BRANDEFENSE COUNTRY REPORT · INDIA 2026

Brandefense India Cyber Threat Landscape Report 2026

Payment integrity, exposed identities and the boundaries of public cyber claims

Odin by Brandefense

Research window: 1 January–22 November 2026

Version 1.0 · Public Research Edition · TLP:CLEAR · 8–22 November 2026

98 of 250

selected estates had a credential listed for sale when checked

6

detailed claim dossiers, with separate validation questions

254

India-labelled extortion listings in the observation window

20

conditional actions with reviewable completion evidence

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	India's digital and security context	10
03	National exposure: the selected organisation portfolio	15
04	What the retained underground material shows	24
05	Incidents and targeting examples by sector	39
06	Hacktivism, DDoS and the availability question	55
07	Threat actors and supported relationships	59
08	Fraud, identity and payment authority	69
09	Banking and financial-services deep dive	74
10	Regulatory and national response	79
11	Outlook and conditional planning	85
12	Action plan	90
	Appendices	96
A	Appendix A. Sources, scope and confidence	97
B	Appendix B. Public evidence-card register	101
C	Appendix C. Sources	103
D	Appendix D. Glossary	107
	About this report	109

Board and executives	01 03 11 12
CISO	03 05 07 10 12
SOC and intelligence	04 06 07 A B C
Fraud and payments	05 08 09 12
Legal and communications	05 06 10 12

About this edition

English master only. No translated edition is produced. AI agents assisted research, analysis and drafting. Source scope and evidence limits are stated in Appendix A.

India-relevant evidence spans payment-workflow abuse, extortion claims, identity-data offers and supplier incidents, each requiring a different validation and response decision.

254

India-labelled extortion listings

250

selected organisation estates

16

extortion listings in the recent window

4

leadership decisions with named owners

Contents and reading routes

Chapter	Question
1 Executive summary	Which findings should change a leadership decision?
2 Digital context	Which dependencies and official measures matter?
3 National exposure	What can the selected organisation portfolio establish?
4 Underground material	What do advertisements and their dates establish?
5 Sector cases	Which incidents, campaigns and warnings affect each response team?
6 Availability and hacktivism	How should claims and operational outcomes be separated?
7 Threat actors	Which source-supported actor relationships are useful?
8 Fraud economy	How do identity and payment processes become fraud opportunities?
9 Banking	Which financial questions need separate investigation?
10 Regulation	Which reporting and control duties apply now?
11 Outlook	Which conditions would change the assessment?
12 Action plan	Who should deliver which evidence in the next 90 days?
Appendices A–D	Scope, evidence register, sources and glossary

Evidence labels apply throughout. An **observation** describes material held or a recorded control result. An **actor claim** describes what an advertiser or claimant says. **Source-attributed reporting** describes an authority's, organisation's or researcher's account. None automatically validates the others.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

What does the evidence support, and which decisions should India-focused security leaders make first?

4

decisions spanning payments, identities, continuity and reporting

Five findings 06

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

India's closing-period official reporting puts payment integrity at the centre of the response agenda. CERT-In describes abuse of business records and approval processes beyond financial firms. Separately, 254 India-labelled extortion listings appear in the retained ransomware source. Underground offers include historical data, while public disclosures retain unresolved scope. These populations cannot be combined into a national breach total. Validate payment authority, investigate identity signals, test recovery and prepare the applicable reporting paths.

The report combines Brandefense's own evidence with opened public sources. Its observation window follows post or publication dates from 1 January through material available on 22 November 2026. Incident occurrence, discovery and disclosure dates remain separate. The recent-activity section covers 8–22 November; it does not represent a completed final day. [S1][S2][S3]

Five findings

1. **Payment authority extends beyond the transaction interface.** CERT-In's 20 November notice describes incidents involving altered business records and approval relationships outside financial firms. A payment that passes routine checks can still rely on an unauthorised underlying change. The practical decision is to require an independent source for beneficiary and approval verification. This is authority campaign reporting, rather than a count of affected organisations. [S40]

2. **Extortion claims span the year and many source labels.** Ransompedia records 254 India-labelled listings in the window, including 16 published during 8–22 November. The leading six labels account for 94 records. Listings are claims; they do not establish encryption, verified loss, a common affiliate or unique affected organisations. Continuity decisions should use a matching claim as an investigation trigger. [S3]

3. **A current advertisement can contain older material.** The retained forum evidence includes offers whose own samples or descriptions refer to earlier years. A new post therefore does not date the underlying extraction or establish current account access. The first decision is to establish ownership, age and relevance before disrupting customers or announcing a new incident. The detailed dossiers in Chapter 4 preserve those limits. [S2]

4. **98 selected estates had a credential listed for sale.** The portfolio contains 250 selected estates. Separately, 227 have recorded device associations and 217 have credential records. The 819,157 device associations and 11,869,357 credential records are cumulative and can overlap. They do not establish current access or national prevalence. Validate the relevant identities and their prior remediation. [S30]

5. **Reporting duties and commencement dates need separate decisions.** CERT-In's existing directions require applicable incidents to be reported within six hours of noticing or being informed. The November DPDP Consent Manager phase does not activate every future safeguard and breach-intimation duty. Sector-specific financial reporting also remains relevant. Legal and security teams should maintain an entity-specific reporting matrix. [S10][S11][S12][S49][S21]

Four decisions for leaders

1. **Verify payment authority independently.** Finance, fraud and service owners should test a beneficiary-change scenario against records outside the system making the change. Escalate if the same administrator can alter both the payment basis and its supposed verification. Record the test and the accepted exceptions within 30 days. [S40]

1. **Validate before disrupting identities.** Give the identity team a route for receiving relevant credential and device signals. For a matching alert, establish account ownership, validity and prior remediation. Revoke sessions or reset credentials when the evidence and incident policy justify it; record a disposition rather than treating every historical record as active access.

