

Codec Networks

Coding Threats. Decoding Solutions.

CONGLOMERATES, HOLDING COMPANIES &
INVESTMENT GROUPS

Secure the Group. Protect Every Deal.

Group cyber governance, M&A due diligence, shared SOC, portfolio assessments and Board reporting for conglomerates, holding companies and investment groups

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

Companies Act, SEBI LODR, CSCRF and PIT, RBI CIC rules, CERT-In and DPDP



How Codec Networks helps

Services, bundles and packages built for the sector



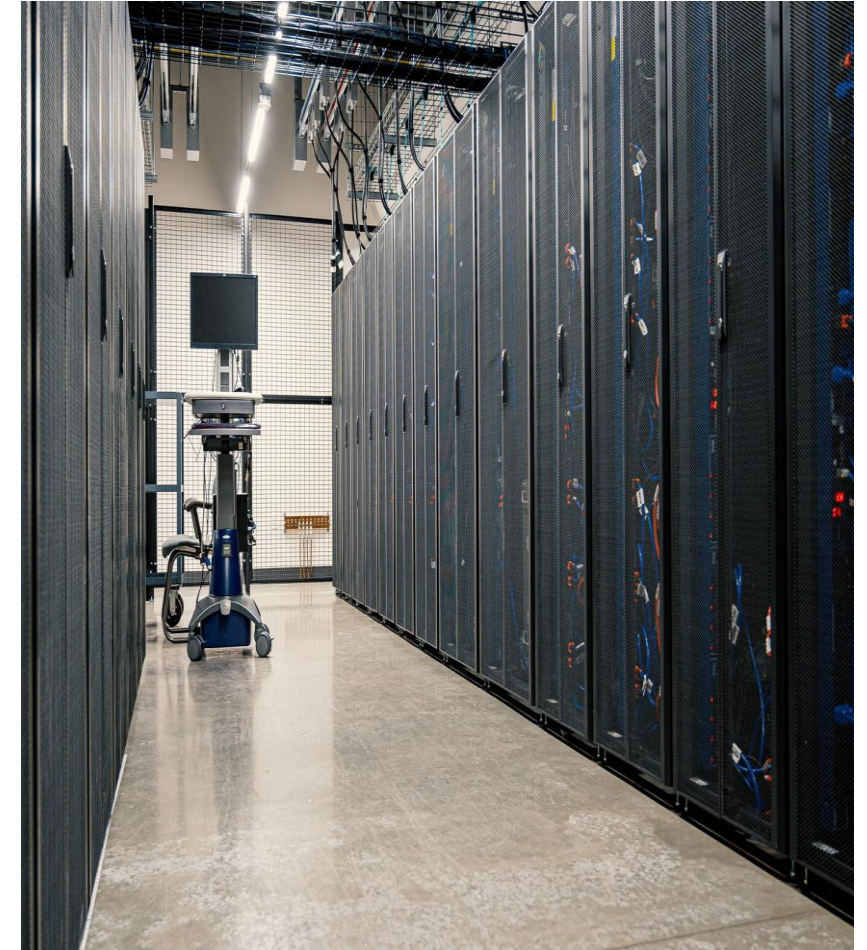
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Group structures concentrate cyber risk, and so do deals

Public figures show what is at stake when one entity or one deal fails

£1.9 bn

UK impact of the 2025 JLR attack
(CMC estimate)

US\$350 m

Cut in Verizon's Yahoo price after
breaches (2017)

~US\$36 bn

PE-VC investment in India in
2025 (Bain)

6 hours

To report cyber incidents to
CERT-In

What this means: Business groups, holding companies, CICs, family offices and PE and VC firms must set one cyber standard for every entity, secure shared directories, ERP and shared services, run cyber due diligence before every deal, assess and monitor portfolio companies, protect treasury from deepfake and email fraud, give the Board and risk committee a group-wide view and report incidents to CERT-In within six hours.

