including day-to-day users.

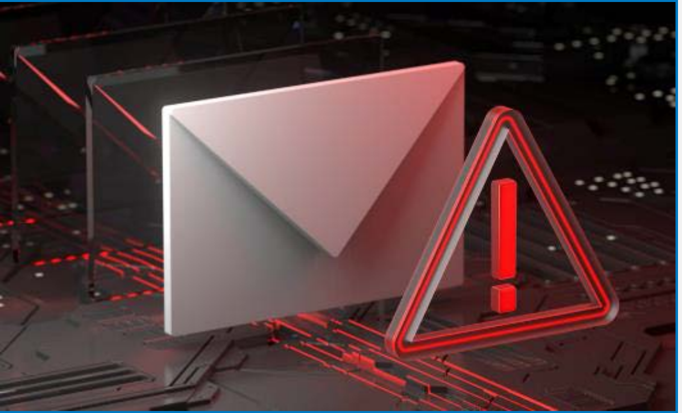
Assign Roles and Responsibilities

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



iStock 1323226102

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

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

Choose your indicators

Measure & analyze

Baseline

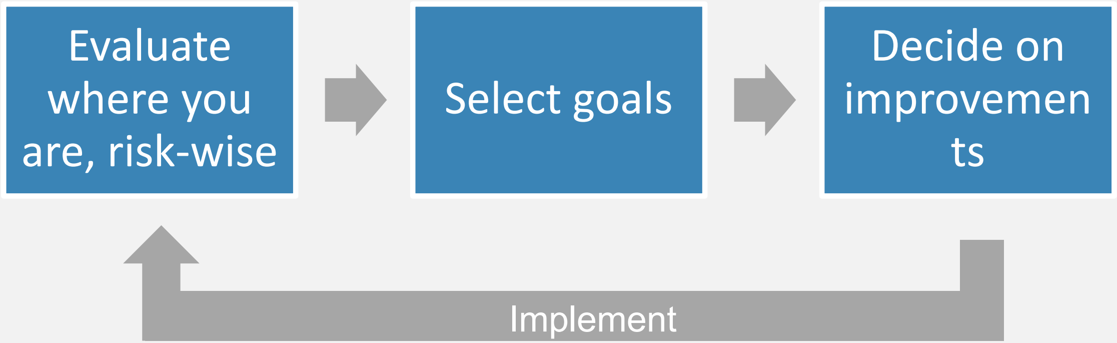
Track over time

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”



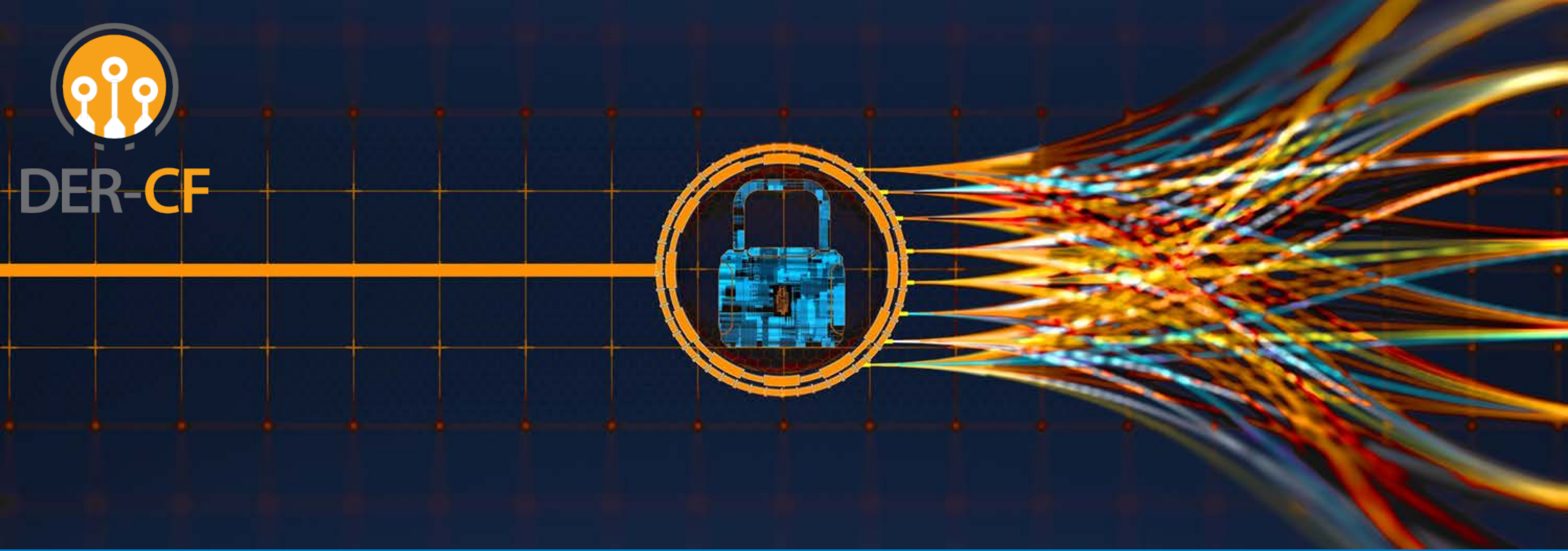
Or as W. Edwards Deming would say: “check, act, plan, do”