1. **Test continuity and supplier containment.** Choose one essential customer journey and test its restoration with a critical supplier unavailable. Confirm who can suspend a harmful integration and who can preserve the relevant logs. Report the tested recovery time and unresolved dependencies by day 90.

1. **Prepare parallel reporting paths.** Legal, security and fraud teams should rehearse a time-limited incident assessment against applicable CERT-In, regulator and police channels. The exercise should preserve the awareness time and separate preliminary facts from later updates. Do not wait for a full root-cause conclusion before assessing a running duty. [S10][S21]

The year in numbers

254

India-labelled extortion listing records, 1 January–22 November [S3]

WHAT IT IS NOT

Confirmed intrusions, successful encryption or unique victim organisations

16

Those listing records published during 8–22 November [S3]

WHAT IT IS NOT

A separate population to add to the annual count

98 of 250

Selected estates with a current credential offer [S30]

WHAT IT IS NOT

Confirmed intrusions, active accounts or a count of credentials

57 out of 100

National Atlas headline for the 250 selected estates [S30]

WHAT IT IS NOT

A national prevalence estimate, loss forecast or sector rating

250

Purposively selected organisation estates across ten sector groups [S5]

WHAT IT IS NOT

A revenue ranking or national prevalence sample

31 / 16 / 6 / 1

Pakistan, Bangladesh, Sri Lanka and Nepal listing records in the same window [S3]

WHAT IT IS NOT

Country-adjusted rates or a national security ranking

3,897

Customer records SBI identified within a larger advertised set in its preliminary review [S53]

WHAT IT IS NOT

Confirmation that the full advertised population was genuine or a core-system intrusion

4

Distinct India-labelled card samples in the India-labelled forum posts [S6]

WHAT IT IS NOT

Fresh 2026 theft, current usability or national fraud loss

Six hours

CERT-In reporting period for applicable incidents after noticing or being informed [S10]

WHAT IT IS NOT

A universal clock for every unverified advertisement

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

The card figure is a narrow post-corpus observation. It includes historical material and does not measure national card exposure, card theft or fraud loss. The selected organisation exposure measures have their own availability limits in Chapter 3. No absent figure is interpreted as zero.

KEY TAKEAWAYS

01

Use independent payment records and identity validation to turn external signals into scoped investigations.

02

Keep advertisements, extortion listings, official campaigns and company disclosures in separate populations.

03

Test recovery, supplier containment and the applicable reporting paths before a live incident.

Report map

Choose the decision you own, then follow the evidence to its limits and completion test.

Board and executives	Fund the controls whose completion can be demonstrated	01 03 11 12
CISO	Prioritise exposures, suppliers and reporting readiness	03 05 07 10 12
SOC and intelligence	Separate source material from attribution and outcomes	04 06 07 A B C
Fraud and payments	Verify who can change the basis for a transfer	05 08 09 12
Legal and communications	Preserve incident scope and assess reporting duties	05 06 10 12

01 Executive summary
Four accountable leadership decisions

02 India's digital and security context
A dated context and population guide

03 National exposure: the selected organisation portfolio
Selected-estate control results and availability boundaries

04 What the retained underground material shows
Claim dossiers and validation questions

05 Incidents and targeting examples by sector
Original disclosures, campaigns and a recent-activity register

06 Hacktivism, DDoS and the availability question
A claim-versus-operations communication framework

07 Threat actors and supported relationships
Source-supported relationships and investigation behaviours

08 Fraud, identity and payment authority
Fraud opportunities and customer-protection tests

09 Banking and financial-services deep dive
Separate financial-service investigation questions

10 Regulatory and national response
An entity-specific reporting and commencement assessment

11 Outlook and conditional planning
Conditions and evidence that would change the plan

12 Action plan
Owners, dates and completion evidence

CHAPTER 02

India's digital and security context

THIS CHAPTER ANSWERS

Which operating conditions shape a proportionate response in India?

6 hours

CERT-In reporting period for applicable listed incidents

2.1 Connectivity is a dependency measure 11
2.2 The official statistics use different clocks 11
2.3 Coordination follows the function 12
2.4 National systems need broad evidence boundaries 13
2.5 Attribution and political neutrality 13
2.6 The regulatory timetable changes the response plan 13
2.7 A government-sector statistic with its own population 14

CHAPTER 02

India's digital and security context

IN SHORT

India's evidence connects large digital-service dependencies with identity, supplier and payment risks. Official statistics describe different periods and reporting systems. They cannot be added to underground posts or ransomware listings. Regulatory duties also differ by entity and activity, while the personal-data framework has phased commencement. Map the service, identity, provider and reporting owner before an incident forces the decision.

