

Codec Networks

Coding Threats. Decoding Solutions.

LOGISTICS, WAREHOUSING & SUPPLY CHAINS

Keep the Cargo Moving. Keep the Platform Trusted.

Fleet and IoT security, partner API testing, warehouse OT assurance, SOC and continuity planning for logistics, warehousing and supply chain companies

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

CERT-In, DPDP, SEBI, NCIIPC and the shipper, GST and transport rules that reach logistics



How Codec Networks helps

Services, bundles and packages built for the sector



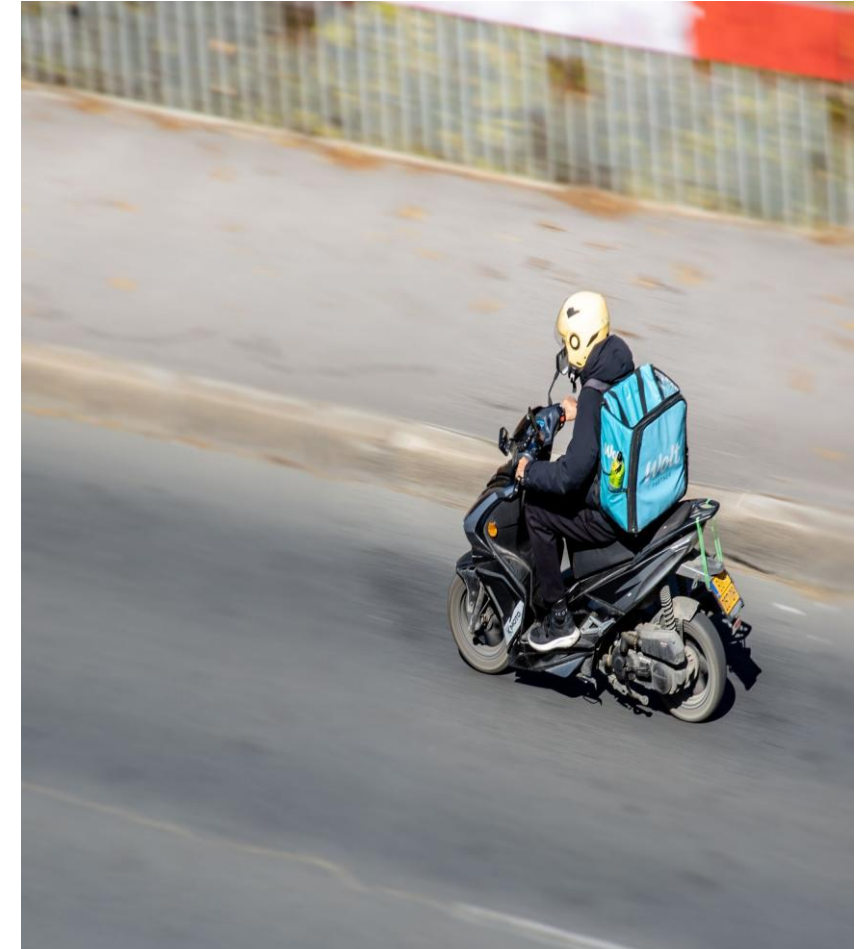
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Cyber incidents in logistics stop cargo

Global incidents and Indian scale show the operational stakes

7.97%

Of GDP: India's logistics cost in
FY24 (DPIIT–NCAER)

US\$250–300 m

Maersk's loss from NotPetya in
2017

US\$60 m

Expeditors' demurrage and
recovery costs after its 2022
attack

6 hours

To report cyber incidents to
CERT-In

What this means: logistics companies must make TMS, WMS and customs filing recoverable, control partner APIs and vendor access, secure fleets and warehouse automation, protect consignee data under DPDP, monitor around the clock and report incidents within six hours.

Sources: DPIIT–NCAER logistics cost study 2025, Maersk and Expeditors statements, public reporting, CERT-In.