Sources: UK Cyber Monitoring Centre (October 2025), Verizon and Yahoo (February 2017), Bain & Company India Private Equity Report 2026, CERT-In Directions (2022).

Who we serve across groups and investment firms



Business groups

Diversified, multi-sector groups



Holdcos

Listed parents and holding companies



CICs

Core investment cos with RBI



Family offices

Single and multi-family offices



Private equity

Buyout and growth funds



Venture capital

VC funds and accelerators



Portfolio cos

Investees and group businesses



Shared services

Group IT, finance and HR centres

The threats that cost groups and investors the most

Six priorities from our 18-threat group and investment assessment



Subsidiary ransomware

Spread through shared IT



Inherited breaches

Attackers inside before close



Deepfake payment fraud

CEO, CFO and promoter fakes



Deal data leaks

Data rooms, UPSI, advisers



Shared identity abuse

One directory, many companies



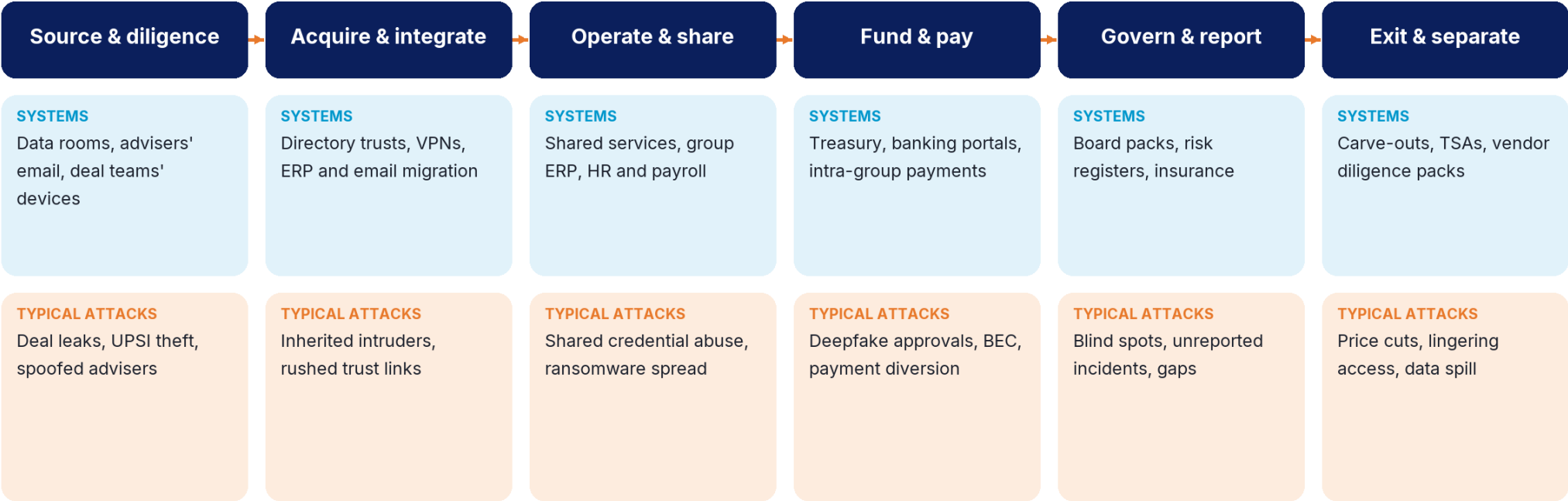
Uneven maturity

The weakest entity sets risk

Attacks target every step from deal to exit

Where Cyber Risk Sits Across the Group and Investment Lifecycle

Every step from first look at a target to exit carries its own attack surface



A group is only as secure as its weakest company: one shared directory, treasury approval or unchecked acquisition can expose every entity and every investor.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