2.1 Connectivity is a dependency measure

TRAI reports 1,092.79 million internet subscriptions at 31 March 2026, including 1,065.88 million broadband subscriptions. The figures were released in October. They count subscriptions, not unique people, and do not supply a denominator for cyberattack probability [S19].

The practical implication concerns the business journey. A customer may depend on a mobile connection, a messaging account, a payment application and a supplier's verification service to complete one task. Security planning should identify those dependencies together.

A reliable service inventory therefore needs more than a list of servers. Record the business function, identity provider, data custodian, payment or communication provider and minimum usable fallback. Give each dependency an accountable owner and a tested contact route.

An interruption in one component does not establish an intrusion in every connected organisation. Likewise, a legitimate application can process an unauthorised instruction when underlying business records or account privileges are altered. The service and the authority behind its instructions require separate checks.

That distinction is central to CERT-In's November business-payment warning. The authority describes unauthorised transactions involving non-financial organisations and provider-operated processes. Its account concerns workflow integrity, without establishing a national victim total [S40]. Chapter 5 examines that proposition separately from bank-system access.

2.2 The official statistics use different clocks

A March parliamentary reply gives 2,944,248 cyber security incidents reported to or tracked by CERT-In during 2025. That is a previous-calendar-year statistic published in 2026. It is not this report's 2026 incident count [S17].

The same reply says CERT-In does not maintain estimated financial losses from cyber incidents. A loss figure from a different reporting system cannot be inserted as the financial value of the CERT-In population [S17].

The following populations support different decisions.

Population	Unit	Useful question
Retained underground posts	Messages and advertisements	Does a relevant claim match an owned asset?
Ransomware listings	Public extortion assertions	Can the organisation recover and assess data impact?
CERT-In statistics	Incidents under the authority's reporting definitions	Which official reporting and response functions apply?
Cybercrime complaints	Reports through the relevant complaint system	Can a credible fraud report reach the response route quickly?
First information reports	Registered criminal cases	What formal investigation has been initiated?
Confirmed disclosures	Particular statements by organisations or authorities	Which access, service or data proposition is supported?

None supplies the missing portion of another. A single complaint can concern several transactions; a provider incident can affect several customers; an advertisement can repeat historical material. Adding these units would produce a misleading national total.

The CERT-In annual-report index available at the cut-off listed 2024 as its latest annual report. It did not supply a completed 2026 annual assessment [S20]. This report consequently retains each available official statistic's actual period.

2.3 Coordination follows the function

CERT-In's directions identify applicable entities, reportable incident categories and operational requirements. They include a designated contact, logging and a six-hour reporting period after noticing an applicable incident or being informed of it [S10]. An unverified advertisement is not automatically the required factual trigger.

The Ministry of Home Affairs describes the national cybercrime response mechanism and financial-fraud reporting arrangements. Its July reply reports complaint handling, funds protected and restoration processes. Those are response-system measures, with their own cumulative periods [S18].

The National Critical Information Infrastructure Protection Centre (NCIIPC) is identified under section 70A as the national nodal agency for critical information infrastructure protection [S23]. That institutional role does not establish that every organisation in a sector has a particular legal designation. Legal and service owners must determine the actual scope.

For a responder, these functions should become a practical contact matrix. Identify the technical reporting route, fraud-escalation route, sector supervisor, police contact and internal authority to submit. Test the matrix without sending a fictitious incident report.

2.4 National systems need broad evidence boundaries

Identity records, financial accounts and public-service themes can appear together in a criminal advertisement. Their combination does not identify the system from which records originated. A legitimate identifier mentioned in a file is not evidence of access to its issuing authority.

The same applies to a supplier's customer names. A document about a bank or government body can be held by a contractor, a customer or another organisation. Validate provenance before extending an incident allegation to every organisation mentioned.

Current website changes also affect interpretation. RBI's bank directory now lists current `.bank.in` websites [S24]. Historical evidence can still mention earlier domains. A current-domain observation does not represent every service, subsidiary or former domain used by a bank.

2.5 Attribution and political neutrality

The report takes no position on governments, elections, political parties, caste, religion, communal issues or territorial questions. Pakistan, Kashmir, China and Bangladesh appear only where a security proposition requires a source-specific boundary.

The May 2025 conflict lies outside the reporting window. Its existence cannot date a 2026 post, establish a new attack, or prove state direction behind a later claim. An actor's invocation of an earlier event remains that actor's explanation.

Language and a self-selected alias do not establish nationality. Political rhetoric does not establish sponsorship. Regional targeting in a vendor report does not attribute an unrelated incident to the same actor. Slurs and loaded framing are omitted.

Apply the same validation and privacy standards to public bodies, businesses, religious organisations, political organisations and civil society. The relevant questions concern authorised access, affected information, service consequences and proportionate response.

2.6 The regulatory timetable changes the response plan

India's personal-data framework is phased. MeitY's November update identifies the Consent Manager phase while placing other key duties in May 2027 [S49]. That change must not be described as full activation of every breach obligation.

Current CERT-In and sector duties therefore remain distinct from future personal-data obligations. Chapter 10 separates their triggers and dates. An organisation should maintain an entity-specific register rather than relying on a single universal notification deadline.

