

Codec Networks

Coding Threats. Decoding Solutions.

FMCG, FOOD & BEVERAGES

Keep the Lines Filling. Keep the Shelves Full.

Plant OT security, distributor portals, supply chain assessments, SOC and resilience for consumer goods groups, food processors, beverage companies, dairies, cold-chain operators and distributor networks

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, SEBI, DPDP, FSSAI and the consumer and retailer rules that reach FMCG companies



How Codec Networks helps

Services, bundles and packages built for the sector



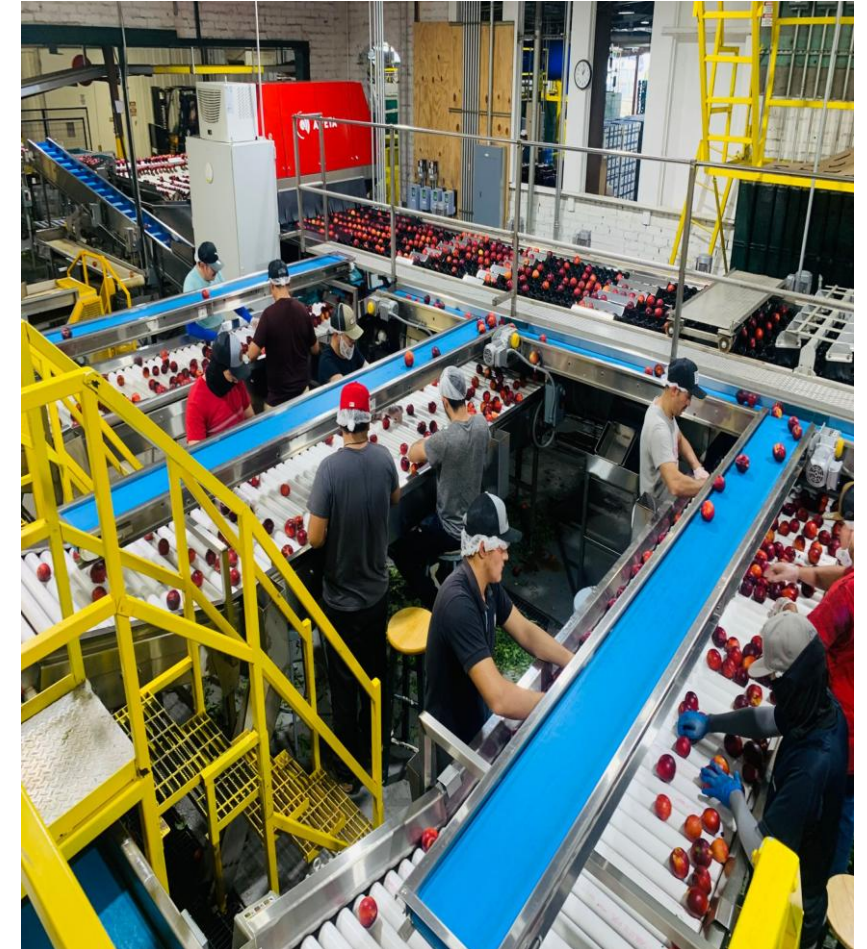
Proof in scenarios

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 FMCG and food empty shelves

Global incidents and India's scale show the commercial stakes

US\$11 m

Ransom JBS paid after plants
were halted (2021)

US\$49 m

Clorox's 2023 cyberattack costs,
with product shortages

~25%

Of the world's milk is produced
in India

6 hours

To report cyber incidents to
CERT-In

What this means: consumer goods companies must separate plants from IT, make ERP and order processing recoverable, secure distributor portals and schemes, assure co-packers and cold-chain partners, protect consumer data, monitor around the clock and report incidents within six hours.

Sources: JBS USA statement (June 2021), Clorox SEC filings (2023-24), Ministry of Fisheries, Animal Husbandry and Dairying, CERT-In.

