OT/IT Cybersecurity for India Renewables 2026: Risks, Compliance, ROI and Roadmap

By Sudarshan Karweer · 13 September 2026 · growthifye.com

A practical 2026 guide to OT/IT cybersecurity for Indian renewables, utilities and C&I energy users: risks, compliance, costs and rollout.

India's renewable and power-sector digitisation story in 2026 is no longer just about visibility and automation. It is about resilience. As solar, wind, BESS, substation automation, remote O&M, smart meters, open-access platforms and cloud analytics scale up, the attack surface across generation, transmission, distribution and C&I energy operations has widened sharply.

For Indian renewable developers, utilities, captive and open-access consumers, and lenders evaluating operating risk, OT/IT [cybersecurity](/coreservices/itconsulting/cybersecurity) has moved from a technical afterthought to a board-level issue. A ransomware event at a corporate IT layer can disrupt invoice cycles and vendor payments. A poorly segmented network can expose plant SCADA, protection relays or PPC interfaces. A compromised VPN account can give attackers a path from remote maintenance access into critical operating systems. In a sector where a few hours of forced downtime can affect generation, scheduling, DSM exposure, SLDC compliance and offtaker confidence, cybersecurity now has measurable financial impact.

This article focuses on a distinct angle from ERP, APM, EAM and analytics platforms: how Indian energy companies should approach OT/IT cybersecurity in 2026, what threats matter most, what regulations and lender expectations are emerging, what typical investment ranges look like, and how to build a practical rollout roadmap.

Why OT/IT cybersecurity is now a commercial issue in Indian energy

Historically, many Indian power and renewable businesses treated cyber risk as a narrow IT responsibility focused on email, laptops and data backups. That is no longer sufficient for three reasons.

First, operational technology is increasingly connected. Utility-scale solar plants routinely expose SCADA, weather stations, string or central inverters, meters, CCTV, PPCs and remote troubleshooting links. Wind portfolios use OEM remote-access arrangements, condition-monitoring systems and central fleet visibility tools. BESS adds EMS, fire-safety controls, HVAC controls and networked protection systems. Utilities operate AMI, OMS, GIS, distribution automation and substation systems with growing interdependence.

Second, the commercial cost of disruption has risen. A 100 MW solar project with a CUF of 24% produces around 576 MWh per day. At a realised tariff of Rs 2.8 to Rs 3.4 per kWh, one day of avoidable outage can mean roughly Rs 16 lakh to Rs 20 lakh of revenue impact before considering contractual consequences. For a 250 MW hybrid or RTC-linked portfolio, the exposure can be materially higher, especially where scheduling commitments, banking constraints or firm delivery obligations apply. For C&I consumers, downtime of energy monitoring, captive dispatch controls or plant electrical systems can also spill into production losses.

Third, lenders, insurers, offtakers and regulators increasingly view cyber maturity as part of operational risk management. For infrastructure assets with 15-25 year lives, cyber posture affects due diligence quality in the same way that transformer redundancy, O&M capability, spare strategy and evacuation readiness do.

The threat scenarios that matter most in 2026

Not every cyber risk deserves the same attention. Indian energy companies should prioritise realistic operational scenarios rather than generic checklists.

The most material scenarios include:

- Ransomware entering through corporate IT and spreading to shared servers used for SCADA reporting, historian exports or remote engineering files
- Compromise of remote-access tools used by OEMs, EPCs, system integrators or local O&M vendors
- Flat networks where plant OT systems can be reached from office networks without proper segmentation
- Weak password practices or unmanaged privileged accounts on HMIs, engineering workstations, PLC support tools or firewall consoles
- Insecure internet-facing devices such as DVRs, routers, dataloggers or outdated remote terminal equipment
- USB-borne malware introduced during field maintenance at substations, plants or control rooms
- Tampering with meter data, alarm thresholds, historian data or reporting logic, affecting settlement, performance analytics or compliance evidence
- Denial-of-service or communication disruption affecting SLDC reporting, remote operations or dispatch coordination
- Third-party software vulnerabilities in SCADA components, VPN appliances, firewalls or Windows-based engineering systems

For C&I users with captive or group-captive renewable supply, another underappreciated risk is compromise of digital platforms that support open-access scheduling, billing validation, meter reconciliation and energy accounting. Even if generation assets remain unaffected, financial leakage can occur if data integrity is lost during critical monthly settlement windows.

