Codec Networks

Coding Threats. Decoding Solutions.

TEXTILES, APPAREL & CONSUMER MANUFACTURING

Ship Every Season. Keep Every Design.

ERP and e-commerce security, IP protection, SOC, privacy and supplier assurance for textile mills, garment and footwear exporters, consumer products manufacturers and brand owners

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, GST and product rules, and the buyer requirements that reach Indian factories

How Codec Networks helps

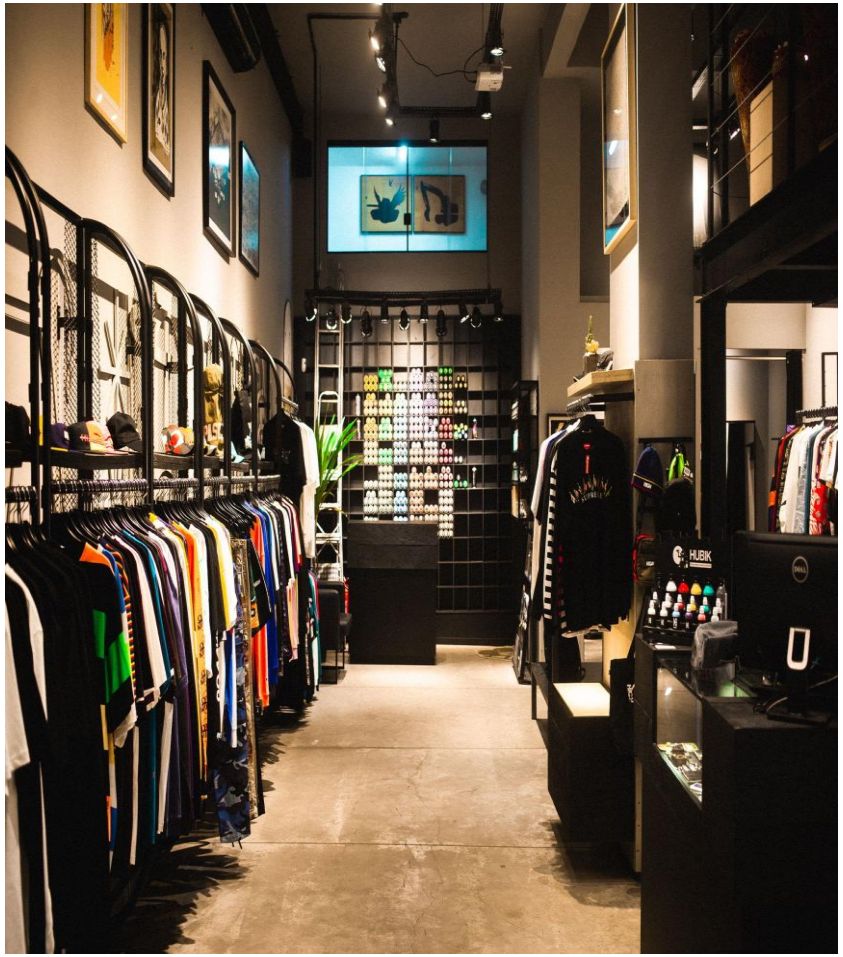
Services, bundles and packages built for the sector

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 apparel and consumer goods cost seasons

Global incidents and India's scale show the commercial stakes

35.5 mn

Consumers affected by VF Corp's December 2023 incident

US$100 m

Sales Hanesbrands lost to ransomware in one quarter (2022)

45 mn+

People directly employed in India's textile sector

6 hours

To report cyber incidents to CERT-In

What this means: manufacturers and brands must make ERP and shipping recoverable, stop payment diversion, protect designs, secure D2C sites and consumer data, assure suppliers and buyers, monitor around the clock and report incidents within six hours.

Sources: VF Corporation Form 8-K/A (2024), Hanesbrands Q2 2022 results, Ministry of Textiles, CERT-In.