2.7 A government-sector statistic with its own population

An original 5 August Lok Sabha answer reports 1,075,220 government-sector cyber-security incidents reported to and tracked by CERT-In through June 2026. The population covers central ministries and departments and state governments. It is not a full-year count of confirmed breaches or affected organisations. [S101]

This statistic cannot be directly compared with the earlier national annual figures or with the report's forum and extortion populations. A leadership dashboard should preserve the sector, reporting period and event definition before drawing a trend.

KEY TAKEAWAYS

01

Keep official statistics, posts, listings and disclosures in their own periods and units.

02

Map identity, supplier and payment dependencies to accountable service owners.

03

Establish current reporting duties without turning future phases or actor rhetoric into present facts.

CHAPTER 03

National exposure: the selected organisation portfolio

03

THIS CHAPTER ANSWERS

Which exposure signals need validation across the selected portfolio?

98 of 250

selected estates had a credential listed for sale when checked

3.1 Universe card 16
3.2 Current listings and the national Atlas headline 17
3.3 Recorded devices and credentials 19
3.4 How to interpret identity evidence 21
3.5 Email, DNS and web-control observations 21
3.6 Bank-domain migration changes the historical boundary 22
3.7 A validation sequence for portfolio owners 23

CHAPTER 03

National exposure: the selected organisation portfolio

IN SHORT

Among 250 selected organisation estates, 98 had a credential listed for sale when checked on 22 November. The national Atlas headline is 57 out of 100. The portfolio has 819,157 recorded device associations and 11,869,357 credential records, which are cumulative and can overlap. Control observations cover 235 estates. These results describe the selected portfolio, without establishing current intrusion or national prevalence. Validate current offers, employee-associated records and service ownership before choosing containment.

3.1 Universe card

Item	Definition
Population	250 selected organisation estates, with one primary domain per row [S5]
Selection	National and regional public bodies, banks, major service providers, industry, universities and healthcare organisations
Purpose	Decision coverage across ten merged sectors, rather than a revenue ranking
Unit	A selected primary domain can represent a group, a service or an organisation with further domains
Independence	Group affiliations and shared services can create overlap; rows are not assumed independent
Control date	Available observations relate to 22 November 2026, rather than the full annual incident window [S4]
Coverage	A result is reported only with its available assessed population; unavailable is not zero
Limitation	Results do not establish current intrusion, account validity or national control prevalence

The sector composition below is the selected portfolio. The mix reflects the selection purpose. A larger cell does not imply that the sector suffers more incidents. [S5]

Sector group	Selected estates
Public administration	30

Sector group	Selected estates
Banking	30
Insurance and financial services	20
Education and research	25
Energy and utilities	20
Industry and manufacturing	25
Technology and communications	25
Transport and logistics	25
Health and life sciences	25
Consumer services and retail	25
Total	250

Selection and ownership are different questions. An official or corporate site can identify an organisation, while its domain may cover several services or be shared with another group entity. The report therefore describes the portfolio as selected estates when interpreting domain-level evidence.

3.2 Current listings and the national Atlas headline

98 of the 250 selected estates had a credential listed for sale. The observation relates to a credential associated with the selected primary domain when checked on 22 November. It does not establish the account owner, current validity, access rights or a successful intrusion. [S30]

The national Atlas headline for the 250 selected estates is 57 out of 100. Higher values indicate greater observed exposure in the selected portfolio. This edition publishes only that national figure. Sector rows show signal counts rather than ratings. [S30]

The table shows estates carrying each fully available signal. A current offer and a historical record are separate propositions. Neither count measures confirmed affected people or business impact.

Current offers, employee-associated devices and document observations require different validation tasks

	Current offers	Employee devices	Documents
Public administration	9/30	20/30	27/30
Banking	2/30	6/30	19/30
Insurance and financial services	13/20	18/20	20/20
Education and research	18/25	24/25	23/25
Energy and utilities	6/20	10/20	15/20
Industry and manufacturing	9/25	19/25	21/25
Technology and communications	12/25	25/25	23/25
Transport and logistics	12/25	19/25	18/25
Health and life sciences	7/25	21/25	21/25
Consumer services and retail	10/25	17/25	18/25

Current credential listings by sector (coral). Cells show estates with each signal / selected estates; signals overlap. Source: selected-estate exposure observations, 22 November 2026 [S30]. Cumulative associations can overlap; not current intrusions or national prevalence.

