OT-IT Cybersecurity for India’s Energy Sector: 2026 Risk, Compliance and ROI

By Sudarshan Karweer · 25 August 2026 · growthifye.com

A practical 2026 guide to OT-IT cybersecurity for Indian energy companies, covering compliance, architecture, costs, ROI and lender expectations.

India’s power and renewable-energy sector is digitising faster than its cyber controls are maturing. Utility-scale solar and wind plants now run on connected SCADA, smart inverters, remote substations, IoT gateways, cloud analytics, mobile O&M applications and API-linked market systems. Commercial and industrial consumers are layering rooftop solar, battery energy storage, open-access procurement, smart meters and demand-response tools on top of legacy electrical infrastructure. The result is clear: cyber risk is now operational risk, revenue risk and lender risk.

For Indian energy companies, the OT-IT cybersecurity conversation in 2026 is no longer about buying another firewall. It is about protecting generation availability, forecasting integrity, dispatch commands, billing accuracy, REC and carbon-data workflows, substation communications, remote maintenance channels and board-level enterprise risk metrics. This is especially relevant for developers, utilities, C&I power users, lenders and policymakers dealing with higher renewable penetration, more digital interconnections and tighter compliance expectations.

This article focuses on a specific angle that is distinct from generic digital transformation: how Indian energy companies should design OT-IT cybersecurity programmes that stand up to current threat patterns, regulatory scrutiny, lender due diligence and operational realities.

Why OT-IT cybersecurity is now a board issue in India’s energy market

Cyber incidents in energy are no longer limited to headline-grabbing attacks on national grids. In India, the more common and financially material problems are often smaller but frequent failures: unauthorised remote access to plant networks, poorly segmented SCADA environments, insecure OEM maintenance connections, shared passwords on substation devices, unpatched Windows engineering stations, weak VPN policies, exposed internet-facing assets and cloud misconfigurations in analytics stacks.

The financial impact is straightforward.

- A 100 MW solar plant with a CUF of 24% produces about 576,000 kWh per day.
- At a realised tariff of Rs 2.80 per kWh, one day of avoidable outage can mean about Rs 16.1 lakh in lost revenue.
- For a 250 MW wind portfolio with a 32% PLF, one day of major dispatch disruption can translate into over 1.92 million kWh of affected generation; at Rs 3.20 per kWh, that is about Rs 61.4 lakh of revenue exposure before considering DSM implications, balancing costs or contractual penalties.
- For C&I consumers, a cyber event affecting captive or group-captive energy systems may trigger expensive grid drawal during peak tariff periods, production loss, data compromise and compliance exposure.

The industry has also moved to distributed operating models. Asset managers may monitor plants in Rajasthan, ■■■■■■, Tamil Nadu, Karnataka and Maharashtra from central control centres. Vendors may support relays, trackers, inverters, met stations and battery EMS remotely. Every connection improves

efficiency, but every connection also enlarges the attack surface.

Boards and lenders increasingly ask five practical questions:

- Can an attacker disrupt generation or dispatch?
- Can operational data be altered without detection?
- Are remote access pathways controlled and logged?
- Does the company have an incident response process that works at plant level?
- Will a cyber event affect debt servicing, insurance claims or valuation?

If the answer to these is uncertain, cybersecurity becomes a financing and governance issue, not merely an IT task.

The 2026 threat landscape for solar, wind, storage and utility assets

Indian energy assets face a different risk mix from generic enterprise environments because OT systems prioritise availability and safety over frequent change. Many field devices were never designed for modern threat conditions.

Key attack vectors in 2026 include:

- Compromised VPN or remote desktop access used by OEMs, EPC contractors or O&M partners
- Phishing attacks that pivot from office IT to shared credentials used in plant operations
- Ransomware affecting historian servers, reporting systems, engineering workstations or backup repositories
- Exploitation of insecure protocols in substations and plant-control networks
- Malware introduced through USB media during maintenance windows
- Misconfigured cloud dashboards exposing generation, site access or control interfaces
- Insider misuse, especially where admin privileges and shared accounts are common
- Supply-chain risks in third-party software, firmware and unmanaged edge devices

Battery energy storage systems deserve specific attention. BESS projects use tightly integrated EMS, BMS, PCS and thermal-management controls. If these systems are not segmented and monitored correctly, the risk is not limited to downtime; it can affect safety, warranty compliance and dispatch reliability in ancillary-services or peak-shaving applications.

For utilities and DISCOMs, the threat surface includes AMI systems, distribution automation, outage management, data concentrators, substation automation and increasingly digital consumer interfaces. For C&I campuses, energy cybersecurity intersects with facility management, EV charging, DG synchronisation, building management systems and process-control environments.