Who we serve across logistics and supply chains



3PL and 4PL providers

Contract logistics, control towers



Express and courier companies

Parcels, sortation hubs, last mile



Freight forwarders and customs brokers

Ocean, air, customs filings



Trucking and fleet operators

Line-haul, telematics, FASTag



Warehouse and fulfillment operators

WMS, automation, Grade A parks



Cold storage and cold chain

Temperature-controlled logistics



Supply-chain platforms

Aggregators, visibility, freight tech



Last-mile and hyperlocal delivery

Rider fleets, PUDO, OTP delivery

The threats that cost logistics companies the most

Six priorities from our 18-threat logistics assessment



Ransomware shutdowns

TMS, WMS and customs filing encrypted



Freight payment fraud

BEC and changed bank accounts



Partner API and EDI abuse

Keys, enumeration, consignee data



Fleet and telematics compromise

Tracking, commands and cargo theft



Warehouse OT and vendor access

Flat networks, standing VPNs



Slow detection & reporting

Missing the 6-hour window

Attacks target every leg from booking to delivery

Where Cyber Risk Sits Across the Logistics Value Chain

Every leg from booking to delivery carries its own attack surface



In logistics, a day of platform downtime is cargo stuck at ports and hubs—and a leaked consignee file is a scam campaign against your customers.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, DPDP, SEBI, NCIIPC and the shipper, GST and transport rules that reach logistics

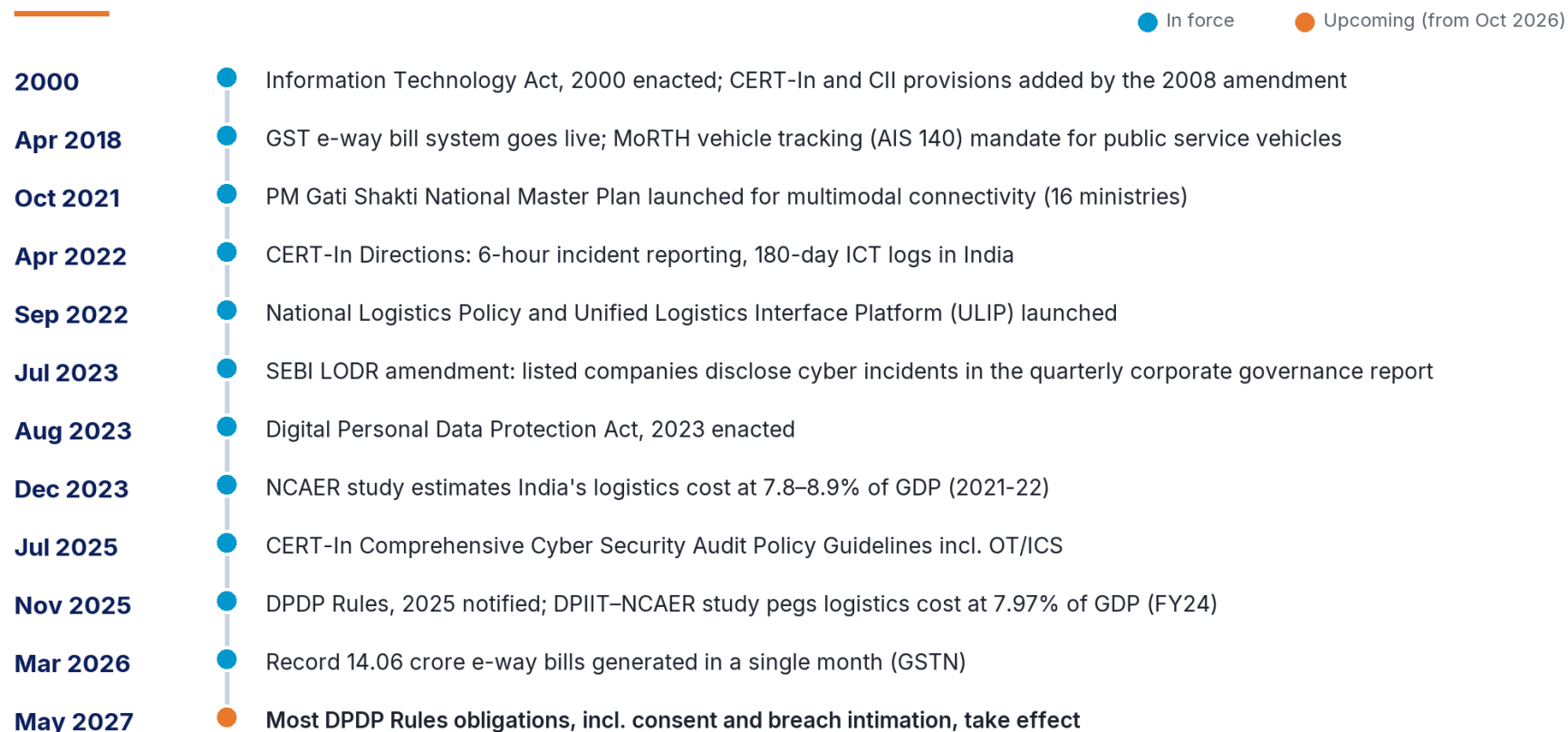
The rules and expectations shaping logistics cybersecurity

