FROST & SULLIVAN

Building Cyber Resilience Across India's Critical Infrastructure

From Policy to Practice: Strengthening Cybersecurity and Industrial Resilience | CyberSec Delhi Conference 2026

Authored by **Pranav Sahai,** Industry Analyst, Global Security and AI, Growth Advisory**, Frost & Sullivan**

The State of Critical Infrastructure Cybersecurity in India

India's critical infrastructure increasingly depends on interconnected digital systems. Power networks, railways, transport hubs, public services and industrial facilities use these systems to monitor operations, coordinate activity and sustain continuity. While connectivity improves efficiency, it also expands the operational consequences of a cyber incident: disruption can extend beyond data and digital services to physical operations, public confidence and economic activity.

At the 2026 CyberSec Delhi Conference, resilience emerged as a central theme. The discussion suggested that the question for infrastructure operators is no longer simply whether security controls exist, but whether people, processes and systems can withstand an incident and recover safely.

Major General Manjeet Singh (Retd.) of Gramax CyberTech captured that distinction:

> ***"Resilience is something much more than compliance. It requires organizations to prepare for disruption, test their response, and sustain essential operations when preventive controls are not enough. That means defining decisions rights before a crisis, rehearsing recovery with operational teams, and learning from every exercise. Resilience becomes credible only when plans can be executed under real pressure."***
>
> **— Major General Manjeet Singh (Retd.), Gramax CyberTech**

Compliance remains important: it establishes expectations and can help organizations formalize responsibility. But compliance alone cannot prove that response plans work under pressure, that critical assets are understood, or that operational teams can restore services after disruption. Resilience requires exercises, clear decision rights, tested recovery procedures and coordination between cybersecurity, engineering, operations and leadership.

Artificial intelligence is changing the tempo of the challenge. Automated tools can help defenders correlate signals and investigate suspicious activity, but attackers can also use automation to increase the speed and scale of their activity**.**

Commander Aditya Varma (Retd.) of Cisco emphasized the resulting operational requirement:

> ***"The defenders also have to defend at machine scale. As AI increases the speed and volume of attacks, security operations must use automation to detect, prioritize, and respond quickly while retaining human oversight. Machine-speed defence also depends on reliable telemetry, well-tuned playbooks, and safeguards against automated errors. Human judgment remains essential when a response could disrupt critical services."***
>
> **— Commander Aditya Varma (Retd.), Cisco**

This does not mean that every security decision should be handed to autonomous systems. It means that organizations need to improve detection and triage speed while retaining oversight for consequential actions. AI-supported operations should be evaluated for reliability, visibility and the ability to explain why an

alert or response was triggered. Human teams remain essential for context, prioritization and decisions that may affect service continuity.

A second recurring issue is visibility. Operators need to know which assets are connected, what those assets communicate with, who can access them and which dependencies are essential to service delivery. Without that baseline, teams may struggle to distinguish normal activity from a genuine threat or to understand the likely consequences of isolating a system.

Workforce readiness is equally important.

Abhijit Singh Anand, Founder and CEO of Zindagi Technologies, distinguished examinations from practical preparation:

> ***"A drill is something that will test your skills on the day of a cyber-attack. Practical exercises expose gaps in coordination and decision-making that examinations and certifications alone cannot reveal. They should test technical response alongside leadership escalation, communications, and recovery choices. Repeated practice helps teams build the confidence and shared understanding needed during an actual incident."***
>
> — **Abhijit Singh Anand, Founder and CEO, Zindagi Technologies**

Exercises should test technical response as well as management escalation, communications, legal coordination and recovery decisions. Awareness also needs to extend beyond specialist teams to employees, contractors, suppliers and smaller partners whose systems may connect to critical operations.

The path forward is therefore practical: maintain an accurate asset and dependency inventory; test response and recovery through realistic exercises; strengthen collaboration between IT, OT and business teams; develop AI capabilities with clear oversight; and make cyber awareness a continuing activity rather than a one-off campaign. Critical infrastructure resilience is not delivered by one tool or policy. It is built through sustained operational discipline and shared responsibility.