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



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

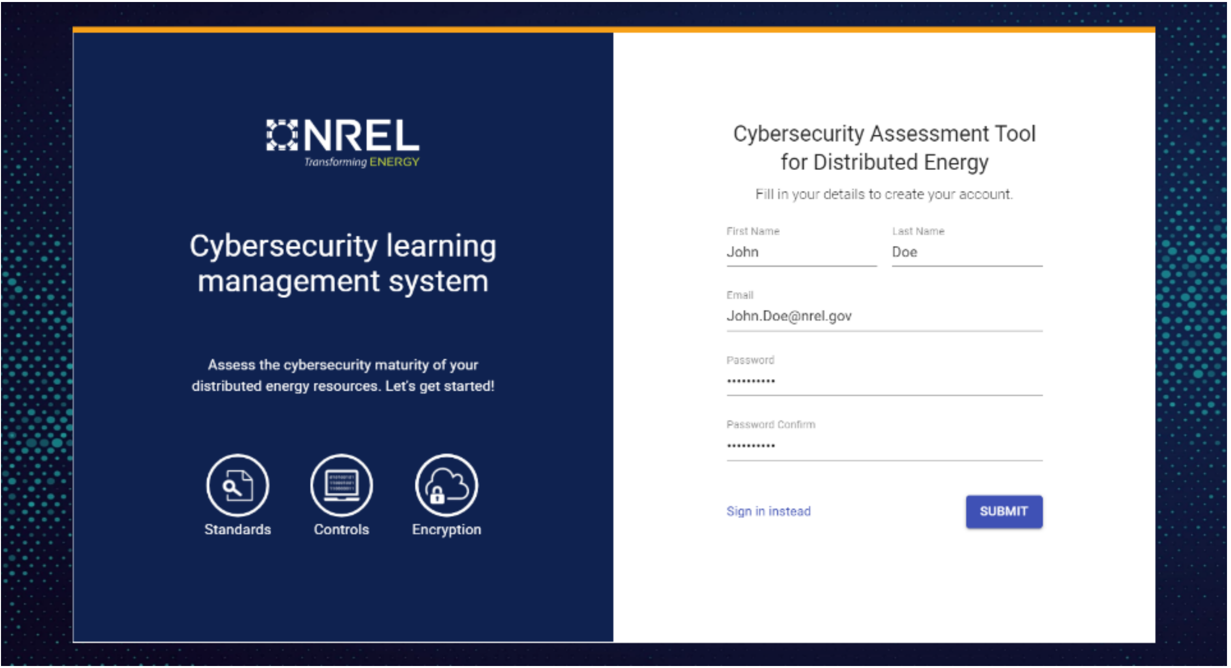
Physical Security Assessment

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



Cybersecurity learning management system

Assess the cybersecurity maturity of your distributed energy resources. Let's get started!