Who we serve across textiles and consumer manufacturing

Spinning and weaving mills

Yarn, fabric, MMF and technical textiles

Processing and job-work units

Dyeing, printing, embroidery, finishing

Garment and home textile exporters

Apparel, made-ups, buyer-nominated supply

Footwear manufacturers

Leather and non-leather footwear

Consumer products manufacturers

Home, personal care and lifestyle goods

Brand owners and licensees

Design, sourcing, retail and wholesale

D2C and e-commerce arms

Brand sites, apps, marketplaces, loyalty

Listed textile and apparel groups

Multi-unit groups with SEBI obligations

The threats that cost manufacturers and brands the most

Six priorities from our 18-threat textiles and apparel assessment

Ransomware shutdowns

ERP, shipping and lines stopped in season

Payment diversion

Buyer and supplier BEC on export proceeds

Design and IP theft

Tech packs, lasts and costings copied out

D2C account takeover

Credential stuffing, skimming, loyalty fraud

Supplier and vendor breaches

Job-workers and service providers compromised

Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from design to the consumer

Where Cyber Risk Sits Across the Textiles, Apparel and Consumer Goods Value Chain

Every stage from design to the consumer carries its own attack surface

In apparel and consumer goods a season cannot be reshipped—a missed vessel date becomes air freight, discounts or a cancelled order.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, SEBI, DPDP, GST and product rules, and the buyer requirements that reach Indian factories

Codec Networks
Coding Threats. Decoding Solutions.

The rules shaping textiles and apparel 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	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
GST e-invoicing	Turnover above ₹5 crore, since Aug 2023	CBIC notification 10/2023
Product certification and labelling	Footwear QCOs from Aug 2024	BIS; Legal Metrology Rules 2011
Card payment security on D2C channels	Standard	PCI DSS v4.0.1
Connected consumer products	Reporting from Sep 2026; full from Dec 2027	EU Cyber Resilience Act

Key dates on the regulatory timeline

Regulatory and Policy Timeline Shaping Textiles and Apparel Cybersecurity

Sector schemes, consumer rules, cross-sector Indian cyber instruments and the buyer and export requirements that reach Indian factories

In force Upcoming (from Oct 2026)

2000	Information Technology Act, 2000; CERT-In and protected-system provisions added in 2008
Apr 2011	Legal Metrology (Packaged Commodities) Rules, 2011 govern declarations on consumer packs
Sep 2021	PLI scheme for textiles approved: ₹10,683 crore for MMF apparel, fabrics and technical textiles
2021	PM MITRA mega textile parks approved: seven sites with a ₹4,445 crore outlay
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
Aug 2024	BIS Quality Control Orders for footwear take effect, requiring ISI certification
Dec 2024	EU Cyber Resilience Act enters into force for connected consumer products
Jul 2025	CERT-In Comprehensive Cyber Security Audit Policy Guidelines
Nov 2025	DPDP Rules, 2025 notified with phased commencement
Sep 2026	EU CRA vulnerability and incident reporting duties apply to manufacturers
May 2027	**Most DPDP Rules obligations, including breach intimation, take effect**
Dec 2027	**EU CRA essential requirements and CE marking fully apply**

Sources: Ministry of Textiles, CBIC, BIS, MeitY, CERT-In, SEBI, EU Official Journal. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

ERP & e-commerce · IP protection · SOC · Privacy · Suppliers · Buyer readiness

Codec Networks
Coding Threats. Decoding Solutions.

One partner from design to doorstep

ERP & E-commerce Security

ERP, PLM, D2C sites, apps, buyer portals

IP Protection

Designs, tech packs, DLP, leaver controls

24/7 SOC

Plants, offices, cloud, fraud detection

Privacy & DPDP

Consumer, loyalty, worker data

Supplier Assurance

Job-workers, tier-2 suppliers, vendors

Buyer Questionnaire Readiness

ISO 27001, PCI DSS, evidence packs

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services

- **B1** Cyber Assessment & VAPT Assurance
- **B2** Application, API & DevSecOps Security
- **B3** Cloud, Infrastructure & Zero Trust
- **B4** Regulatory Cyber Audit & Compliance
- **B5** GRC, ISO, SOC 2 & PCI DSS Maturity
- **B6** Data Privacy & DPDPA Program
- **B7** Managed SOC, MDR & Threat Monitoring
- **B8** Forensics, Incident Response & Malware RCA
- **B9** Third-Party & Supply-Chain Risk
- **B10** Cyber Simulation, Awareness & Tabletop
- **B11** Emerging Tech, AI & Web3 Security