India’s policy and compliance context in 2026

Cybersecurity expectations in India’s power sector are shaped by a mix of sectoral directives, national cyber frameworks, data-governance obligations and lender requirements. Companies should not wait for a single perfect rulebook; they should align to the applicable stack of obligations.

Relevant anchors in 2026 include:

- Directions and cybersecurity expectations issued under the Ministry of Power and sectoral institutions governing power-system operations and critical infrastructure practices

- CERT-In requirements relating to cyber incident reporting timelines, log retention and synchronisation of system clocks
- The Digital Personal Data Protection Act where employee, customer or vendor data is involved
- Sector-specific utility and grid-operation requirements applicable to SLDC, RLDC and market-interfacing systems
- Contractual obligations from lenders, insurers, investors and multilateral agencies requiring cyber risk assessment and control evidence
- Internal governance expectations aligned to standards such as ISO 27001, IEC 62443 and the NIST Cybersecurity Framework

For energy companies, IEC 62443 is particularly relevant because it addresses industrial automation and control systems. It gives a practical structure for zoning, conduits, asset criticality, access control, secure maintenance, patch governance and system hardening.

A useful 2026 compliance principle is this: do not build a programme that is only audit-friendly; build one that is operationally survivable. Many plants can produce policy documents for audits, but far fewer can show tested asset inventories, firewall rule reviews, remote-access logs, OT backup restoration drills, offline recovery capability and tabletop exercises involving plant managers.

What a practical OT-IT security architecture should look like

A workable architecture for Indian energy companies does not start with expensive software. It starts with visibility and segmentation.

First, create an accurate asset inventory across:

- Inverters, relays, RTUs, PLCs and data loggers
- SCADA servers, historians and engineering stations
- Networking equipment, firewalls and serial-to-IP converters
- Weather stations, tracker controllers and met masts
- BESS control systems and auxiliary equipment
- Endpoint devices used by O&M teams
- Cloud workloads, APIs and analytics integrations

In many portfolios, companies discover that 10% to 20% of connected assets were either undocumented or owned informally by vendors. That is an unacceptable baseline for critical infrastructure.

Second, segment networks by function and criticality.

A minimum architecture usually includes:

- Corporate IT zone

n- OT DMZ for controlled data exchange

- Plant-control network segmented from office and internet traffic
- Separate secure paths for vendor remote support
- Restricted engineering workstation access
- Logging and monitoring infrastructure with time-synchronised records

Third, harden remote access.

Remote connectivity is often the weakest link in Indian energy operations because geographically dispersed sites depend on external support. Minimum controls should include:

- Multi-factor authentication for all privileged and remote sessions
- Named individual accounts, never shared generic logins
- Time-bound access approvals
- Session recording for critical vendor access
- Jump servers in a DMZ rather than direct device exposure
- Blocked USB by default, with controlled exceptions

Fourth, establish OT-aware monitoring.

Traditional SOC tools built only for office environments often miss energy-specific anomalies. OT-aware monitoring should detect:

- Unexpected configuration changes in relays or controllers
- New devices appearing in plant networks
- Unusual traffic between SCADA and field devices
- Repeated failed logins to engineering stations
- Unapproved remote sessions outside maintenance windows
- Data integrity anomalies in generation or metering streams

Fifth, define backup and recovery around operational continuity.

For energy assets, cyber resilience means more than backing up files. Companies need tested restoration for:

- SCADA configurations
- Relay settings
- PLC logic and HMI configurations
- Historian databases
- EMS and BESS control parameters
- Critical network device configurations

An offline, immutable backup strategy is increasingly expected by insurers and lenders.

Cost, ROI and how to justify cybersecurity investments

Indian promoters and asset managers often ask the right question: what is the commercial case for OT-IT cybersecurity?

The answer lies in avoided downtime, lower incident-recovery cost, improved insurability, better lender confidence and reduced contract friction with offtakers and technology partners.

Indicative 2026 budgeting ranges for mid-sized Indian energy businesses can look like this:

- Cyber maturity assessment for a 500 MW renewable portfolio: Rs 12 lakh to Rs 35 lakh depending on site count and depth
- Basic OT network segmentation and secure remote-access redesign for multiple sites: Rs 40 lakh to Rs 1.5 crore

- Managed detection and response with OT visibility for a portfolio platform: Rs 25 lakh to Rs 90 lakh annually
- Plant-level hardening, asset discovery and log integration: Rs 5 lakh to Rs 20 lakh per site depending on existing architecture
- Incident response retainer and tabletop exercise programme: Rs 8 lakh to Rs 30 lakh annually

These are not trivial numbers, but compare them with outage economics. If a 300 MW portfolio prevents just two days of high-impact disruption in a year, the payback can be immediate. There is also soft but real value in smoother technical due diligence, fewer lender queries, faster insurance discussions and stronger confidence from strategic investors.