Who we serve across FMCG, food and beverages



Consumer goods groups

Home, personal care and packaged foods



Food processors

Snacks, staples, ready meals, meat and seafood



Beverage companies

Soft drinks, juices, water, brewing, spirits



Dairies and cooperatives

Milk collection, processing, chilled products



Cold-chain and warehouse operators

Cold storage, refrigerated transport, 3PLs



Distributor networks

Distributors, stockists, sales agents, DMS



D2C and quick-commerce channels

Brand apps, loyalty, marketplaces



Listed FMCG groups

Multi-plant groups with SEBI obligations

The threats that cost consumer goods companies the most

Six priorities from our 18-threat FMCG, food and beverage assessment



Ransomware shutdowns

ERP, orders and plants stopped



Distributor scheme fraud

Portals and claims abused for payouts



Plant OT compromise

PLCs, lines and recipes reached from IT



Partner and cold-chain outages

3PLs and cold storage taken offline



Consumer data breaches

Loyalty apps and APIs leaking profiles



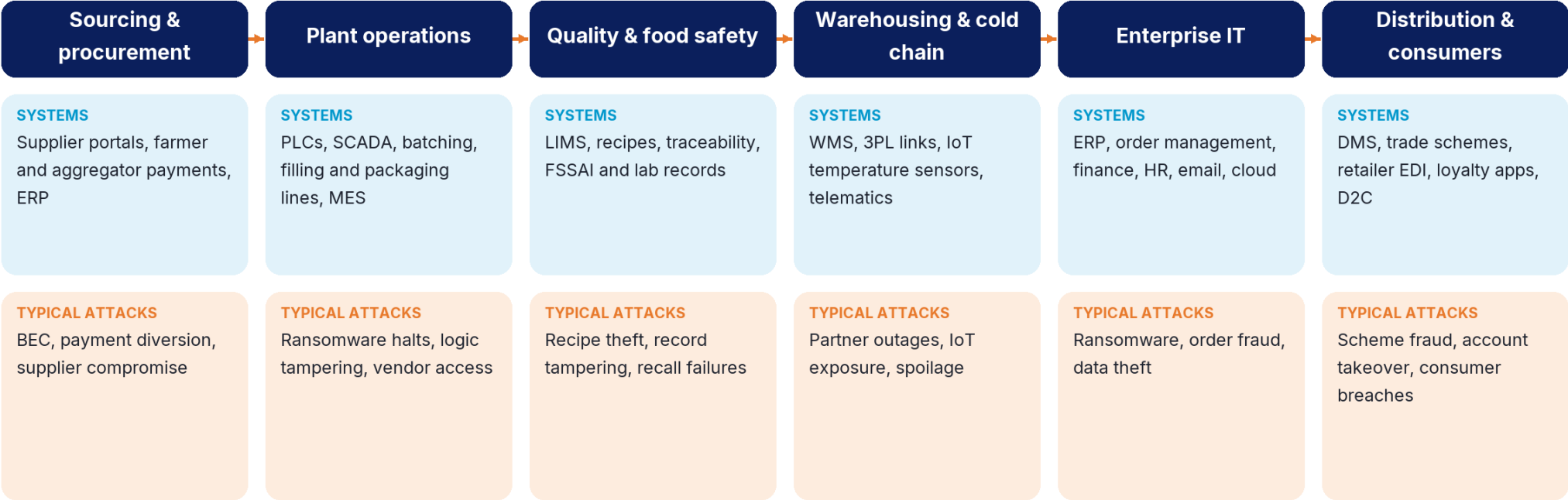
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from sourcing to the shelf

Where Cyber Risk Sits Across the FMCG, Food and Beverages Value Chain

Every stage from sourcing to the shelf carries its own attack surface



In FMCG and food, lost production is lost shelf space—and a tampered recipe, batch record or temperature log is a food safety event.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, SEBI, DPDP, FSSAI and the consumer and retailer rules that reach FMCG companies

The rules shaping FMCG, food and beverage 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	CERT-In audit guidelines, 2025
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023
Consumer, loyalty and worker data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Food safety licences, records and recalls	Continuous	FSS Act 2006; FSSAI; FoSCoS
Pack declarations	Continuous	Legal Metrology (Packaged Commodities) Rules 2011
GST e-invoicing	Turnover above ₹5 crore, since Aug 2023	CBIC notification 10/2023
Industrial security good practice	Standards	IEC 62443; ISO/IEC 27001

Key dates on the regulatory timeline

Regulatory and Policy Timeline Shaping FMCG, Food and Beverages Cybersecurity

Food safety and consumer statutes, sector schemes and the cross-sector Indian cyber instruments that reach FMCG companies

● In force

● Upcoming (from Oct 2026)

2000	● Information Technology Act, 2000; CERT-In and protected-system provisions added in 2008
2006	● Food Safety and Standards Act, 2006 enacted; FSSAI established under it
Apr 2011	● Legal Metrology (Packaged Commodities) Rules, 2011 govern declarations on consumer packs
Jun 2020	● FSSAI's Food Safety Compliance System (FoSCoS) begins replacing the old licensing portal
Mar 2021	● PLI scheme for food processing approved with a ₹10,900 crore outlay for 2021-22 to 2026-27
Apr 2022	● CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Jul 2023	● SEBI LODR amendment: listed companies disclose cyber incidents quarterly
Aug 2023	● GST e-invoicing mandatory above ₹5 crore turnover; DPDP Act enacted
Jul 2025	● CERT-In Comprehensive Cyber Security Audit Policy Guidelines, including OT/ICS
Nov 2025	● DPDP Rules, 2025 notified with phased commencement
May 2027	● Most DPDP Rules obligations, including breach intimation, take effect

Sources: FSSAI, Department of Consumer Affairs, MoFPI, CBIC, MeitY, CERT-In, SEBI. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Plant OT · Distributor portals · Supply chain · IT/OT SOC · Resilience · Consumer data

One partner from plant to shelf



Plant OT Security

PLCs, SCADA, batching, packaging lines



Distributor Portal Security

DMS, sales apps, claims, retailer APIs



Supply Chain Assessment

Co-packers, 3PLs, cold storage, agencies



24/7 IT/OT SOC

Plants, depots, cloud, fraud analytics



Resilience & Recovery

Backups, dispatch playbooks, exercises



Consumer Data & DPDP

Loyalty, D2C, CRM, app and API testing

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

Single plants, dairies and regional brands

- IT and plant assessment (B1)
- Backup and dispatch recovery review (B3)
- Email security and BEC controls (B3, B10)
- Policy and retailer evidence pack (B5)