Sector group	Estates	Current offers	With employee associations	With document observations
Public administration	30	9	20	27
Banking	30	2	6	19
Insurance and financial services	20	13	18	20
Education and research	25	18	24	23
Energy and utilities	20	6	10	15
Industry and manufacturing	25	9	19	21
Technology and communications	25	12	25	23
Transport and logistics	25	12	19	18

Sector group	Estates	Current offers	With employee associations	With document observations
Health and life sciences	25	7	21	21
Consumer services and retail	25	10	17	18
Total	250	98	179	205

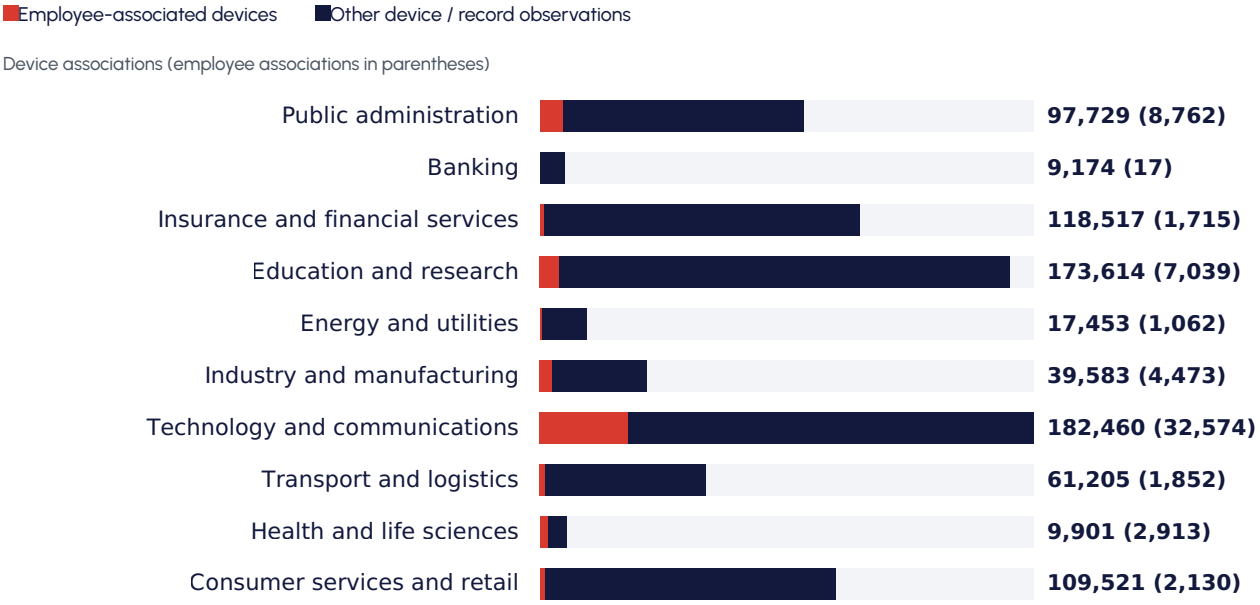
A current listing should enter an account-validation queue. Establish whether the account belongs to the organisation, remains active and has already been remediated. Where evidence supports active unauthorised access, follow the incident process. The listing alone is not that conclusion.

3.3 Recorded devices and credentials

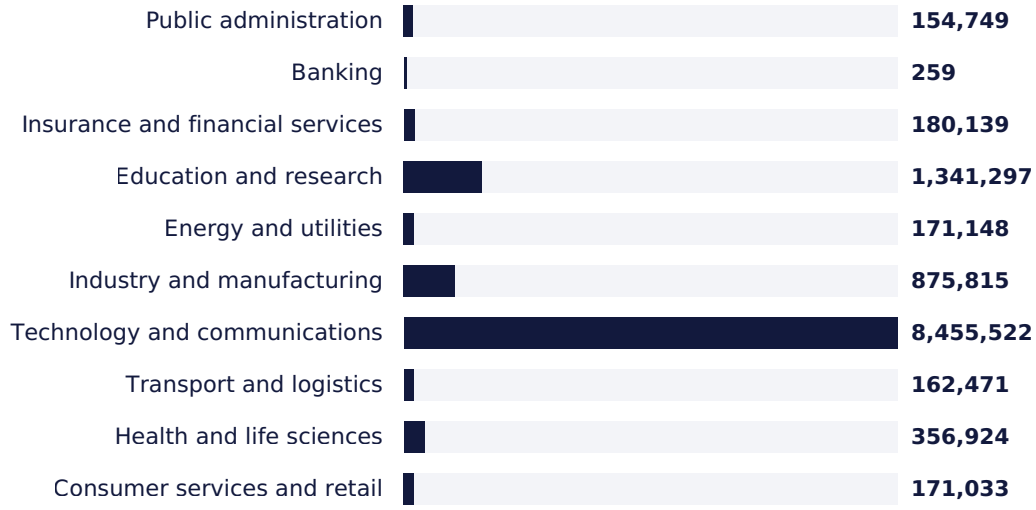
The selected portfolio has 819,157 recorded device associations, including 62,537 employee-associated device records. There are 11,869,357 credential records across the selected domains. These are cumulative records held when checked, irrespective of capture date; they are not 2026-only populations. [S30]

Figure c04 separates device, employee-associated and credential observations across the selected sectors. The populations can overlap and require different validation tasks. [S30]

Device and credential associations describe different exposure populations



Credential records (separate scale)



Document observations (separate scale)



Panels use independent scales; overlapping populations are never added together. Source: selected-estate exposure observations, 22 November 2026 [S30]. Cumulative associations can overlap; not current intrusions or national prevalence.