For C&I consumers, the ROI case can be even sharper where cyber incidents could interrupt manufacturing. A single unplanned production halt can cost far more than an annual OT security programme. In sectors such as metals, chemicals, cement, food processing, data centres and automotive manufacturing, cyber-driven energy downtime can quickly become an enterprise-loss event.

A practical ROI model should include:

- Estimated loss per hour of generation or production interruption
- Recovery cost from corrupted OT and IT environments
- Vendor call-out and reconfiguration cost
- Potential penalties, settlement losses or missed market opportunities
- Cyber-insurance premium and deductible implications
- Financing friction and delayed transaction timelines

What lenders, investors and policymakers should ask in due diligence

Cybersecurity is becoming part of technical and operational diligence, especially for large portfolios, transmission-linked assets, storage projects and digitally intensive utility systems.

Lenders and investors should ask for evidence on:

- Asset inventory completeness and ownership mapping
- OT-IT network diagrams with segmentation controls
- Privileged access and vendor-access governance
- Patch and vulnerability management exceptions for OT systems
- Backup and restoration test records
- Security monitoring coverage across central and site environments
- Incident response plans involving both IT and plant operations teams
- Roles and liabilities in EPC, O&M and OEM contracts

This last point is often overlooked in India. Many contracts specify uptime obligations and response times but say very little about cybersecurity accountability, secure remote access, log retention, firmware provenance, breach notification or forensic cooperation. In 2026, that omission creates avoidable legal and operational ambiguity.

Policymakers and utilities can improve sector resilience by encouraging minimum cyber baselines in procurement and interconnection processes. For example:

- Standard cyber clauses in utility tenders and O&M contracts
- Baseline remote-access controls for grid-connected assets
- Minimum logging and event-retention requirements for critical plants
- Cyber-drill expectations for operators of key infrastructure
- Guidance for integrating distributed energy resources securely into utility environments

A 12-month action plan for Indian energy companies

For companies that know the risk is real but are unsure where to begin, the first year should focus on control foundations rather than tool sprawl.

Months 1-3:

- Run an OT-IT cyber maturity assessment across representative sites
- Build a validated asset inventory and criticality map
- Identify internet-exposed assets and remove unsafe direct exposures
- Review all remote-access pathways used by staff and vendors

Months 4-6:

- Implement or strengthen network segmentation and OT DMZ controls
- Enforce MFA and named accounts for privileged users
- Establish centralised logging for critical systems
- Update cyber clauses in vendor, O&M and EPC agreements

Months 7-9:

- Deploy OT-aware monitoring and anomaly detection
- Test backup restoration for SCADA, relay settings and key controllers
- Conduct phishing awareness and admin-access hygiene training
- Build incident response playbooks for plant and central teams

Months 10-12:

- Run tabletop exercises involving operations, IT, management and legal teams
- Close high-priority vulnerabilities that are operationally safe to remediate
- Align documentation to IEC 62443 and enterprise governance standards
- Report cyber KPIs to leadership with financial-risk translation

The most useful KPIs are not vanity metrics. Track:

- Number of unmanaged or unknown OT assets
- Percentage of privileged access under MFA
- Number of direct vendor connections removed or redesigned
- Backup restoration success rate
- Mean time to detect and isolate OT incidents
- Patch exception backlog by asset criticality

The strategic takeaway for India’s energy transition

India’s energy transition depends on digital infrastructure as much as physical infrastructure. Solar, wind, storage, smart grids, open access, market integration and flexible demand all increase the importance of trustworthy digital operations. OT-IT cybersecurity is therefore not a support function. It is a reliability, bankability and competitiveness function.

For renewable developers, the goal is to protect generation, lender confidence and portfolio value. For C&I consumers, it is to protect energy continuity and industrial output. For utilities, it is to secure grid operations and consumer trust. For policymakers, it is to reduce systemic vulnerability in an increasingly connected power system.

The firms that will perform best in 2026 and beyond are not necessarily those spending the most on cyber tools. They are the ones that understand their operational dependencies, segment their networks properly, control remote access, test recovery in real conditions and treat cyber resilience as part of asset performance.

If your organisation is planning new renewable assets, refinancing an operating portfolio, modernising control environments or evaluating cyber risks across IT and OT systems, contact Growthifye’s advisory desk for a practical assessment and implementation roadmap tailored to India’s energy sector.

ABOUT THE AUTHOR

Sudarshan Karweer — Chief Executive Officer, Growthifye

Over 23 years in management consulting — concept to scale — building and scaling new-age digital and energy businesses. An EY alumnus, Sudarshan leads Growthifye's renewable energy & storage advisory, EPC, transmission engineering and green-financing practices for developers, utilities and C&I consumers across India.
Contact: info@growthifye.com · +91 99676 45323 · growthifye.com