Securing India's Industrial Backbone

Operational technology (OT) and industrial control systems (ICS) sit at the intersection of digital security and physical operations. They monitor or control processes in environments such as power generation, manufacturing, rail transport, aviation and maritime logistics. Unlike many enterprise IT systems, industrial environments may have long equipment lifecycles, specialized protocols, tightly managed maintenance windows and a strong requirement for availability. Security measures must account for those realities rather than assume that conventional IT responses can be applied without adaptation.

Col. Alok Shankar Pandey of Dedicated Freight Corridor Corporation of India Limited highlighted the risk asymmetry that makes OT security distinct:

> ***"The probability of which happening is very, very, very low. But as and when it happens, the impact will be exponentially high. Critical-infrastructure planning must therefore weigh consequences as seriously as likelihood, with tested crisis plans, secure backups, and recovery drills. Because safety and continuity are inseparable in operational environments, containment decisions must account for physical processes. Continuous monitoring and cross-functional coordination are vital to reducing downtime."***
>
> — **Col. Alok Shankar Pandey, DFCCIL**

Not every industrial incident is equally likely, and not every compromise will cause physical harm. However, risk assessments must weigh operational consequences alongside event probability. A control-system

disruption can affect safety, production, logistics or the delivery of an essential service. Recovery can also be more complex when equipment cannot be taken offline quickly or restored from a standard backup.

In power environments, security teams need visibility across control systems, engineering workstations, substations, communications and enterprise networks. Understanding the legitimate communications between assets can help identify unexpected connections and support more informed containment decisions. Prem Prakash Rai of APCPL underscored this basic requirement: operators must know their networks and what they communicate with. That knowledge is a starting point for segmentation, access governance and incident investigation.

Manufacturing facilities face a related challenge as production equipment, industrial robots, sensors and business applications become more connected. Operators need to establish what normal activity looks like for each process and manage remote access by vendors and maintenance partners. Changes to industrial systems should be coordinated with engineering and operations teams so that security improvements do not inadvertently undermine safety or availability.

Aviation and maritime environments add further dependencies. Airports bring together facilities management, access control, baggage handling, maintenance and IT systems. Ports connect terminal operations, cargo handling, logistics, access management and external partners. In both settings, cybersecurity planning should map dependencies and include the operational teams responsible for keeping services running. These sector examples are contextual applications of the OT/ICS challenge; the conference transcript did not provide detailed case studies for every sector.

Across industrial environments, several priorities recur: build and maintain an inventory of OT assets; map connections and critical dependencies; apply least-privilege access and carefully govern third-party connectivity; monitor for anomalous activity; and prepare safe response options in advance. Asset isolation, patching and recovery cannot be treated as purely technical choices when they may affect physical processes.

> ***"Critical infrastructure resilience depends on connecting security insight to operational context—so that every access decision strengthens continuity rather than creating another blind spot. That requires security teams to understand how systems support physical operations, which dependencies are essential, and what consequences may follow from containment. When cybersecurity and operational teams make decisions together, organizations can reduce risk without compromising safety or availability."***
>
> **— Pranav Sahai, Industry Analyst, Global Security and AI, Frost & Sullivan**

Readiness must also be demonstrated, not assumed. Cyber ranges, tabletop exercises and scenario-based drills can test how security teams, engineers and business leaders respond when telemetry disappears, a workstation is suspected of compromise, or an essential service becomes unavailable. As Anand's distinction between certification and drills suggests, theoretical knowledge does not automatically translate into operational performance.

Securing the industrial backbone requires a partnership between cybersecurity specialists and the people who understand the process of being protected. The objective is not to pursue security at the expense of operations, but to make security decisions that preserve safety, continuity and recoverability. OT/ICS protection is strongest when technical controls, engineering judgment and tested response plans are designed together.

Turning India's Critical Infrastructure Cybersecurity Policy into Practice

India's critical infrastructure cybersecurity challenge is partly a policy question and partly an implementation question. National directions and sector guidance can define responsibilities, encourage timely reporting and establish a baseline for security practices. Their value, however, depends on whether organizations can translate those expectations into everyday controls, clear ownership and a response capability that works during a real incident.

