

Securing the future of the power sector: CEA's Cyber Security Guidelines

May 2023





Background

Energy infrastructure, specifically the power sector, is considered critical to a functioning society as it enables other essential systems such as financial, communication, transportation, water, and sewer networks. A prolonged power outage in a large region would have a debilitating effect on national economic security and public health and safety, leaving the population vulnerable.

Due to the power sector's criticality, it is a prime target for cyber attackers who can cause significant disruptions in services and even cause physical damage to the infrastructure. While India has existing cyber security directives and guidelines in place, they are not specific to the power sector. The Ministry of Power has directed the Central Electricity Authority (CEA) to prepare regulations on cyber security in the power sector to address the specific needs and challenges of the sector.

In the meantime, the CEA has formulated a guideline on cyber security in the power sector under the provision of Section 3(10) in the 'Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019'. The guideline has been prepared after extensive consultations with stakeholders and inputs from CERT-In, the National Critical Information Infrastructure Protection Centre, NSCS (National Cyber Safety and Security Standards), IIT-Kanpur, and subsequent discussions with the Ministry of Power. All power sector utilities are mandated to follow the guidelines to ensure cyber security in the power sector.

In this paper, we discuss the increasing sources of cyber risk in the power sector, cyberattacks on the power sector, government measures to manage cyber risks, and the guidelines laid down by the CEA to protect the power sector from cyberattacks.

Growing cyber risk in the power sector

Cyber security has become a concern in the power sector because of several factors. Firstly, the increased connectivity because of the adoption of technologies such as smart grids, industrial control systems (ICS), and internet of things (IoT) devices has created more entry points for attackers to exploit. And secondly, attackers have become more sophisticated and organised, employing advanced techniques such as ransomware and supply chain attacks to target critical infrastructure systems. These attacks can be difficult to detect and can cause significant damage. The traditional "air gap" between Information Technology (IT) and Operational Technology (OT) systems is no

longer effective in protecting power systems against cyber threats. Attackers can use social engineering to bypass firewalls and the idea of an air gap has lost its significance. Cyber attacks in the power sector typically involve tactics such as initial access, execution, persistence, privilege escalation, defense evasion, command and control, and exfiltration. Once an attacker gains entry, they can take control of the IT network and operations of OT systems, potentially even remotely. This can lead to the loss of sensitive operational data, which can be used to design more advanced and dangerous attacks in the future.



RISK MANA

Concern over increase in cyber attacks on the power sector

The Indian power sector boasts an installed capacity exceeding **416 GW¹**, making it one of the largest in the world. In recent times the sector has become vulnerable to cyber threats with the growing use of technology in power generation, transmission, and distribution.

The Indian government has been concerned about the increasing cyber threats to the power sector. The Ministry of Power has conducted cybersecurity drills and exercises to test the preparedness of power utilities to deal with cyber incidents.

CERT-In has also issued advisory warnings of potential cyber threats to the country's power sector, including ransomware attacks and phishing attempts targeting power utilities. The advisory recommended that power utilities implement robust security measures and conduct regular cybersecurity audits to detect and prevent cyber threats.

The power sector is critical to the functioning of the economy and society, and any disruption of its operations could have far-reaching consequences. While the government is working on modernising India's power transmission system to counter cyber attacks, more needs to be done.

There is an urgent need for the power sector to implement a comprehensive cyber security strategy that includes regular security assessments, penetration testing, incident response planning, employee training, and incident response teams to detect and respond to cyber incidents. The CEA guidelines are a step in this direction.

Managing cyber risk in the power sector

The Indian Computer Emergency Response Team (CERT-In) is a national nodal agency responsible for promptly detecting and responding to cybersecurity incidents. To ensure the safety of the Indian power sector, the Ministry of Power has established six sector-specific CERTs (Computer Emergency Response Teams). These CERTs secure the thermal, hydro, transmission, grid operation, renewable energy, and distribution sub-sectors.