India’s 2026 compliance and governance context

The compliance landscape is tightening, even if implementation maturity still varies by organisation. Energy-sector executives should track cyber governance across three layers: sectoral directions, general digital law and contractual requirements.

At the sector level, central and state power-sector entities continue to operate in an environment shaped by cybersecurity directions applicable to power systems, CERT-In reporting expectations, and critical-infrastructure protection principles. Grid-connected entities that interface with load dispatch systems, transmission networks or utility control environments should assume that auditability, logging, incident response and controlled connectivity will attract more scrutiny over time, not less.

At the enterprise level, the Digital Personal Data Protection framework matters where employee, vendor or consumer data is processed, especially by utilities, retail suppliers and platform operators. While OT systems may not be personal-data heavy, adjacent IT platforms often are.

At the contractual level, lenders, insurers, large commercial offtakers and multinational investors increasingly ask questions such as:

- Is there formal separation between IT and OT networks?
- Are critical assets covered by MFA-enabled remote access?
- Are backups offline, tested and recoverable?

- Is there a current asset inventory of plant cyber-connected equipment?
- Are cyber incidents reportable under financing or insurance covenants?
- Are OEM and EPC support pathways governed by access-control and logging standards?

For Growthifye's clients, this means cybersecurity should not sit only inside the IT department. It should be part of project risk reviews, O&M governance, EPC handover checklists and lender diligence data rooms.

What a practical OT/IT cybersecurity architecture looks like

Indian energy companies do not need to pursue an overly complex architecture from day one. They do need a disciplined baseline. In 2026, a practical energy-sector cyber stack usually includes the following building blocks.

First is asset visibility. Many organisations cannot answer a basic question: exactly which cyber-connected assets exist at each site, what firmware or OS versions they run, which ports are open, and who supports them. Without that baseline, patching and risk prioritisation become guesswork.

Second is network segmentation. A corporate ERP or email compromise should not provide a path into plant SCADA or substation automation systems. At minimum, companies should establish clear zoning between corporate IT, plant OT, DMZ services and vendor remote-access pathways. In multi-site portfolios, each site should be reviewed separately rather than assumed identical.

Third is identity and access control. Shared administrator credentials remain common in plants and substations. In 2026, that is hard to justify. MFA for remote access, named accounts, role-based privileges, session logging and time-bound vendor access are now baseline controls.

Fourth is secure remote operations. Many portfolios rely on OEM and integrator support from multiple cities or countries. That does not need to stop, but access should be brokered through controlled gateways rather than open VPN sprawl. Jump servers, approval workflows and recorded sessions materially reduce risk.

Fifth is monitoring and detection. Traditional IT SIEM approaches are useful but insufficient on their own for OT-heavy environments. Energy companies should monitor network anomalies, configuration changes, failed logins, unusual traffic to PLC or HMI segments, and suspicious remote sessions. Even a lightweight managed SOC model can be effective if tuned for plant realities.

Sixth is backup and recovery. The right question is not whether backups exist, but whether they can restore operations quickly. Critical items include SCADA servers, historian configurations, HMI images, firewall configs, relay settings, PPC logic, EMS/BMS configurations and key engineering files. Recovery drills should test realistic outage scenarios.

Seventh is governance. A strong architecture fails if no one owns exceptions, patch windows, vendor onboarding or incident escalation. This is where capabilities such as Cybersecurity and Program governance become essential, especially for portfolios with mixed OEM technologies and decentralised plant teams.

Typical investment ranges and ROI logic in India

Cybersecurity ROI is often challenged because the benefit is risk avoided, not revenue directly created. But for energy businesses, the business case is stronger than many assume.

In India, 2026 costs vary widely by scale and complexity, but indicative ranges for planning are as follows:

- Small C&I captive or rooftop-heavy enterprise with 1-3 critical sites: Rs 20 lakh to Rs 75 lakh for baseline assessment, segmentation improvements, MFA-enabled remote access, backup hardening and

essential monitoring

- Mid-sized renewable portfolio of 250-500 MW across multiple solar or wind sites: Rs 75 lakh to Rs 2.5 crore for OT discovery, network redesign, secure remote access, central log monitoring, backup recovery improvements and policy rollout
- Large IPP, utility or discom programme across many sites and control environments: Rs 3 crore to Rs 15 crore+ depending on legacy estate, SOC scope, substation depth, AMI exposure and remediation backlog

Operating costs typically include managed monitoring, license renewals, periodic assessments, incident-response retainers and training. For many organisations, annual run-rate costs fall in the range of 12% to 20% of initial programme investment, though highly distributed fleets can be higher.