The Indian Computer Emergency Response Team (CERT-In), operating under the Ministry of Electronics and Information Technology, issued directions under Section 70B of the Information Technology Act on 28 April 2022 [1] . These directions include requirements relating to reporting specified cyber incidents, maintaining relevant logs, and time synchronization. Organizations should consult the current official directions and associated guidance to confirm which obligations apply to them and how requirements should be implemented. Critical information infrastructure also has a dedicated institutional context through the National Critical Information Infrastructure Protection Centre (NCIIPC).

The practical task is to make compliance operational. Incident reporting is difficult if an organization has not defined who can declare an incident, who gathers evidence, who contacts the appropriate authority and who coordinates with business or plant operations. Log retention is less useful if logs are incomplete, clocks are inconsistent or responders cannot access the evidence when needed. Policy implementation therefore depends on preparation before an incident occurs.

Lt. General Dr. Rajesh Pant, Chairman, Cybersecurity Association of India framed the distinction clearly:

> ***"You cannot stop the cyber-attacks. You must create resilience. The objective is to coordinate across sectors, absorb disruption, recover essential services, and continuously strengthen national cyber preparedness. This requires information sharing, clear institutional roles, and regular exercises that connect government, industry, and operators. A resilient ecosystem is one that adapts after each incident rather than returning unchanged to business as usual."***
>
> **— Lt. General Dr. Rajesh Pant, Chairman, Cybersecurity Association of India**

For critical infrastructure, this means testing whether prescribed processes can support actual response and recovery. A plan should specify decision rights, escalation routes, communication responsibilities and recovery priorities. Exercises can expose gaps that documentation alone may not reveal, including unclear ownership between IT and OT teams or uncertainty about when a system can safely be disconnected.

OT and ICS environments make implementation especially demanding. Industrial assets may have long lifecycles, limited maintenance windows and direct consequences for physical operations. Organizations need to interpret security requirements in ways that account for safety and availability while still addressing visibility, access, monitoring and recovery. Col. Alok Shankar Pandey of DFCCIL warned that although some events may be unlikely, their impact can be very high. That is a reason to plan proportionately for consequences, not to rely on probability alone.

AI introduces another governance challenge. Automated detection and response may help organizations keep pace with faster threats, but they also create questions about oversight, accountability and the conditions under which systems may take action. Organizations should document where AI is used,

[1] CERT-In, Directions under Section 70B
https://www.cert-in.org.in/Directions70B.jsp

evaluate its performance, maintain appropriate human review and ensure that response decisions can be examined after an event. Policy and governance need to support responsible adoption without assuming that automation removes the need for skilled operators.

Skills form the bridge between written requirements and effective security. Training should include practical drills, incident simulations and cross-functional exercises, not only awareness sessions or certification. Senior leaders need to understand their role in decisions about service disruption, public communication and recovery. Technical teams need to know how to preserve evidence and coordinate with engineering teams. Suppliers and smaller partners may also need clear expectations where their access or systems form part of a critical service.

A more practical approach to policy execution combines four elements: clear accountability; a current understanding of assets and dependencies; repeatable incident-reporting and response procedures; and exercises that test recovery under realistic conditions. Regulators and organizations each have a role: policy can establish expectations and coordination mechanisms, while operators must turn those expectations into demonstrable capability.

India's critical infrastructure security will not be measured not only by rules, audits and security products, but also by whether organizations can detect a disruption, coordinate decisions, report incidents appropriately and restore essential services. Policy creates the greatest value when it enables demonstrable operational resilience and when implementation experience continuously strengthens controls and guidance.

Editorial note:

This combined draft draws on the supplied CyberSec Delhi Conference post-show interview transcript and the three agreed editorial angles. The OT/ICS section uses manufacturing, aviation and maritime examples as sector context because the transcript does not provide detailed case studies for each sector. Before publication, verify all speaker quotations and titles against the original audio and event materials, and validate policy references against current official CERT-In and NCIIPC sources.

Reference links for editorial verification

- CyberSec India Expo — official event page: https://cybersecindiaexpo.com/
- CyberSec India Expo — conference agenda: https://www.cybersecindiaexpo.com/conference_agenda
- CERT-In — Directions under Section 70B: https://www.cert-in.org.in/Directions70B.jsp
- CERT-In — Guidelines repository: https://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIE