TECHGUARD LABS FOUNDATION

Telecom Cybersecurity

Israel-India TelGuard · Coimbatore, Tamil Nadu

~132,000

DDoS attacks hit Indian telecom in H2 2025

Wired and Wireless carriers ranked #1 and #2 most-targeted sectors nationally. (NETSCOUT India DDoS Threat Intelligence, Jul–Dec 2025)

6 hours

To file an initial security incident report

Under Telecom Cyber Security Rules 2024 (Rule 7) (Department of Telecommunications, India 2024)

Mandatory

Audit trails, SOC coverage, and log retention

are now baseline compliance requirements under Telecom Cyber Security Rules 2024. (Department of Telecommunications, India 2024)

TECHGUARD TELGUARD

Network Security Architecture & Segmentation

✓ *Critical asset map; Trust-zone and segmentation matrix; Exposure register; VAPT remediation roadmap*

Threat-led review of telecom network layers: internet edge, peering/transit, DNS, CGNAT/BNG, packet/core network, OSS/BSS, NOC/SOC, customer portals, corporate IT and vendor access. We map trust zones, admin paths and lateral-movement routes that could turn one compromised system into a customer-impacting outage.

Incident Response Playbooks

✓ *Incident playbooks · Regulatory reporting pack · Evidence templates · Post-incident forensic checklist*

Telecom-specific IR workflows for DDoS, DNS compromise, route leak/hijack, OSS/BSS exposure, vendor compromise, credential abuse and customer-data incidents. Built to support fast internal escalation and 6-hour / 24-hour regulatory reporting evidence.

DDoS Readiness Program

✓ *DDoS risk register; Scrubbing & upstream escalation playbook; Tabletop exercise report; 24/7 contact tree*

Practical readiness review for volumetric, protocol and application-layer attacks against public websites, DNS, customer portals, APIs, service platforms and peering/transit links. Includes attack-surface review, capacity model, scrubbing-provider coordination and tabletop simulation.

Core Network & Routing Monitoring

✓ *Monitoring coverage matrix; Log-source onboarding plan; BGP/DNS/DDoS/O&M use cases; Escalation runbook*

Assessment of whether your SOC/NOC can detect BGP anomalies, DNS abuse, DDoS onset, configuration drift, O&M changes, suspicious privileged access and blind spots in telecom logs.

Supply Chain & Vendor Assurance

✓ *Vendor risk scorecards; Remote-access inventory; Trusted-product evidence; Patch / EOL remediation tracker*

Structured due diligence over telecom equipment vendors, integrators, managed service providers, field-maintenance teams and remote-access channels. We identify vendor paths that can change live network configurations, access customer data or bypass standard controls.

Quick Self-Check

☐ Do you know which routers, DNS, BNG/CGNAT, firewalls, OSS/BSS, NMS and customer portals are internet-facing or partner-accessible?

☐ Have your DDoS playbooks been tested with your upstream carrier and NOC?

☐ Are all privileged O&M, vendor and emergency accounts named, MFA-protected, time-bound and fully logged?

☐ Can you produce an incident report in under 6 hours?

"No" = you have an open door

Why TechGuard

- **Israeli Battle-tested cyber methodologies**
  ERA IT Consulting & Audit (est. 2008) + Ariel University partnership
- **Local Coimbatore team**
  On-site delivery — no international consultant travel costs
- **Board-ready reporting —**
  Findings delivered in executive language; GRC posture mapped against DoT, TRAI, and CERT-In requirements.
- **Legal compliance**
  DPDP Act, and CERT-In compliance integrated into every engagement

What Happens Without Protection — Real India Cases

Hathway ISP | Dec 2023

Hundreds of gigabytes of data allegedly taken from Indian ISP/digital TV provider Hathway appeared on a hacking website; the breach exposed 4.7M unique email addresses, names, IP/physical addresses, phone numbers, password hashes and support ticket logs.

Entry: ISP customer/support data repository compromise.

BSNL Website DDoS | Apr 2025

BSNL's main website reportedly faced two consecutive DDoS attacks lasting more than 30 minutes, leaving the website inaccessible for several days and affecting bill payments, service requests and customer support.

Entry: Public web-front availability + DDoS escalation and resilience gaps.

Protect Service Continuity Before Attackers Disrupt It

techguardlabs.com · info@techguardlabs.com · Coimbatore, Tamil Nadu | Israel

Ariel University (Israel) | ERA IT Consulting & Audit | SNR Sons Charitable Trust | SREC | Promitei Ltd