Each sectoral CERT has developed a model Cyber Crisis Management Plan (C-CMP) that is tailored to the needs of its sub-sector. These model plans have been distributed to the constituent utilities for the development and implementation of their own organisation-specific C-CMPs. The purpose of these plans is to enable utilities to respond quickly and recover efficiently from any cyber incident that may occur.

Source:
1. <https://cea.nic.in>



Setting a standard: New guidelines aim to enhance cyber security measures across the power sector

Currently, in India, there are numerous cybersecurity directives and guidelines, but none of them are specific to the power sector. To address this issue, the Ministry of Power has instructed the CEA to create regulations on cyber security for the power sector. As an interim measure, the CEA has been directed to issue guidelines on cyber security for the power sector under the provisions of Regulation 10 on Cyber Security in the "Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019."

Objective of the CEA guidelines²

- 01** Creating cyber security awareness
- 02** Creating a secure cyber ecosystem
- 03** Creating a cyber-assurance framework
- 04** Strengthening the regulatory framework
- 05** Creating mechanisms for security threat early warning, vulnerability management, and response to security threats,
- 06** Securing remote operations and services
- 07** Protection and resilience of critical information infrastructure
- 08** Reducing cyber supply chain risks
- 09** Encouraging the use of open standards
- 10** Promotion of research and development in cyber security
- 11** Human resource development in the domain of cyber security

Source:
2. <https://cea.nic.in/>



Overview of the CEA (Cyber Security in Power Sector) Guidelines, 2021

This comprehensive guideline on cybersecurity in the power sector is the first of its kind. It outlines the necessary measures for enhancing cybersecurity preparedness across various utilities in the sector to improve cybersecurity readiness. Divided into 14 articles, the guideline provides a structured framework for addressing cybersecurity threats in the power sector.

Articles

Cyber Security Policy

Protect OT systems by implementing an air gap between OT and IT networks

1

Identification of Critical Information Infrastructure (CII)

REs³ must provide information on their cyber assets, critical business processes & information infrastructure to NCIIPC

3

Article 5: Cyber Security Requirements

Ensure that the RE's Information Security Division (ISD) is operational 24/7

5

Phasing out of Legacy System

Ensure upgradability of IT technologies and phase out equipments/systems

7

Cyber Supply Chain Risk Management

Include specified cyber security clauses in procurement bids; source critical systems from trusted sources & have products cyber-tested if no trusted source is available

9

Cyber Crisis Management Plan(C-CMP)

Prepare and update C-CMP with sectoral CERT review, Board approval, annual review, and CISO enforcement during a cyber crisis.

11

Security and Testing of Cyber Assets

RE must secure cyber assets through updates, patching, testing, configuration security, and additional controls

13

Appointment of CISO

Appoint a qualified CISO for Responsible Entities

2

Electronic Security Perimeter

Identify & document electronic security perimeters

4

Cyber Risk Assessment and Mitigation Plan

Document and implement a Cyber Risk Assessment and Mitigation Plan

6

Cyber Security Training

Review and update cyber security training and ensure IT & OT/O&M personnel undergo mandatory training

8

Cyber Security Incident Report and Response Plan

Report cyber incidents to CERT-In, conduct mock drills, and update contact info with C-CMP within 15 days.

10

Sabotage Reporting%

RE must incorporate procedures for identifying, reporting, and preserving records of cyber sabotage

12

Cyber Security Audit

REs must implement ISMS, audit IT and OT systems yearly with CERT-In empaneled cyber security OT auditors

14

Abbreviation:
3. RE=Responsible Entities

[For detailed information on CEA guidelines click here](#)



Grant Thornton Bharat's Cyber Services

Grant Thornton offers end-to-end cyber security protection to power companies from cyber security assessment and threat management to crisis and resilience. We understand the critical nature of IT and OT infrastructure in the power sector, and we have developed our standard operating procedure basis our experience.

Our services

Cyber Security & Governance

- Cyber maturity assessments
- Framework design- NIST, CIS, ISO 27001
- Cyber training and awareness
- Cyber sustenance and certification assistance

Data Protection and Privacy

- Privacy maturity assessments
- Data privacy management- GDPR, DPP, ISO
- Virtual CISO and CDO services
- Privacy digitalisation and automation

Threat Management

- VAPT, source code review, and secure configuration
- SOC design, implementation, and integration
- Threat intelligence and incident management
- SOC as a service– managed services

Infrastructure Security

- Infra-security maturity assessments
- Cloud security architecture design
- IoT and OT security architecture design
- System testing and validation

Identity and access management

- IDAM implementation, migration, integration, and automation
- Privilege access review and account forensics
- IAM operations- staff augmentation

Third-party risk management

- TPRM framework design and implementation
- On-site and remote vendor assessments
- VRM KPI monitoring and dashboards
- VRM digitalisation and automation

Crisis and Resilience

- Cyber crisis, business continuity, and IT-DR
- C&R orchestration- staff augmentation
- Crisis simulation and red teaming exercises
- Cyber crisis response and recovery

Compliance and attest

- Computer system validation
- Regulatory audits- RBI, SEBI, IRDAI, UIDAI
- SOC I/II, SSAE 16/18, HITRUST audits
- Internal audits- IT and cyber security

Advantages with Grant Thornton Bharat

200+
cyber
professionals

CERT-In
empaneled

**Certified
professionals**
CISA, CISSP, OSCP,
CEH, ISO27001,
27701, AMBCI, etc.

**Marquee
clients**
Industry leaders
and emerging
businesses

**Quality
deliverables**
Leveraging best-in
class tools and SME
quality review



Conclusion

Power companies because of the critical nature of their infrastructure and the reliance on technology in their operations often have a large number of connected systems and devices, including industrial control systems (ICS), which are used to control and monitor power generation and distribution. These systems can be vulnerable to attacks. Furthermore, the integration of legacy systems, which lack modern security features, with newer technologies that may be more vulnerable to attack, makes the power sector a prime target for cybercriminals, nation-state actors, and other malicious actors.

Building a cyber security framework that is secure, vigilant, and resilient is crucial. This includes developing a robust incident response plan, deploying state-of-the-art security technologies, and providing regular training to employees on how to identify and respond to cyber threats. In addition, power companies can collaborate with peers, governments, suppliers, and other industrial sectors to share intelligence, participate in practice exercises, develop new standards and frameworks, and establish incident response teams. This can help to improve the overall cyber resilience of the power sector and reduce the risk of cyberattacks.



Great
Place
To
Work®

Certified

NOV 2022 – NOV 2023

INDIA

We are Shaping a Vibrant Bharat

A member of Grant Thornton International Ltd, Grant Thornton Bharat is at the forefront of helping reshape the values in the profession. We are helping shape various industry ecosystems through our work across Assurance, Tax, Risk, Transactions, Technology and Consulting, and are going beyond to shape a more #VibrantBharat.

Our offices in India

- Ahmedabad ● Bengaluru ● Chandigarh ● Chennai
- Dehradun ● Gurugram ● Hyderabad ● Kochi
- Kolkata ● Mumbai ● New Delhi ● Noida ● Pune



Scan QR code for office addresses

www.grantthornton.in

Connect
with us



@GrantThorntonBharat



@GrantThorntonIN



@GrantThorntonBharat



@GrantThorntonBharatLLP



@Grantthornton_bharat



Gtbharat@in.gt.com

© 2023 Grant Thornton Bharat LLP. All rights reserved.

"Grant Thornton Bharat" means Grant Thornton Advisory Private Limited, the sole member firm of Grant Thornton International Limited (UK) in India, and those legal entities which are its related parties as defined by the Companies Act, 2013, including Grant Thornton Bharat LLP.

Grant Thornton Bharat LLP, formerly Grant Thornton India LLP, is registered with limited liability with identity number AAA-7677 and has its registered office at L-41 Connaught Circus, New Delhi, 110001.

References to Grant Thornton are to Grant Thornton International Ltd. (Grant Thornton International) or its member firms. Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered independently by the member firms.