Requirement	Frequency / deadline	Source
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
ICT log retention	180 days, in India	CERT-In Directions, 2022
Independent cyber audits	Risk-based, incl. OT/ICS and cloud	CERT-In audit guidelines, 2025
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023
Protected systems in transport	Per notification	NCIIPC (IT Act Section 70A)
Consignee, driver and employee data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Vehicle location tracking devices	Per MoRTH notifications	AIS 140; Motor Vehicles Act rules
E-way bill and customs filing integrity	Ongoing	GST and Customs Acts; GSTN, ICEGATE
Shipper and customer security requirements	Per contract	Questionnaires, NIS2 flow-down, ISO/IEC 27001

Key dates on the regulatory timeline

Regulatory and Policy Timeline Shaping Logistics Cybersecurity

Cross-sector cyber instruments, logistics policy and the digital platforms the sector now depends on



Sources: MeitY, CERT-In, DPIIT Logistics Division, MoRTH, GSTN, NCAER, SEBI. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Fleet & IoT · Partner APIs · Warehouse OT · Logistics SOC · Continuity · Supply-Chain Risk

One partner from booking to delivery



Fleet & IoT Security

Telematics, driver apps, FASTag, commands



Partner API Testing

Shipper, carrier and merchant APIs, EDI, portals



Warehouse OT Assurance

WMS, AS/RS, sorters, PLCs, vendor access



24/7 Logistics SOC

Platform, hub, fleet and mailbox monitoring



Continuity & Recovery

Backups, playbooks, exercises



Supply-Chain Risk & Privacy

SaaS and vendor risk, DPDP, questionnaires

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

Regional fleets, warehouses and forwarders

- Platform and network assessment (B1)
- Email, BEC and payment control review (B3, B10)
- Backup and recovery review (B3)
- Policy and questionnaire pack (B5)

Assurance

National 3PLs, couriers and multi-site operators

- Annual VAPT of portals, APIs and apps (B1, B2)
- Warehouse OT and vendor access review (B1, B9)
- Independent audit and ISO 27001 (B4, B5)
- 24x7 SOC with BEC and API monitoring (B7)

Continuous Resilience

Large integrated logistics groups and platforms

- Continuous testing and red teaming (B1, B10)
- Fleet, IoT and automation programme (B11, B3)
- SaaS and partner risk programme (B9)
- SOC with threat hunting and Board reporting (B7, B4)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Incidents to CERT-In in six hours; 180-day logs (CERT-In Directions)	SOC, IR retainer and reporting support	B7, B8
Independent cyber audits incl. OT and cloud (CERT-In guidelines, 2025)	Independent IT/OT audits	B4, B1
Consignee, driver and employee personal data (DPDP)	DPDPA programme	B6
Quarterly incident disclosure, listed companies (SEBI LODR)	Incident records, disclosure support	B4, B8
Vehicle tracking devices and data (MoRTH AIS 140 notifications)	Telematics and VLT security review	B1, B11
E-way bill, GST and customs filing integrity (GSTN, ICEGATE)	Credential, access and filing controls	B3, B7
Shipper security requirements (contracts, NIS2 flow-down)	ISO 27001 and questionnaire readiness	B5, B9

Five new case studies, five broken chains

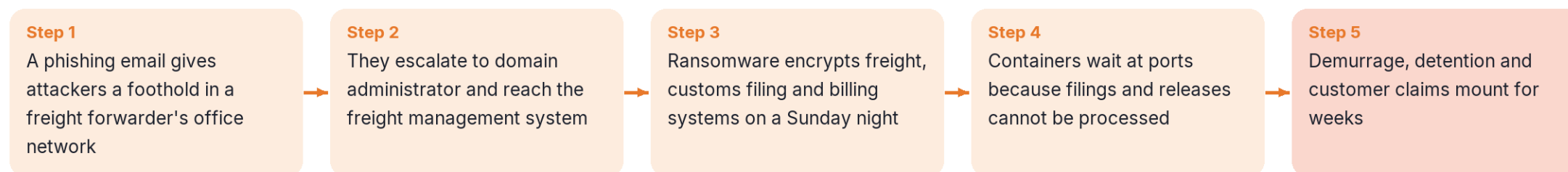
Illustrative composite scenarios written for 2026—not client engagements