The ROI case usually comes from avoiding one or more of the following:

- Generation loss from cyber-induced outage or prolonged recovery
- DSM penalties or scheduling disruption due to telemetry/reporting failures
- Delayed invoicing or settlement because of data-system unavailability
- Insurance issues or higher deductibles after control gaps are identified
- Lender concern leading to tighter reserve expectations or delayed approvals
- Reputational damage with C&I offtakers who expect digital reliability
- Emergency remediation spending that is 2-5x more expensive than planned hardening

For example, if a 300 MW solar-wind portfolio loses even 8-10 hours of coordinated operations during a high-generation window, the direct revenue and balancing impact can alone justify a meaningful share of a basic cyber programme. Add recovery labour, external forensics, controller reconfiguration, claim management and management distraction, and the economics become clearer.

A rollout roadmap for developers, utilities and C&I energy users

The right rollout model is phased, risk-based and linked to operations, not only compliance.

Phase 1 should be a 6-10 week diagnostic. This covers site and enterprise asset inventory, architecture mapping, critical-access review, vulnerability prioritisation, backup maturity, third-party access pathways and incident-response readiness. The output should be a board-readable risk heatmap plus a sequenced remediation plan. This is often where [IT strategy & roadmaps](/coreservices/itconsulting/itstrategyandroadmaps) work becomes valuable, because cyber controls must align with plant operations, cloud adoption and broader systems architecture.

Phase 2 should address the highest-risk gaps first:

- Remove or secure exposed internet-facing devices
- Enforce MFA for all remote access
- Segment IT and OT environments
- Clean up shared and dormant accounts
- Harden backup strategy with offline and tested restore points
- Establish vendor-access approval and logging

Phase 3 should institutionalise monitoring and governance:

- Deploy central logging and alerting

- Define OT-specific incident playbooks
- Train plant managers, control-room users and field technicians
- Include cyber checks in preventive-maintenance and shutdown planning
- Add security clauses and access standards in OEM, EPC and AMC contracts

Phase 4 should focus on resilience at scale. For larger platforms, that means standard reference architectures for new sites, cyber requirements in EPC design reviews, periodic red-team or tabletop exercises, and tighter integration with [Data & analytics platforms](/coreservices/itconsulting/dataandanalyticsplatforms) so that operational anomalies and cyber anomalies can be correlated.

For lenders and investors, a useful practical test is simple: can the borrower demonstrate visibility, control, recovery and accountability? If yes, cyber risk is being managed. If not, the issue is not just technical debt; it is operational and financial fragility.

What decision-makers should do in the next 90 days

If you are a renewable developer, utility, industrial energy consumer or infrastructure lender, the immediate next step is not to buy tools blindly. It is to establish decision-grade clarity.

Over the next 90 days, organisations should:

- Identify which plants, substations, BESS sites, control rooms and corporate systems are most business-critical
- Map all remote-access routes used by OEMs, O&M vendors and internal teams
- Review whether OT and IT are genuinely segmented or only assumed to be
- Test backup restoration for at least one critical operational system
- Confirm who owns cyber governance across operations, IT and management
- Add cyber diligence questions into financing, acquisition and O&M review processes

In India’s 2026 energy market, digital maturity without cyber maturity is not modernisation. It is unmanaged exposure. The companies that will outperform are not necessarily those spending the most, but those building disciplined, auditable, operations-aware cyber controls across both IT and OT environments.

If your organisation is planning renewable growth, modernising utility operations or digitising multi-site energy assets, contact Growthifye’s advisory desk to assess your OT/IT cybersecurity posture and define a practical rollout roadmap tailored to Indian energy operations.

Explore Growthifye's related capabilities

This analysis connects directly to our advisory practice: [IT strategy & roadmaps](/coreservices/itconsulting/itstrategyandroadmaps) · [ERP & asset management systems](/coreservices/itconsulting/erpandassetmanagementsystems) · [Data & analytics platforms](/coreservices/itconsulting/dataandanalyticsplatforms) · [Cloud migration](/coreservices/itconsulting/cloudmigration).

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 84510 99371 · growthifye.com