Measure	Selected-portfolio result	Interpretation
Estates with device associations	227 of 250	Associations require ownership and freshness validation
Estates with credential records	217 of 250	Records can be historical and overlap
Device associations	819,157	Not unique people or confirmed current infections
Employee-associated devices	62,537	A source association, not verified employment
Credential records	11,869,357	Not unique accounts, working passwords or confirmed intrusions

Measure	Selected-portfolio result	Interpretation
Estates with document observations	205 of 250	A reference to a domain does not establish the document's sensitivity
Document observations	6,782	Require content and ownership validation

A device can carry logins associated with several organisations. One person can appear in several credential sources. These populations are not added to each other or to the incident and fraud figures elsewhere in the report.

Employee-associated records merit an identity and endpoint review, with the asset owner confirming their meaning. Student and shared-domain contexts can complicate an employment inference. Other device records may concern customers or unrelated users; their ownership is not established by association alone.

3.4 How to interpret identity evidence

An external identity record becomes useful when it can be connected to an owned account, device or application. The immediate question is whether it still creates a plausible path to the organisation. That assessment belongs to the owner of the relevant identity system.

For an employee-associated signal, check whether the account exists, whether its access is still required and whether prior remediation covers the exposure. A change of password may leave another question about sessions or tokens. Follow the incident policy when evidence justifies containment.

Customer and employee associations should remain separate. A login to a customer-facing service can originate from a customer's device. It does not establish an intrusion into the service operator. Universities and other shared identity environments also require care before interpreting a record as belonging to an employee.

Historical records and current market offers are different evidence types. A repeated offer can be current as an advertisement while containing old information. Conversely, an old source date does not establish that a still-authorised session or key is harmless. Validate the consequential proposition rather than the seller's general description.

The completion record should state which account or device was assessed, who owned the decision and what closed it. Appropriate outcomes include already remediated, not associated with the organisation, active exposure contained or further investigation required. A count of alerts closed does not establish that the underlying risk was removed.

3.5 Email, DNS and web-control observations

Available control observations cover 235 of the 250 selected estates. The assessed set contains 193 estates with an observed DMARC reject or quarantine policy. Unavailable estates are not counted as missing controls. [S4]

Observation	Result	Assessed population
DMARC reject	120	235 estates
DMARC quarantine	73	235 estates
Other or unavailable DMARC outcome	42	235 estates
SPF record observed	212	235 estates
DKIM record observed	141	235 estates
DNSSEC delegation record observed	62	235 estates
Certificate did not validate	12	202 available certificate results
HSTS observed	129	156 available web-control results

The table describes observations at the cut-off, rather than the security of every service operated by the selected organisations. 15 selected estates have no control assessment in this table. An unavailable service result does not establish an absent control.

A domain policy describes an instruction or a visible configuration. It is not a test of every message, receiver or customer journey. A DMARC enforcement policy does not prevent every form of impersonation, including deceptive display names and unrelated lookalike domains.

A published SPF record also requires service-level interpretation. The team responsible for mail should know which senders are authorised and whether messages align correctly. An apparently strong policy can disrupt legitimate mail if the sender inventory is incomplete.

Absence of an observed DKIM record does not establish that an organisation never signs mail. A DNSSEC delegation record does not, by itself, establish a valid chain for every answer. Certificate validation and transport controls likewise answer a narrower question than overall application security.

Unavailable web-control evidence should remain distinct from an observed missing control. Some services had no available result; the report does not assign a cause to an unavailable result.

3.6 Bank-domain migration changes the historical boundary

RBI's current bank directory identifies `.bank.in` domains for many Indian banks. The selected portfolio follows the current directory. A measure tied only to a current primary domain does not describe every older bank domain. [S24]

The migration therefore changes the interpretation of an apparently small external footprint. A new domain can have fewer historical records without demonstrating that the bank has less exposure. Domain aliases, service boundaries and the observation date must accompany an investigation.

The public report does not reproduce a roster of bank domains. For each organisation, the identity and application owners should maintain the authorised domain inventory and a dated migration record. A closed alert on a legacy domain may still matter if the related account or service remains active.

3.7 A validation sequence for portfolio owners

Start with ownership. Confirm which legal or service owner is responsible for the selected estate and which additional domains belong in the same operational review. Record shared platforms and supplier-controlled components without assuming they are independent organisations.

Next, identify the relevant signal and its population. A current listing, a historical record, a mail policy and an extortion claim require different evidence. Do not combine their counts into an affected-person or breach total.

Assign a validation task with a trigger for escalation. Active access may require immediate containment. An unsupported advert may require preservation and schema comparison. A policy change should require sender testing, an approved rollout and a rollback route.

Finally, review completion evidence at the service level. Verify that the intended protection or containment works and that legitimate users can still complete essential tasks. Record any accepted exception, its owner and its review date.

KEY TAKEAWAYS

01

98 of the 250 selected estates had a credential listed for sale; validate the relevant accounts.

02

Device and credential figures are cumulative, overlapping associations rather than confirmed current intrusions.

03

Keep the national rating, signal counts and control results separate.

CHAPTER 04

What the retained underground material shows

04

THIS CHAPTER ANSWERS

Which advertisements matter, what do they establish, and what should the named service owner validate first?