Companies Act, SEBI LODR, CSCRf and PIT, RBI CIC rules, CERT-In and DPDP

The rules shaping group and investment firm security

Requirement	Frequency / deadline	Source
Board risk duties	Risk policy statement in Board's report	Companies Act 2013, s.134(3)(n)
Risk management committee	Role to cover cyber security; top 1,000	SEBI LODR Regulation 21
Cyber incident disclosure	In quarterly governance reports	SEBI LODR Reg 27(2)(ba)
Price-sensitive deal data	Structured digital database, controls	SEBI PIT Regulations 2015
Fund and portfolio managers	Cyber resilience by entity category	SEBI CSCRF, Aug 2024
Core investment companies	Group risk committee; CRO if large	RBI CIC directions, 2020
Cyber incident reporting	To CERT-In within 6 hours; 180-day logs	CERT-In Directions, 2022
Independent audits	Risk-based audits, including OT and ICS	CERT-In guidelines, Jul 2025
Personal data in the group	Safeguards and breach intimation	DPDP Act 2023; Rules 2025

Key dates on the regulatory timeline

Legal and Regulatory Timeline Shaping Group and Investment Firm Security

Board duty, market, fund, data and incident milestones that reach holding companies, CICs, family offices, funds and their group and portfolio companies

● In force

● Upcoming (from Oct 2026)

Aug 2013	● Companies Act 2013 enacted: Board risk policy statement and independent director duties
Sep 2016	● Marriott completes its Starwood purchase; a breach in Starwood's systems dated from 2014
Feb 2017	● Verizon cuts its price for Yahoo by US\$350 million after breach disclosures
Jun 2017	● NotPetya hits Maersk, Mondelez and other multinationals across group networks
Aug 2020	● RBI revises CIC framework: group risk committee, CRO for CICs over ₹5,000 crore
May 2021	● SEBI extends the risk management committee rule to the top 1,000 listed entities
Apr 2022	● CERT-In Directions: 6-hour incident reporting and 180-day ICT logs kept in India
Jul 2023	● Listed entities begin disclosing cyber incidents in quarterly governance reports
Aug 2023	● Digital Personal Data Protection Act 2023 enacted
Aug 2024	● SEBI issues CSCRF, covering regulated entities incl. AIF and portfolio managers
Jul 2025	● CERT-In Comprehensive Cyber Security Audit Policy Guidelines, including OT and ICS
Sep 2025	● Cyber attack halts JLR's UK car production; CMC later estimates £1.9 billion UK impact
Nov 2025	● DPDP Rules notified
May 2027	● Most DPDP Rules obligations, incl. security safeguards and breach intimation, apply

Sources: MCA, SEBI, RBI, CERT-In, MeitY, UK Cyber Monitoring Centre, company statements and widely reported events. Confirm against the official instruments.

Codec Networks

How Codec Networks helps

Governance · Due diligence · Shared SOC · Portfolio · Identity & payments · Board

One partner from deal room to Board room



Group Cyber Governance

Standard, scoring, roles



M&A Due Diligence

Pre-signing to Day 100



Shared SOC

One SOC for every entity



Portfolio Assessments

Baseline, benchmark, exit



Identity & Payments

Directories, treasury, BEC



Board Reporting

Metrics, exercises, insurance

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

Family offices and VC funds

- Treasury and payment control review (B10)
- Deepfake and BEC awareness (B10)
- Investee cyber baseline (B5)
- IR retainer (B8)

Assurance

PE funds and acquisition platforms

- M&A cyber due diligence (B1, B9)
- Compromise assessment before close (B8)
- Portfolio maturity scoring (B5)
- Portfolio SOC (B7)

Continuous Resilience

Diversified groups and holdcos

- Group cyber standard and scoring (B5)
- Shared directory and cloud review (B3)
- CERT-In empanelled audits (B4)
- Shared 24x7 SOC (B7)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Risk policy statement in the Board's report (Companies Act)	Group cyber risk assessment	B5, B4
Risk committee role covering cyber security (SEBI LODR Reg 21)	Board and RMC cyber reporting	B5, B10
Cyber incidents in quarterly governance report (SEBI LODR)	Incident records and SOC evidence	B7, B8
Incidents to CERT-In in six hours; 180-day logs (CERT-In)	Shared SOC, IR retainer	B7, B8
Cyber resilience for AIF and portfolio managers (SEBI CSCRF)	CSCRF gap review and audit	B4
Tamper-proof records of who holds UPSI (SEBI PIT Regulations)	Deal data and database review	B2, B3
Safeguards and breach intimation for group data (DPDP Act)	Group DPDPA programme	B6

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1

The Subsidiary That Took the Group Down

An acquired firm's VPN lets ransomware reach a shared group ERP; MFA and tiered admin stop it

B3 · B7 · B8

2

The Breach That Came With the Deal

An intruder inside a target stays after closing; diligence and a compromise check find it first

B1 · B9 · B8

3

The Promoter's Voice on the Call

A deepfake call approves transfers from a family office; call-backs and dual approval stop it

B10 · B7 · B8

4

The Portfolio Nobody Measured

Ransomware at one investee cuts an exit price; a portfolio baseline and SOC prevent it

B5 · B1 · B7

5

The Shared Services Login

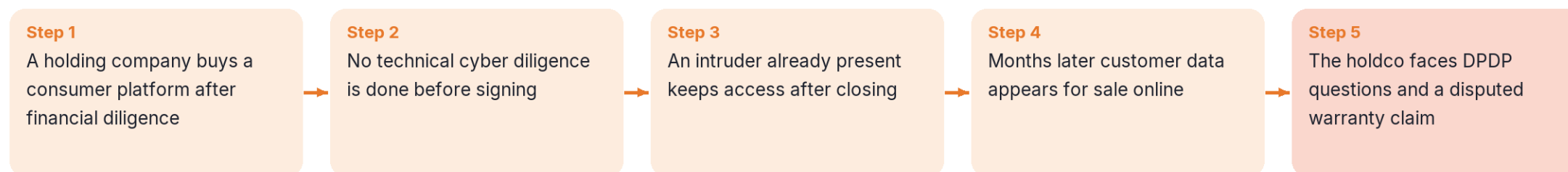
A vendor admin login exposes HR data for 20 group firms; MFA and PAM prevent it

B3 · B9 · B6

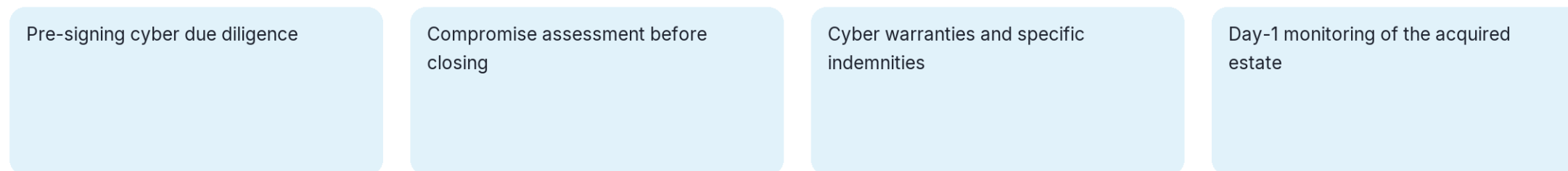
Example: finding the intruder before closing

Case 2: The Breach That Came With the Deal

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: the target's external exposure and leaked credentials, identity and privileged access, signs of existing compromise on endpoints, servers and cloud, data stores holding personal data, backups and recovery, past incidents and disclosures, and the warranties, indemnities and Day-1 monitoring the buyer needs before it connects the target to the group.

Why groups and investment firms 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 the Companies Act, SEBI LODR, the PIT Regulations and CSCRF, RBI's CIC directions, CERT-In Directions and audit guidelines, the IT Act and DPDP



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

Group structure and shared services, directories and cloud tenants, treasury and payment flows, deal pipeline and data rooms, acquisitions, portfolio companies, suppliers, Board reporting, insurance, group data

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.