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

Mills, job-workers and single factories

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

Assurance

Exporters and multi-unit manufacturers

- ERP, PLM and portal testing (B2)
- IP protection programme (B3, B6)
- Annual independent audit (B4)
- 24x7 SOC (B7)

Continuous Resilience

Brand owners, listed groups and D2C businesses

- Continuous web, API and app testing (B2)
- Supplier assurance programme (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	SOC, IR retainer and reporting support	B7, B8
Risk-based independent cyber audits (CERT-In guidelines 2025)	Independent IT and plant audits	B4, B1
Quarterly cyber incident disclosure by listed companies (SEBI)	Incident records, disclosure support	B4, B8
Consumer, loyalty, employee and worker personal data (DPDP)	DPDPA programme	B6
Brand vendor codes and security questionnaires (buyer contracts)	ISO 27001 and questionnaire readiness	B5, B9
Card payments on D2C sites and apps (PCI DSS v4.0.1)	PCI DSS readiness and testing	B5, B2
Connected consumer product security (EU CRA, from Sep 2026)	Product and firmware security assessment	B2, B11

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Order Book That Went Dark Before the Vessel Sailed**	Ransomware stops an exporter's shipping documents; segmentation and tested backups keep goods moving	**B3 · B7 · B8**
2	**The Buyer Who Never Changed Banks**	A compromised mailbox diverts export proceeds; verification and monitoring stop it	**B10 · B2 · B7**
3	**The Sample Room That Lived on a Shared Drive**	A contractor downloads next season's designs; access reviews and DLP catch it	**B3 · B6 · B8**
4	**The D2C Site That Accepted Everyone's Passwords**	Credential stuffing and skimming hit a brand site; testing and bot controls prevent it	**B2 · B6 · B7**
5	**The Dyehouse That Stopped Three Factories**	A job-worker's ransomware starves garment units; supplier assurance and buffers prevent it	**B9 · B10 · B7**

Example: breaking an ERP-to-shipment shutdown chain

Case 1: The Order Book That Went Dark Before the Vessel Sailed

ILLUSTRATIVE ATTACK PATH

Step 1
Phishing gives attackers a foothold in a garment exporter's network

→

Step 2
Ransomware encrypts ERP, the cutting-room system and shipping documents

→

Step 3
Lines keep sewing but packing lists, invoices and e-way bills cannot be issued

→

Step 4
The season's largest order misses its vessel and goes by air at the exporter's cost

→

Step 5
Buyer penalties, air freight and a vendor-status review by the brand

WHERE CONTROLS BREAK THE CHAIN

- Segmentation so production and dispatch survive an IT outage
- Immutable, tested backups of ERP, PLM and export documents
- EDR and 24x7 SOC to catch the intrusion before encryption
- Manual shipping playbooks rehearsed with merchandising and logistics

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

Codec Networks

What we test: which packing, invoicing, e-invoicing and export document processes depend on ERP, segmentation between office, plant and cloud, the ability to ship without IT, immutable backups and restore times, EDR and SOC detection, and crisis decision-making in a tabletop exercise with merchandising and logistics leadership.

Why manufacturers and brands choose Codec Networks

CERT-In empanelled

For information security auditing services; NICSI empanelled for application audits

Certified

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

Regulation-mapped

Mapped to ISO/IEC 27001, PCI DSS, CERT-In and DPDP expectations and your buyers' security questionnaires

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 MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Units, ERP, PLM and e-commerce platforms, buyers and their requirements, job-workers and suppliers, consumer data and your audit and shipment 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.

Codec Networks
Coding Threats. Decoding Solutions.