6

detailed claim dossiers, with separate validation questions

4.1 Universe card 25

4.2 Read the advertisement's object before assigning an incident 26

4.3 Six detailed dossiers 27

4.4 Other retained offers and what they do not establish 34

4.5 Recent activity: 8–22 November 36

4.6 Additional recent claims retain separate boundaries 37

4.7 A validation record that supports a decision 38

CHAPTER 04

What the retained underground material shows

IN SHORT

The retained forum material contains payment-data offers, supplier-access menus, identity-document claims and recent education and medical-payment advertisements. Some posts explicitly describe older material. Others request access or data rather than demonstrate possession. A bank name in a payment field does not identify a bank intrusion. Treat each advertisement as a scoped investigation lead, and establish ownership, age and the affected service before deciding on containment or a public statement.

4.1 Universe card

Item	Definition
Source	Brandefense Blackhole retained posts and accompanying source information [S1][S2]
Primary window	Post dates 1 January–22 November 2026; material available when checked on the cut-off date
Country association	India-related source labels and the meaning of the retained text; an association does not establish targeting
Reading unit	One post can advertise several datasets, repeat an earlier offer or discuss another post
Case unit	A dossier explaining one selected advertisement or related claim family; not a unique confirmed incident
Public presentation	Generic victim roles, actor aliases where useful and clearly labelled English paraphrases
Not established	Dataset authenticity, current access, unique affected people, a completed sale or a new intrusion date

The post cards preserve evidence boundaries while omitting victim identifiers and sensitive sample content. Their English text is labelled as a paraphrase. It is not represented as an original-language quotation or an independently verified description of the advertised data.

The India-labelled forum observations contain 1,505 posts, including 67 published during 8–22 November. These are circulation records, rather than targets or incidents. The material includes offers, old archives, global menus and replies. A post count cannot establish how many claims were authentic or how many organisations suffered an intrusion. [S2][S9]

Publication month	India-labelled forum posts
2026-01	371
2026-02	150
2026-03	105
2026-04	107
2026-05	71
2026-06	84
2026-07	108
2026-08	185
2026-09	139
2026-10	91
2026-11 through 22 November	94
Total	1,505

November is a partial month. Differences between months describe visibility in this source, rather than a national attack trend. Use the dated narrative and owned evidence to decide whether an offer warrants investigation.

4.2 Read the advertisement's object before assigning an incident

Three questions prevent many false escalations. What is being offered: a dataset, a credential, a service or access? What links it to India: a target assertion, a sample label or a country in a global menu? Which part is independently supported?

A payment record can refer to an originating institution, a beneficiary bank and a service provider. Those references describe roles in a transaction. They do not establish separate intrusions at all named institutions. Similarly, a business-contact directory can contain many company names without showing access to their systems.

Historical material still matters. A record can support convincing impersonation even when the account password has changed. That is a reason to test account recovery and payment-change procedures. It is not a reason to describe the record as newly stolen.

The six dossiers below separate the observed offer from its proposed origin and consequences. They do not estimate how often such claims are genuine across India. The selection illustrates distinct validation decisions rather than a statistical sample of all incidents.

4.3 Six detailed dossiers

A

CASE A

A payment archive with older sample dates

Evidence card B01 | 31 Jan 2026 | Forum | Payments

Unverified archive claim

CLAIM	On 31 January, a forum seller described a multi-file payment-data archive. The offer referred to transaction and beneficiary information.
CHRONOLOGY	The retained post is from January 2026. Date strings visible in the advertised sample refer to 2023 and 2024. Those strings do not establish when the archive was extracted or assembled.
WHAT IS ESTABLISHED	A dated advertisement and its older-looking transaction context. Bank references occur inside payment-related fields, rather than as independent evidence of several bank incidents.
ALTERNATIVES	An older export, a mixed collection, a supplier-held archive or a newly obtained copy of historical records. The post does not resolve those possibilities.
LIMITS	The source system, advertised size, population, price and possession claim are unverified. An old record date alone does not settle extraction age.
RESPONSE	Ask the relevant internal or supplier owner whether the claimed schema could describe an authorised export. Assess any genuinely implicated customer or intermediary through trusted incident channels.

Bottom line

An older record date is not an extraction date or a list of bank victims.

Evidence card B01 — 31 Jan 2026

INS | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A seller offered a payment-data archive; transaction-date strings in its sample point to older underlying material.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
Post date is not breach date; beneficiary-bank references do not establish those banks were subject to intrusion.

Evidence card B02 — 4 Feb 2026

AYYUBI | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A poster offered a business-contact dataset with company and contact fields.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
Directory membership is not evidence of unauthorised access to an organisation's systems.

A useful closure record would identify whether the data structure belongs to the organisation, which systems could produce it and whether the same information was previously disclosed. A company name in a directory is insufficient closure evidence in either direction.

B

CASE B

A mobility-payment database bundles several data roles

Evidence card B04 | 4 Mar 2026 | Forum | Mobility and payments

Unverified dataset claim

CLAIM	A 4 March offer described a mobility-payment database with account, vehicle and transaction-related information.
CHRONOLOGY	The post is dated in the report window. Dates inside referenced vehicle or insurance information do not date the seller's acquisition or a provider incident.
WHAT IS ESTABLISHED	The advertiser packaged several kinds of operational information together. The target assertion and database size remain the seller's claims.
ALTERNATIVES	A provider export, a partner dataset, information assembled from several sources or a misleading advertisement. A database description does not establish the collection route.
LIMITS	The material does not establish separate incidents at payment brands, insurers or banks mentioned in its fields. No access to their systems is demonstrated.