Cybersecurity Assessment Tool for Distributed Energy

Fill in your details to create your account.

First Name: John

Last Name: Doe

Email: John.Doe@nrel.gov

Password: ••••••••••

Password Confirm: ••••••••••

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

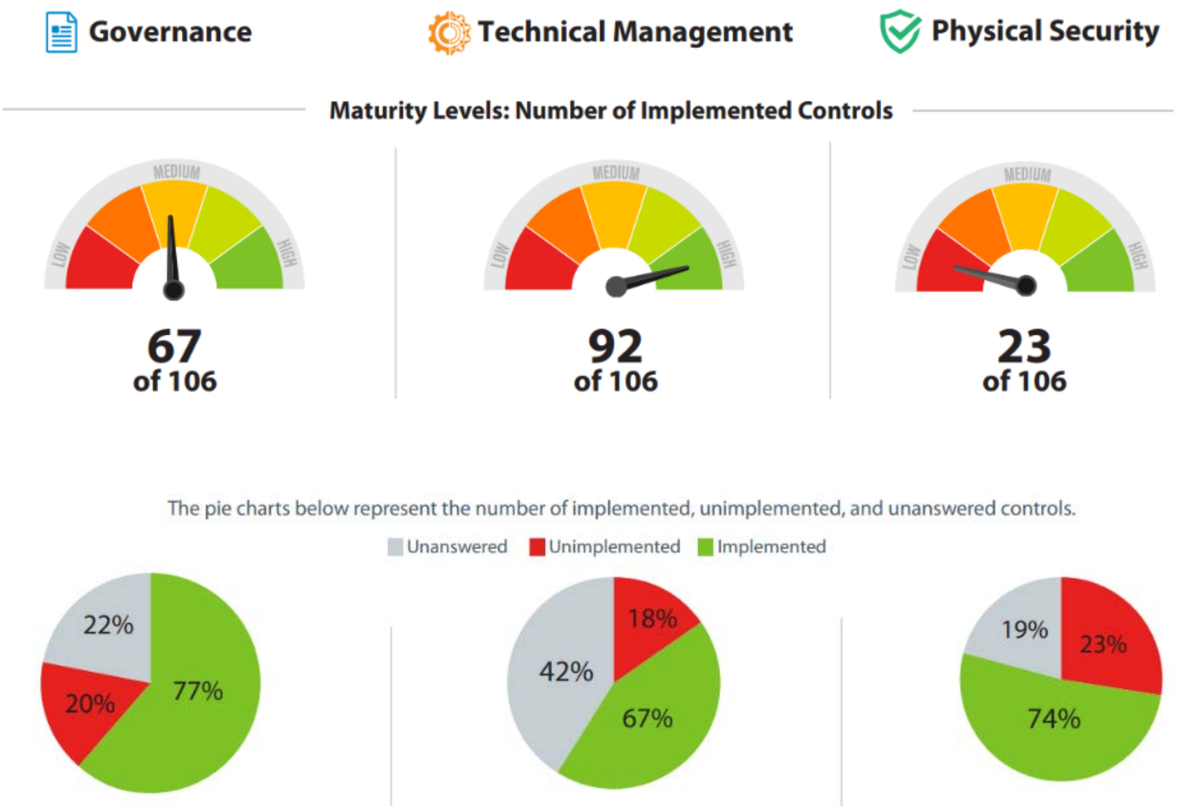
iStock 612623118

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



Maturity Levels: Number of Implemented Controls

The pie charts below represent the number of implemented, unimplemented, and unanswered controls.

Summary

- Utilities are subject to many types of attacks and must plan accordingly.
- Cybersecurity governance helps an organization detect, prevent, and respond to cyber incidents and mitigate risks.
- An organizational security policy is the “go-to” document for a utility’s cybersecurity program.
- Effective implementation of strong cybersecurity policies requires participation from all team members, including day-day users.
- 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.

Q&A

Tami.Reynolds@nrel.gov

www.nrel.gov

NREL/PR-5R00-82814

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