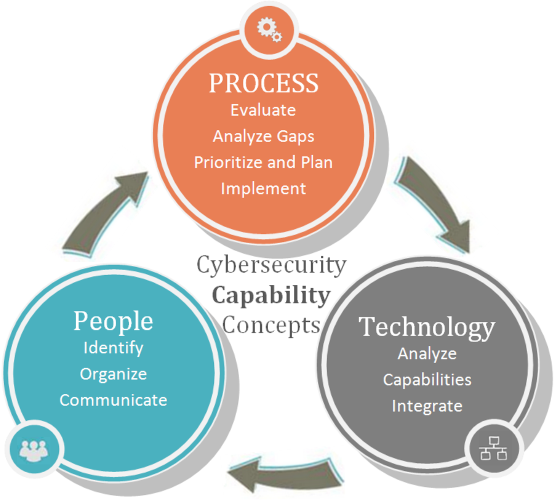
Electricity Subsector
CEO Cybersecurity Checklist

Executive Summary

This checklist, developed by government and industry partners, is intended to reinvigorate security conversations between CEOs and their support staff. These initial questions are intended to trigger more in-depth discussions to identify strengths and weaknesses, which will help guide security decision-making.

More in-depth guidance is available from various sources, examples are provided at the end of this document.



QUESTIONS

SYSTEMS AND ASSETS[1]

Do you maintain an inventory of your technology systems and assets?	🖧 ⚙
Have you identified the systems, assets, information, and processes that are essential to your organizational mission?	⚙
Do you have appropriate access control policies and procedures in place for all systems and assets with particular focus on those that are essential?	🖧 ⚙ 👥
Are your essential systems and assets appropriately separated or secured from your non-essential systems and assets?	🖧 ⚙

RESOURCES

Do you routinely assess the threats to your organization and the resources available for an appropriate defense?	🖧 ⚙ 👥
Do you routinely assess the resources available to govern and implement your security strategy?	⚙

INCIDENT RESPONSE

Do you maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity and physical security events?	⚙ 👥
Do you routinely exercise your response plans and procedures?	⚙ 👥
Do you perform post-event analysis? If not, do you have a list of support companies and government agencies that can be called for assistance?	⚙ 👥
Do you incorporate lessons learned into your policies, plans, and procedures?	⚙

[1] Systems and assets include technology assets, electronic equipment, energy management system (EMS) servers, software applications, firewalls, dial-up modems, data historians, mobile devices, web servers, remote terminal units (RTU).

RISK IDENTIFICATION AND MANAGEMENT

Do you have an enterprise-wide all-hazards risk management strategy?	⚙ 👥
Are your operations, cyber, and physical security teams engaged in your risk management strategy?	⚙ 👥
Do you periodically conduct risk assessments, including outsourced vulnerability assessments, and are the results reported to you?	⚙
Does your risk management strategy address cybersecurity supply chain risks?	🖧 ⚙ 👥
Does your risk management strategy address insider threat risks?	⚙ 👥
Does your risk management strategy include a change management process that prevents unintended consequences?	⚙

INFORMATION SHARING and SITUATIONAL AWARENESS

Do you maintain and integrate situational awareness of operations, cyber and physical threats?	🖧 ⚙ 👥
Do you maintain information sharing relationships with external entities (both government and commercial) to collect and provide cybersecurity and physical security information?	⚙ 👥

For more in-depth discussions:

10 Cyber Questions for Every CEO (EEI) – Assessment of the company's cybersecurity posture: Available by request

CEO Checklists (FERC OEIS) – Information System Protection checklist series to assess cybersecurity program strength and a more detailed checklist for Business Section Leaders: Available by request

Critical Controls for Effective Cyber Defense – Recommended set of actions to thwart the most pervasive attacks: http://www.counciloncybersecurity.org/images/downloads/Critical%20Controls%20v4.1.pdf

Cybersecurity Questions for CEOs (DHS) – Key questions about cyber risks: https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

Cyber Security Essentials: A Public Power Primer
https://ebiz.publicpower.org/APPAEbiz/ProductCatalog/Product.aspx?ID=4909

Electricity Subsector-Cybersecurity Capability Maturity Model (ES-C2M2) – Practices grouped into ten domains, e.g., risk management, incident response, and allows for consistent benchmarking across an organization: http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model-es-c2m2

FBI Cyber Task Forces – Investigative tools and techniques in response to known or suspected cyber incidents or intrusions: http://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1

Security Guideline for the Electricity Sector: Physical Security – Measures include defense in depth and environmental design:
http://www.nerc.com/comm/CIPC/Security%20Guidelines%20DL/Physical%20Security%20Guideline%202012-05-18-Final.pdf