Assurance

Multi-plant food and beverage companies

- IEC 62443 assessment and segmentation (B1, B3)
- DMS, app and API testing (B2)
- Annual independent audit (B4)
- 24x7 IT/OT SOC (B7)

Continuous Resilience

Listed FMCG groups and national brands

- Continuous OT and application testing (B1, B2)
- Supply chain and cold-chain assurance (B9)
- SOC with fraud and brand monitoring (B7)
- DPDP programme and Board reporting (B6, B4)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Cyber incidents to CERT-In within six hours; 180-day logs	IT/OT SOC, IR retainer and reporting support	B7, B8
Risk-based independent audits incl. OT (CERT-In guidelines 2025)	Independent IT/OT audits	B4, B1
Quarterly cyber incident disclosure by listed companies (SEBI)	Incident records, disclosure support	B4, B8
Consumer, loyalty, distributor and worker data (DPDP)	DPDPA programme	B6
Food safety records, traceability and recalls (FSS Act, FSSAI)	Record integrity and recall system reviews	B1, B5
Pack declarations and e-invoicing (Legal Metrology, GST)	Compliance system integrity controls	B3, B5
Retailer, co-packer and insurer security requirements	ISO 27001, IEC 62443 and evidence readiness	B5, B9

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1

The Plant That Ran Out of Labels

Ransomware stops an FMCG group's orders and labels; segmentation and tested backups keep shelves stocked

B3 · B7 · B8

2

The Scheme That Paid Itself

A distributor portal flaw inflates claims; API testing and analytics catch it

B2 · B9 · B7

3

The Chiller That Phoned Home

Cold-chain IoT reaches a dairy's pasteuriser HMIs; IoT assessment and segmentation prevent it

B11 · B3 · B1

4

The Aggregator Payments That Went Elsewhere

A phished mailbox diverts farmer payments; verification and monitoring stop it

B10 · B2 · B7

5

The Loyalty App That Leaked Its Customers

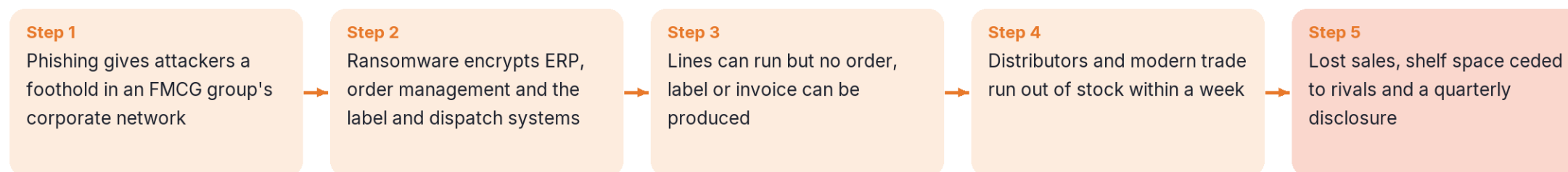
An exposed API leaks consumer profiles; app testing and DPDP controls prevent it

B2 · B6 · B9

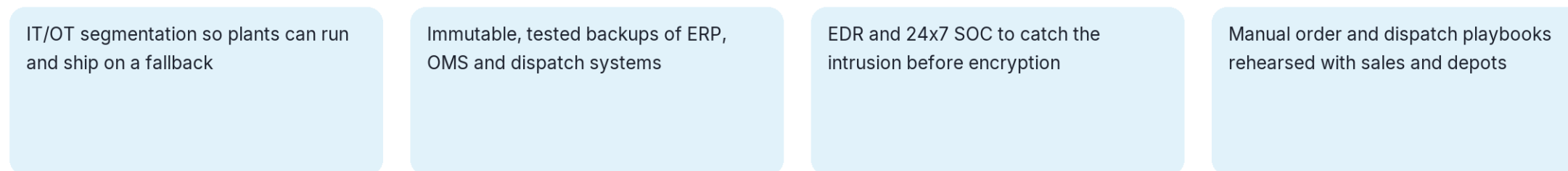
Example: breaking an ERP-to-shelf shutdown chain

Case 1: The Plant That Ran Out of Labels

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 order, label, dispatch and invoicing processes depend on ERP and order management, IT/OT segmentation between office, plant and depots, the ability to serve distributors without IT, immutable backups and restore times, EDR and SOC detection, and crisis decision-making in a tabletop exercise with sales, plant and supply chain leadership.

Why consumer goods companies choose Codec Networks



CERT-In empanelled

For information security auditing services; NISIR empanelled for application audits



Certified

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



Regulation-mapped

Mapped to IEC 62443, ISO/IEC 27001, CERT-In and DPDP expectations and your retailers' and insurers' 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

Plants and co-packers, PLCs and lines, ERP and order management, distributor platforms, cold-chain partners, consumer data and your 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.