RESOURCE CENTER

Enhancing power grid security: Meeting NERC CIP requirements with Bitwarden

Get the full interactive view at https://bitwarden.com/es-la/resources/enhancing-power-grid-security-meeting-nerc-cip-requirements-with-bitwarden/

bitwarden

Overview

The North American Electric Reliability Corporation (NERC) is a non-profit international regulatory body dedicated to setting compliance standards that help reduce risks to the electricity grid and power systems serving hundreds of millions of people in the United States, Canada, and part of Mexico.

The NERC Critical Infrastructure Protection (CIP) requirements outline why a cybersecurity framework designed to protect and secure critical assets is vital for the dependable and effective delivery of electricity across North America's bulk electric system (BES). These standards are enforced as regulations, making them a legal requirement.

The Federal Energy Regulatory Commission (FERC) plays a crucial role in enforcing these NERC CIP standards to enhance the security and reliability of the electric grid, particularly after significant blackouts in history.

NERC cited an uptick in cyber threats against North American power grids, stating in a webcast that the "grids' virtual and physical weak spots, or points in software or hardware that are susceptible to cyber criminals, grew to a range of 23,000 to 24,000."

This article elaborates on the nature of rising threats to the power grid. It also explores how enterprise-grade password management enhances security resilience for the energy sector, strengthens password security, and ensures access controls that limit internal and external threats in compliance with NERC CIP standards.

Table of Contents

The power grid as an attack vector

The power grid is a critical component of economic growth, affecting both infrastructure and national security. Simply put, without a functioning bulk power system, society would grind to a halt. This also makes it an exceptionally attractive target for cybercriminals.

A recent finding by the Government Accountability Office (GAO) reveals the mounting challenges for securing operational technology in the energy industry, noting:

> "There are several points of vulnerability in the U.S.'s system of electricity grids. For example, grid distribution systems — which carry electricity from transmission systems to consumers — have grown more vulnerable, in part because their operational technology increasingly allows remote access and connections to business networks. This could allow threat actors to access those systems and potentially disrupt operations.
>
> Nations and criminal groups pose the most significant cyber threats to U.S. critical infrastructure, according to the Director of National Intelligence's 2022 Annual Threat Assessment. These threat actors are increasingly capable of attacking the grid."

"Nations and criminal groups pose the most significant cyber threats to U.S. critical infrastructure."

Director of National Intelligence's 2022 Annual Threat Assessment

Recent attacks against the power grid exploit physical and cybersecurity vulnerabilities. NERC referred to cyber threats as "more difficult to directly quantify." As noted above, security

weaknesses in the power system have increased, leading to an average of 60 additional cyberattacks per day.

Breaking down NERC CIP standards for critical infrastructure protection

There are 13 NERC CIP requirements relevant to power grid companies:

- BES cyber system categorization: Requires organizations to identify assets that could compromise the larger BES in the event of a cyberattack and to categorize and secure those assets accordingly. This includes identifying and securing 'BES cyber assets' and 'critical cyber assets' to ensure the reliable operation of the BES.
- Security management controls: Organizations must implement security management controls, such as training personnel and reporting security incidents, that protect BES cyber systems against compromise.
- Personnel and training: Individuals accessing BES cyber systems must be given a risk assessment and trained in security awareness.
- Electronic security perimeters: Organizations must define and then protect electronic security perimeters (ESPs) that protect BES assets.
- Physical security of BES cyber systems: Teams must have a physical security plan to protect BES cyber systems from compromise.
- System security management: This standard specifies the technical, operational, and procedural requirements necessary for protecting BES cyberinfrastructure, such as monitoring for and removing malicious code and changing known default passwords.
- Incident reporting and response planning: Describes incident response requirements, such as how frequently to document and how long to retain evidence of incidents.
- Recovery plans for BES cyber systems: Addresses recovery plan requirements to support the continued stability of the BES in the event of an incident.
- Configuration change management and vulnerability: To prevent and detect unauthorized changes to BES cyber systems, organizations must follow the specifications for when and how to set configurations.
- Information Protection: Companies must protect information critical to the operation of the BES during storage, use, and transit.
- Communications Between Control Centers: Data transmitted between control centers must be protected at all times.
- Supply Chain Risk Management: Organizations must implement security controls to mitigate supply chain risk.
- Physical Security: Organizations must put in place a plan to protect their physical locations and substations from physical attacks.

Use a password manager to ensure strong and unique passwords for accounts to help mitigate the risk of successful password spraying or credential stuffing attacks.

The NERC CIP compliance checklist is quite extensive. Focusing here on password security recommendations, the guidelines recommend that organizations:

- Revoke access to shared accounts in order to prevent a situation where passwords on substation and generation devices are constantly changed due to staff turnover.

- Use a password manager to ensure strong and unique passwords for accounts to help mitigate the risk of successful password spraying or credential stuffing attacks, as well as to minimize insecure or accidental password sharing with unauthorized individuals.
- Implement multifactor authentication to further bolster security.
- Prevent online password attacks by limiting the number of guesses an attacker can make.

Why Bitwarden is the best password solution for bulk electric system

A successful cyberattack against an electric grid system could grind operations and critical power supply to a halt. Fortunately, NERC CIP compliance software, such as Bitwarden, is the first line of defense against cybercriminals. By enabling energy suppliers to generate and manage strong and unique passwords, Bitwarden reduces their vulnerability to password-related breaches. Other key benefits include:

- **Role-based access controls** that allow administrators to customize and issue granular permissions, as well as control who has access to certain functions. By limiting user access based on necessity, power grid organizations maintain control over sensitive systems.
- An **end-to-end encrypted vault** that protects not just passwords but company cards and other personally identifiable information (PII).
- **Multifactor authentication capabilities** empower organizations with a second authentication layer to deter brute-force attacks or insider threats.
- **Password-sharing capabilities** enable teams and departments to safely generate, manage, and share complex passwords and other sensitive data from any location or device.
- **Seamless and flexible integration options** include Single Sign On (SSO) with identity providers and directory services (including SCIM).
- **Easy onboarding** with a centralized admin console where enterprise policies can be enabled and users are automatically provided.
- **Cross-platform access** with an unlimited number of devices.
- **Vulnerability reports** that reveal weak or reused passwords and detailed event logs to monitor user and group access to sensitive data with audit trails.
- **Regular third-party security audits**, cryptographic analysis, and penetration testing of Bitwarden to ensure the password manager upholds the highest security standards.

Did you know?

Using an enterprise-wide password manager like Bitwarden not only offers your company strong security, it also includes seamless and flexible integration with Single Sign On (SSO) options.

Because the bulk electric system powers the economy, impacts national security, and propels everyday life, it is vitally important that credentials used by energy providers remain highly protected with strong and unique passwords. Implementing an enterprise-wide password manager will also greatly benefit organizations that need to meet stringent and legally binding NERC CIP requirements.

Get started with Bitwarden

To explore Bitwarden business features and capabilities, get started with a free trial today.