

Codec Networks

Coding Threats. Decoding Solutions.

PROFESSIONAL & BUSINESS SERVICES

Protect the Client. Protect the File. Protect the Firm.

Confidential data protection, email and cloud security, privacy, managed SOC and fraud investigations for professional and business services firms

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, confidentiality duties, and RBI, SEBI and client expectations



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



Professional services are a high-value, high-trust target

Public data and regulator decisions show what is at stake

US\$3.05bn

BEC losses reported to the FBI
IC3 in 2025

11.5m

Documents leaked from one law
firm in 2016

£14m

UK ICO fine on outsourcer Capita
(October 2025)

6 hours

To report cyber incidents to
CERT-In

What this means: professional and business services firms must protect client files and deal information, secure email and cloud identities against takeover, stop payment and payroll diversion, govern client, staff and candidate data under DPDP, prove their controls to demanding clients, and report incidents within six hours.

Sources: FBI IC3 Internet Crime Report 2025, ICIJ Panama Papers reporting, UK Information Commissioner's Office, CERT-In.

Who we serve across professional and business services



Law firms and legal services

Litigation, transactions, advisory



CA and audit firms

Audit, assurance, tax, advisory



Tax and corporate services

Company secretarial, RTAs, filings



Management and tech consulting

Strategy, deals, transformation



Recruitment and executive search

Candidates, clients, assessments



Staffing and contract workforce

Associates, compliance, payroll



Payroll and HR outsourcing

Payroll runs, benefits, HRMS



Business support and shared services

BPO, GCCs, finance operations

The threats that cost professional firms the most

Six priorities from our 18-threat professional services assessment



Business email compromise

Client and payroll payments diverted



Data theft and extortion

Client files posted on leak sites



Ransomware

Practice and delivery systems frozen



Supply chain compromise

File-transfer and SaaS providers



People data exposure

Candidate, staff and payroll records



Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from mandate to archive

Where Cyber Risk Sits Across the Professional Services Engagement

Every stage from pitch to archive carries its own attack surface



In professional services, the client's secrets are the product: a single leaked file, diverted payment or exposed payroll can cost the mandate, the client and the firm's licence to be trusted.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, DPDP, confidentiality duties, and RBI, SEBI and client expectations

The rules shaping professional services 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. cloud and applications	CERT-In audit guidelines, 2025
Client, staff and candidate data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Client confidentiality (accountants)	Disclosure without consent is misconduct	Chartered Accountants Act, 1949
Advocate-client privilege	Professional communications protected	Bharatiya Sakshya Adhiniyam, s.132
Vendors to banks and NBFCs	Controls, audit rights, oversight	RBI IT outsourcing directions, 2023
Vendors to SEBI-regulated entities	Cyber resilience expectations	SEBI CSCRF, 2024
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023

Key dates on the regulatory timeline

Regulatory and Policy Timeline Shaping Professional Services Cybersecurity

Confidentiality, privacy, outsourcing and cyber instruments that reach firms directly or through their clients

● In force

● Upcoming (from Oct 2026)

2000	● Information Technology Act, 2000; CERT-In and Section 70A added by the 2008 amendment
Apr 2022	● CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Mar 2023	● Bar Council of India notifies rules for foreign lawyers and law firms on reciprocity
Apr 2023	● RBI Master Direction on IT outsourcing; applies to new contracts from 1 October 2023
Jul 2023	● SEBI LODR amendment: listed companies disclose cyber incidents quarterly
Aug 2023	● DPDP Act, 2023 enacted; firms act as data fiduciaries and data processors
Jul 2024	● Bharatiya Sakshya Adhiniyam in force; Section 132 keeps advocate-client privilege
Aug 2024	● SEBI Cybersecurity and Cyber Resilience Framework for SEBI-regulated entities
Jul 2025	● CERT-In Comprehensive Cyber Security Audit Policy Guidelines
Oct 2025	● Supreme Court limits summoning of advocates by investigators under Section 132
Nov 2025	● DPDP Rules notified; four labour codes take effect, reshaping payroll and HR
May 2027	● Most DPDP Rules obligations, incl. security safeguards and breach intimation, apply

Sources: MeitY, CERT-In, RBI, SEBI, Bar Council of India, Ministry of Labour and Employment, Gazette of India. Confirm against the official instruments.

Codec Networks

How Codec Networks helps

Confidential data · Email & cloud · Privacy · Client assurance · Managed SOC · Fraud investigations

One partner from mandate to archive



Confidential Data Protection

Classification, access, DLP



Email & Cloud Security

M365, MFA, portals



Privacy & DPDP

Client, staff, candidates



Client Assurance

ISO 27001, SOC 2, audits



24/7 Managed SOC

BEC and takeover detection



Fraud Investigations

BEC, payroll, insider cases

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

Boutique law, CA, consulting and recruitment firms

- Email and Microsoft 365 review (B3)
- External and remote-access assessment (B1)
- Privacy quick assessment (B6)
- Phishing and BEC awareness (B10)

Assurance

Mid-size firms, staffing and payroll providers

- Client portal and application testing (B2)
- ISO 27001 or SOC 2 readiness (B5)
- DPDP programme (B6)
- 24x7 managed SOC (B7)

Continuous Resilience

Large firms, networks, GCCs and shared services

- Continuous testing and red teaming (B1, B10)
- Client assurance and vendor programme (B5, B9)
- SOC with threat hunting (B7)
- Board, client and regulator reporting (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, reporting support	B7, B8
Independent cyber audits (CERT-In audit guidelines, 2025)	Independent firm and portal audits	B4, B1
Client, staff and candidate data (DPDP Act and Rules)	DPDPA programme for firms	B6
Processor contracts and safeguards for client data (DPDP)	Contract clauses, data mapping	B6, B9
Client confidentiality (CA Act 1949; BSA 2023 Section 132)	Access, DLP and leaver controls	B3, B5
Vendor controls expected by banks (RBI IT outsourcing rules)	Evidence packs, audits, ISO 27001	B4, B5
Quarterly incident disclosure, listed companies (SEBI LODR)	Incident records, disclosure support	B4, B8

Five new case studies, five broken chains

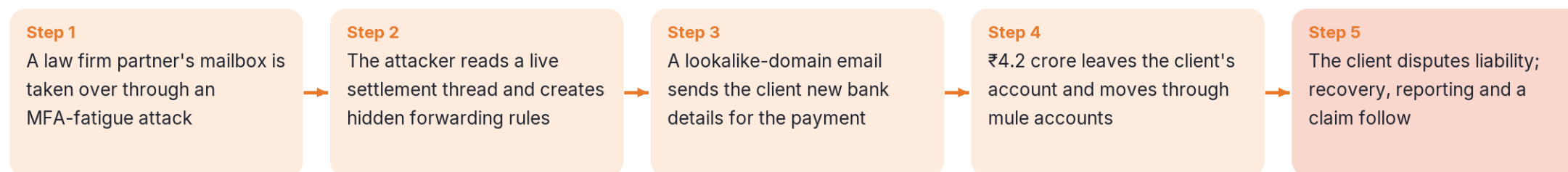
Illustrative composite scenarios written for 2026—not client engagements

1	The Settlement That Went to the Wrong Account	A partner's hijacked mailbox diverts a client settlement; MFA, SOC alerts and call-backs stop it	B3 · B7 · B8
2	The Audit Files That Appeared on a Leak Site	A VPN without MFA lets attackers steal and encrypt audit files; segmentation and SOC limit it	B1 · B7 · B8
3	The Payroll File That Left Through a Partner	A file-transfer zero-day exposes payroll for 40 employers; vendor risk and minimisation contain it	B9 · B6 · B7
4	The Recruiter Who Was Not Hiring	An open candidate bucket fuels fake-job scams; cloud testing and brand monitoring stop it	B2 · B6 · B7
5	The Help Desk That Reset the Wrong Password	A social-engineered MFA reset diverts vendor payments; identity checks and PAM break the chain	B3 · B10 · B7

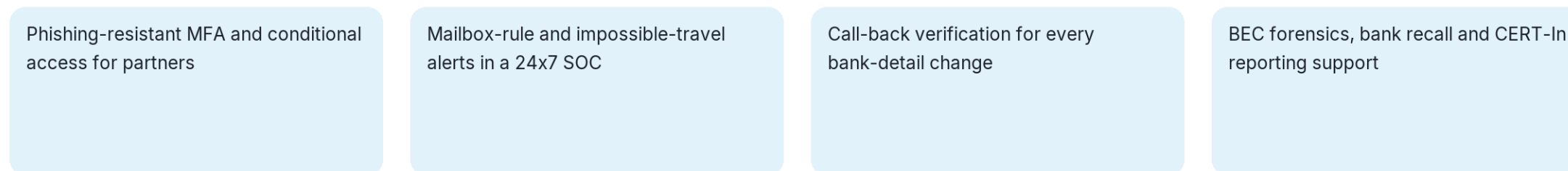
Example: breaking a BEC payment-diversion chain

Case 1: The Settlement That Went to the Wrong Account

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: whether partner and finance mailboxes resist MFA-fatigue and token theft, whether hidden forwarding rules and lookalike domains are detected, whether every bank-detail change is verified by call-back, whether the SOC sees impossible travel and rule changes in real time, and how leadership handles the client, the bank recall and CERT-In reporting in a tabletop exercise.

Why professional 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 CERT-In, DPDP, professional confidentiality duties, RBI and SEBI vendor expectations, SOC 2 and ISO/IEC 27001



Tests the whole chain

Technical, process and monitoring tests together



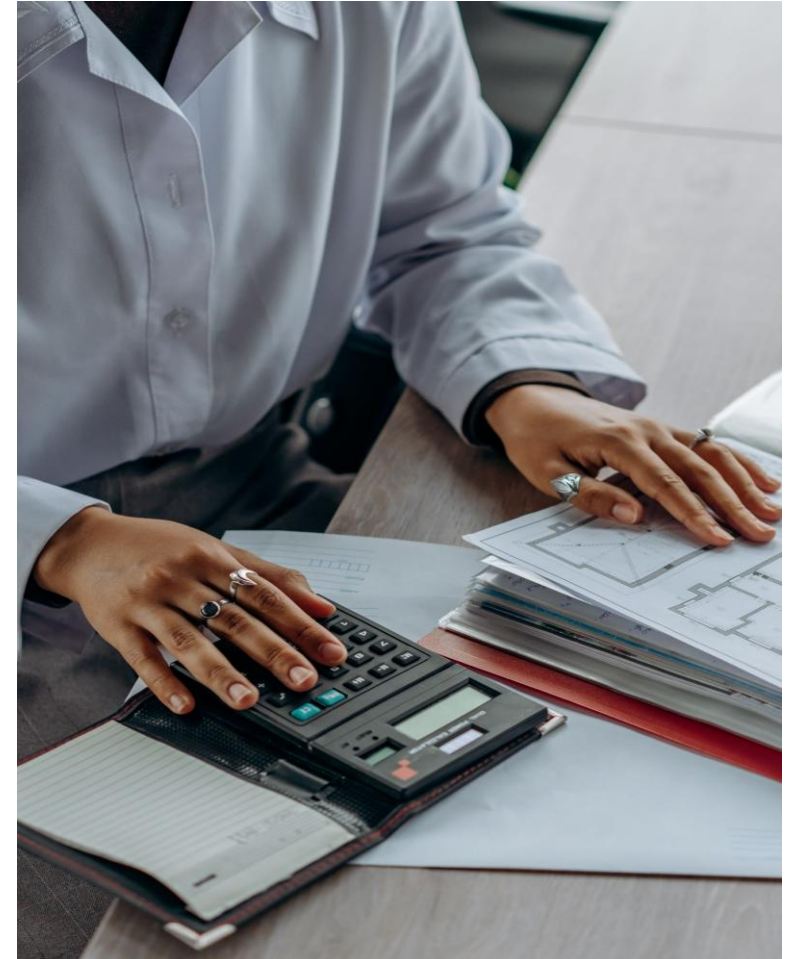
Full stack, one partner

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

Email and cloud tenants, document and practice systems, client portals and file transfer, payroll, HR and recruitment platforms, finance operations, vendors and client contract obligations

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.