1	The Forwarder That Went Dark	Ransomware encrypts freight and customs systems; segmentation, backups and SOC keep cargo moving	B3 · B7 · B8
2	The Bank Account That Changed	A hijacked mailbox diverts shippers' freight payments; MFA, monitoring and call-backs stop it	B10 · B7 · B3
3	The API Key in the Tracking Widget	A leaked merchant key exposes millions of consignees; API testing and monitoring prevent it	B2 · B7 · B6
4	The Warehouse That Stopped Picking	A vendor VPN and flat network halt sorters and WMS; segmentation and brokered access contain it	B1 · B3 · B9
5	The Fleet That Could Be Seen by Everyone	Default telematics credentials enable cargo theft; IoT assessment and access controls prevent it	B11 · B1 · B7

Example: breaking a forwarder ransomware chain

Case 1: The Forwarder That Went Dark

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: which operations depend on the freight system, customs filing and billing, segmentation between office IT and operational platforms, immutable backups and restore times, EDR and SOC detection of privilege escalation, and crisis decision-making in a tabletop exercise with operations leadership.

Why logistics companies choose Codec Networks



CERT-In empanelled

For information security auditing services; NISCI empanelled for application audits



Certified

ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 20000-1:2018



Regulation-mapped

Mapped to ISO/IEC 27001, IEC 62443, OWASP, CERT-In expectations, DPDP and your shippers' requirements



Tests the whole chain

Technical, process and monitoring tests together



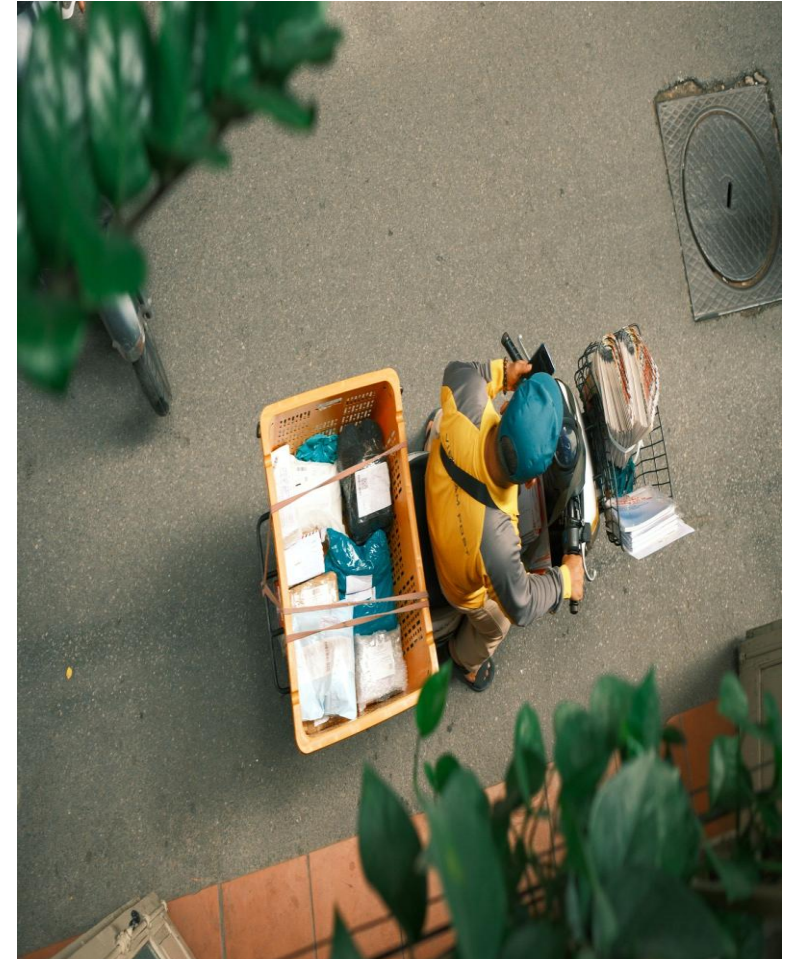
Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected



Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST



How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement



Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Platforms, portals and APIs, hubs and warehouses, automation vendors, fleets and telematics, critical partners and your peak-season and audit calendar

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

 New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001

 Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018

 011 430 496 96 · 011 437 522 99 · +91 99716 76124 · +91 88007 88220 · +91 88003 31124

 mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities.