

Codec Networks

Coding Threats. Decoding Solutions.

REAL ESTATE, CONSTRUCTION & FACILITIES

Secure the Building. Protect the Deal.

Building management and IoT security, CCTV and access control assessment, ERP and portal security and a 24x7 building SOC for real estate, construction and facilities 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, RERA, SEBI, DPDP and the MeitY CCTV requirements that reach every building



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 property happen in front of tenants

Global incidents and Indian obligations show the stakes

150,000

Camera feeds reached in the
2021 Verkada breach (FTC)

US\$2.77 bn

Business email compromise
losses reported to the FBI in
2024

Apr 2025

MeitY CCTV essential security
requirements in effect

6 hours

To report cyber incidents to
CERT-In

What this means: property companies must separate building systems from IT and tenants, control vendor access, test cameras and doors, protect buyer and tenant data, stop payment diversion, monitor buildings around the clock and report incidents within six hours.

Sources: US FTC, FBI IC3 2024 Annual Report, MeitY, CERT-In.

Who we serve across real estate, construction and facilities



Residential developers

Housing projects, townships, plotted developments



Commercial developers and REITs

Office parks, malls, listed REITs



EPC and construction

Contractors, infrastructure and industrial projects



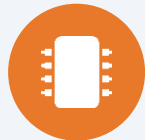
Co-working and flex operators

Managed offices, hot desks, enterprise suites



Facility management

Integrated FM, security and maintenance



Smart buildings and proptech

BMS, IoT, tenant apps, platforms



Industrial and logistics parks

Warehousing, data centre and industrial estates



Government and PSU projects

Public housing, infrastructure, institutional buildings

The threats that cost property companies the most

Six priorities from our 18-threat sector assessment



Ransomware shutdowns

ERP, CRM and project systems encrypted



Building system takeover

BMS, lifts and HVAC reached from outside



CCTV and door exposure

Cameras and access control open to attackers



Payment diversion

Fake bank-detail changes on contractor bills



Buyer and tenant data theft

KYC, PAN and visitor records stolen



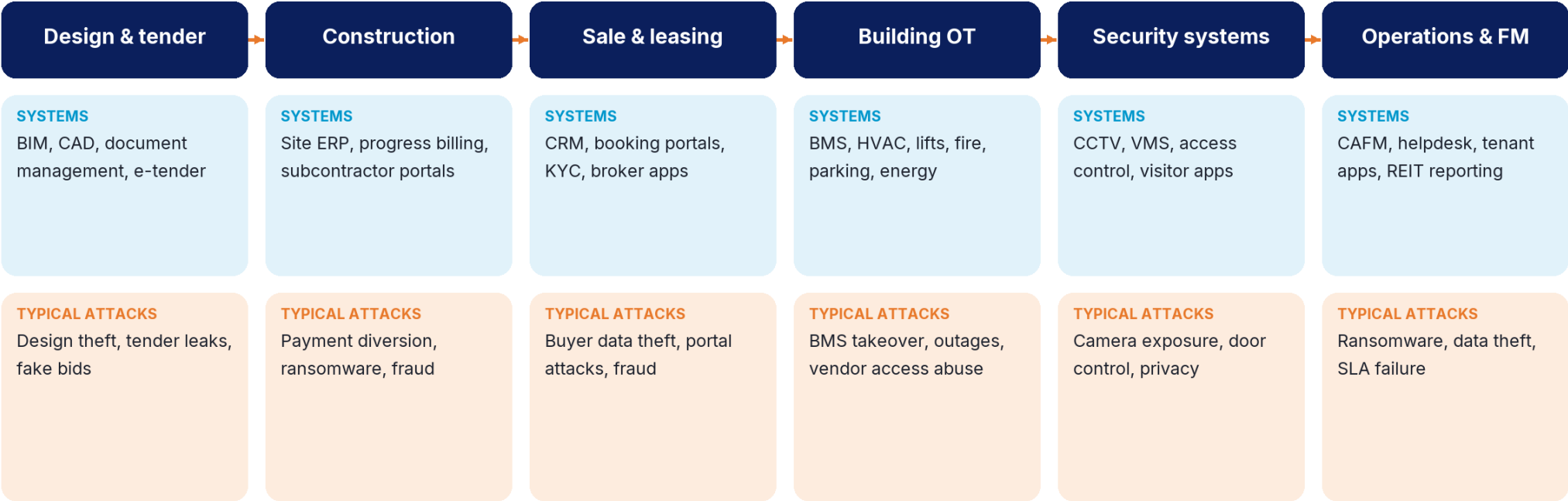
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from design to daily operations

Where Cyber Risk Sits Across the Property Lifecycle

Every stage from design to daily operations carries its own attack surface



In real estate and facilities, a cyber incident is a tenant incident—doors, lifts, cameras and comfort fail in public, and buyer and tenant data is at stake.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, RERA, SEBI, DPDP and the MeitY CCTV requirements that reach every building

The rules and standards shaping real estate and facilities 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	CERT-In audit guidelines, 2025
Project registration, escrow and disclosures	Per project	RERA 2016; state rules
REIT governance and unit-holder reporting	Periodic	SEBI REIT Regulations, 2014
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023
Buyer, tenant and visitor data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
CCTV security requirements	In effect from April 2025	MeitY Compulsory Registration Order
Building and security good practice	Standards	ISO/IEC 27001; IEC 62443

Key dates on the regulatory timeline

Regulatory and Standards Timeline Shaping Real Estate and Facilities Cybersecurity

Sector instruments, cross-sector Indian cyber and privacy rules and the CCTV requirements that reach every building

● In force

● Upcoming (from Oct 2026)

2000	● Information Technology Act, 2000 enacted; CERT-In and protected systems added in 2008
2014	● SEBI (Real Estate Investment Trusts) Regulations notified, creating the listed REIT framework
Mar 2016	● Real Estate (Regulation and Development) Act, 2016 enacted; state RERAs follow
May 2017	● RERA fully in force: project registration, escrow and disclosure duties for promoters
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	● Digital Personal Data Protection Act, 2023 enacted
Mar 2024	● SEBI amends REIT Regulations to introduce Small and Medium REITs (SM REITs)
Apr 2024	● MeitY adds essential security requirements for CCTV cameras to the compulsory registration regime
Aug 2024	● PMAY-Urban 2.0 approved: one crore urban houses over five years
Apr 2025	● CCTV essential requirements take effect; STQC testing for cameras sold in India
Jul 2025	● CERT-In Comprehensive Cyber Security Audit Policy Guidelines
Nov 2025	● DPDP Rules, 2025 notified with phased commencement
May 2027	● Most DPDP Rules obligations, incl. breach intimation, take effect

Sources: MeitY, CERT-In, SEBI, MoHUA. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

BMS & IoT · CCTV & access · ERP & portals · Payments · Privacy · Building SOC

One partner from site to smart building



BMS & IoT Security

BMS, HVAC, lifts, fire, IoT, segmentation



CCTV & Access Control

Cameras, VMS, doors, visitor systems



ERP & Portal Security

ERP, CRM, booking and tenant apps



Payment Fraud Defence

Bank-detail controls, BEC simulation



Buyer & Tenant Privacy

DPDP for buyer, tenant and visitor data



24/7 Building SOC

Monitoring and threat hunting

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-project developers, contractors and FM firms

- IT and building system assessment (B1)
- Payment fraud controls review (B10, B2)
- Backup and recovery review (B3)
- Policy and questionnaire pack (B5)

Assurance

Multi-project developers and property groups

- BMS, CCTV and access control assessment (B1, B3)
- ERP, CRM and portal testing (B2)
- Annual audit and DPDP programme (B4, B6)
- 24x7 building SOC (B7)

Continuous Resilience

REITs, large developers and national FM operators

- Portfolio building security programme (B1, B3)
- Vendor and integrator risk programme (B9)
- SOC with threat hunting (B7)
- Board, SEBI and unit-holder reporting (B4, B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Cyber incidents to CERT-In within six hours; 180-day logs	Building SOC, IR retainer and reporting support	B7, B8
Risk-based independent cyber audits incl. OT (CERT-In, 2025)	Independent IT and building OT audits	B4, B1
Quarterly cyber incident disclosure (SEBI LODR, REIT rules)	Incident records, disclosure support	B4, B8
Buyer, tenant, resident and visitor data (DPDP)	DPDPA programme	B6
CCTV security and STQC testing (MeitY ER, Apr 2025)	CCTV and VMS assessment, evidence pack	B1, B5
Project registration, escrow and buyer data (RERA)	ERP, CRM and collection controls	B2, B10
Occupier and lender security questionnaires	ISO 27001 and questionnaire readiness	B5, B9

Five new case studies, five broken chains

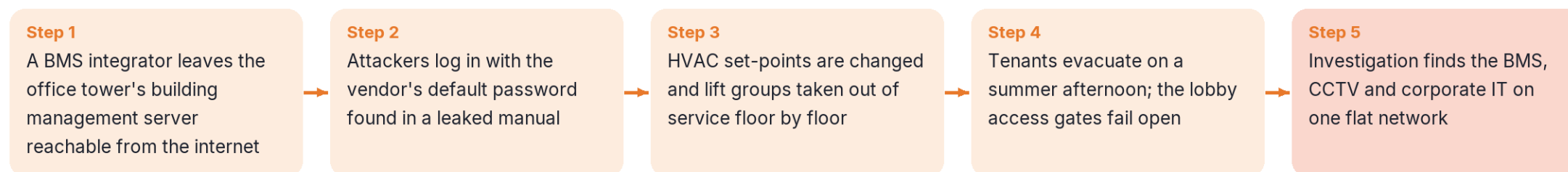
Illustrative composite scenarios written for 2026—not client engagements

1	The Building That Answered to the Internet	An exposed BMS lets attackers stop lifts and cooling; segmentation and vendor access controls prevent it	B1 · B3 · B7
2	The Running Account Bill That Paid Someone Else	A phished subcontractor thread diverts ₹3.8 crore; verification and monitoring stop it	B10 · B2 · B7
3	The Cameras Nobody Owned	A shared cloud CCTV credential exposes forty sites; assessment, MFA and DPDP controls fix it	B1 · B6 · B9
4	The Launch Weekend With No CRM	Ransomware hits a developer at launch; backups, SOC and a breach playbook limit it	B3 · B7 · B8
5	The Co-working Space That Shared Everything	A member laptop reaches door controllers and client data; segmentation and testing prevent it	B3 · B1 · B2

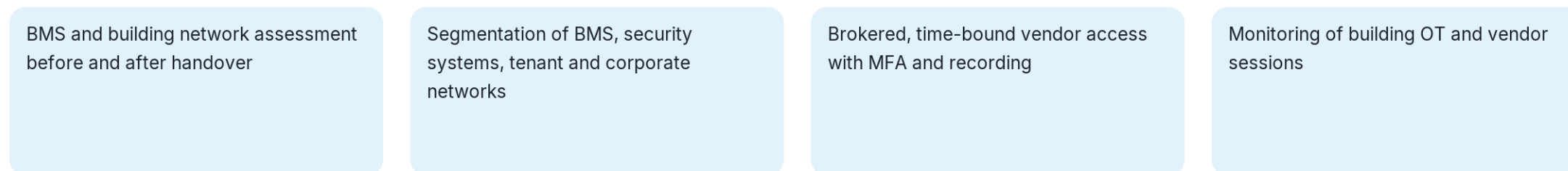
Example: breaking an internet-to-building-system chain

Case 1: The Building That Answered to the Internet

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 BMS, lift and CCTV systems are reachable from the internet or tenant networks, which vendors hold remote access and how it is brokered, whether building systems share a network with corporate IT, how set-point and door changes are monitored, and how FM, security and tenant teams respond in a tabletop exercise.

Why property 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 CERT-In, DPDP, SEBI and MeitY CCTV expectations and your occupiers' requirements



Tests the whole chain

Technical, process and monitoring tests together



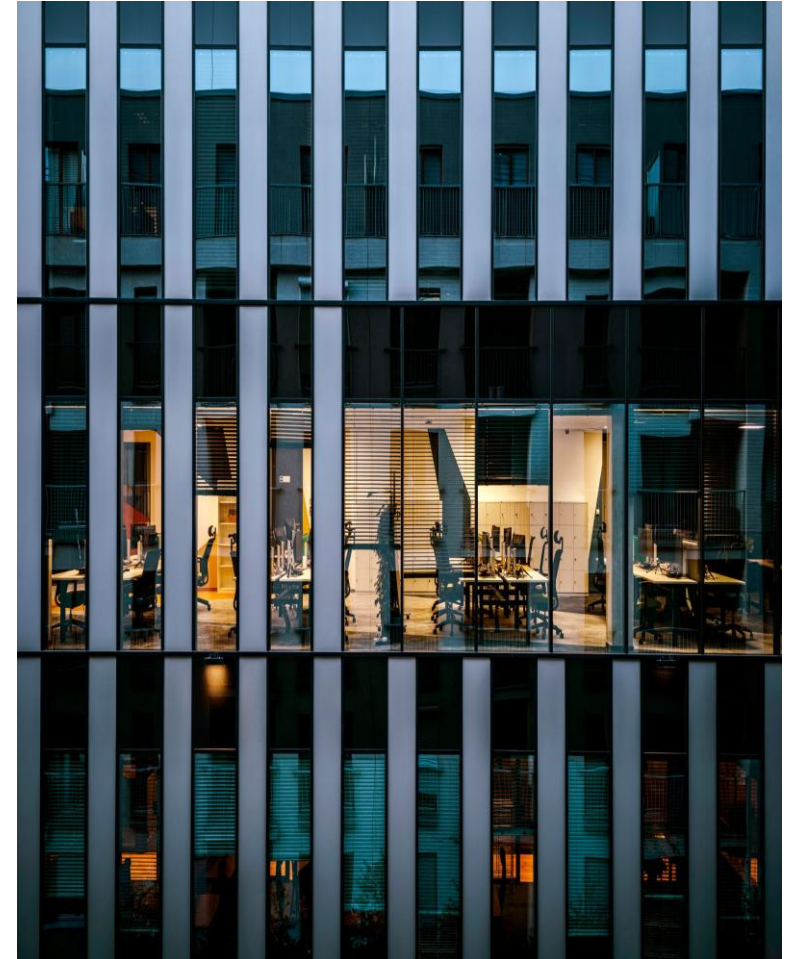
Full stack, one partner

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 MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Projects and buildings, BMS, CCTV and access control, vendors, ERP, CRM and portals, buyer and tenant data and your audit and occupier 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.