RESPONSE	Review retention and permissions for payment-support records and external verification responses. Establish the service boundary before estimating downstream exposure or notifying partners.

Bottom line

Establish the record holder and service boundary before interpreting partner references.

Evidence card B03 — 17 Feb 2026

Mckay | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A poster explicitly re-uploaded a global archive labelled 2023.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
Historical recirculation; advertised global totals cannot be converted to India counts or fresh theft.

Evidence card B04 — 4 Mar 2026

Eliphas | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A seller described a mobility-payment database with account, vehicle and transaction-related fields.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
Provider attribution and database size are unverified; bank fields are not separate bank breaches.

The response should distinguish who holds the record from who is named within it. This distinction determines which owner can investigate an export and which partner may only need a fraud warning. Treating every reference as a victim would misdirect both tasks.

CASE C

C

Supplier cloud access appears in a global menu

Evidence card B06 | 23 Mar 2026 | Forum | Technology suppliers

Unverified access menu

CLAIM	On 23 March, a discounted access menu included two India-based IT-supplier entries, described as an enterprise-software partner and an integrator.
CHRONOLOGY	The retained date establishes when the offer appeared. It does not establish when any alleged access began or how long it remained usable.
WHAT IS ESTABLISHED	A seller advertised entries in a multi-country menu. The advert does not demonstrate working access, data volume or a completed transaction.

ALTERNATIVES	A genuine supplier account, overstated permissions, historical access or a false menu entry. A seller's commercial description does not determine actual reach.
LIMITS	No customer intrusion is established. The supplier's relationship with a customer cannot substitute for evidence of delegated permissions or access to that customer's environment.
RESPONSE	Review supplier administrative identities and revocation procedures. Establish which privileges reach the organisation, then validate genuinely implicated accounts and containment options.

Bottom line

A supplier advert does not establish working access or customer intrusion.

Evidence card B05 — 18 Mar 2026

krisko383 | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A buyer requested banking access and asked suppliers for offers.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
A request is demand, not evidence of access already obtained.

Evidence card B06 — 23 Mar 2026

vexin | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A discounted global access menu included two India-based IT-supplier entries.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
No working access or completed sale verified; do not infer customer compromise.

A buyer's separate request for banking access is a demand signal. It is not evidence that the requested access exists. Supplier ownership and privilege mapping should guide investigation even when a sale narrative suggests a larger downstream incident.

CASE D

D

A travel-finance offer combines documents and credential claims

Unverified documents and access

Evidence card B08 | 21 Aug 2026 | Forum | Travel and finance

CLAIM	On 21 August, a poster described a travel-finance dataset containing identity-verification documents, loan information and claimed cloud or partner credentials.

CHRONOLOGY	The post is a 2026 circulation event. The assertions of freshness and validity are the poster's, rather than independently established dates or account states.
WHAT IS ESTABLISHED	The offer combines document-related and access-related claims. These create different validation tasks even if they appear in one advertisement.
ALTERNATIVES	An old collection, an aggregated lender or partner export, overstated secret validity or a genuine current incident. The post does not settle provenance.
LIMITS	No advertised secret was tested. The claimed record population and current access remain unverified. Document exposure does not establish the validity of associated credentials.
RESPONSE	Use the organisation's own systems to assess genuinely implicated secrets and partner access. Evaluate document misuse and customer-protection needs separately from the advertised population.

Bottom line

Assess document misuse and genuinely implicated credentials separately.

Evidence card B07 — 16 Apr 2026

Antelope | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: An April reply quoted a database description explicitly labelled December 2021.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
The quoted old archive is not a new April 2026 incident; collection provenance remains unresolved.

Evidence card B08 — 21 Aug 2026

updap | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A poster described a travel-finance dataset that combined identity documents, loan information and credential claims.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
Claims of freshness, valid keys and record totals remain unverified; no secrets tested.

An identity document can remain useful for impersonation after a technical secret is rotated. A response that closes only the credential task may therefore leave a customer-protection question unanswered. Conversely, a document claim alone does not justify revoking unrelated service access.

CASE E

E

An education backup is described as openly available

Evidence card B17 | 16 Nov 2026 | Forum | Education

Unverified backup claim

CLAIM	On 16 November, a poster said an education-management backup exposed employee, applicant and academic information.
CHRONOLOGY	This is recent activity within 8–22 November. The post's date does not establish when the alleged backup became accessible or when any information was copied.
WHAT IS ESTABLISHED	A recent advertisement describes an open-backup route. That is the poster's explanation, rather than a verified finding about the service.
ALTERNATIVES	An old export, a current access-control failure, a partner-held backup or an unsupported claim. The alleged route requires investigation by the responsible owner.
LIMITS	The claimed size and applicant population are unverified. Payroll bank references do not establish bank intrusion. Sensitive attributes are not reproduced in this report.
RESPONSE	Review external backup access and education-platform hosting. Preserve relevant logs and determine verified employee or applicant scope before deciding on notification.

Bottom line

Confirm the backup owner, access and scope through authorised evidence.

Evidence card B15 — 11 Nov 2026

protowisher | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A November 11 post described student, staff, attendance and financial tables and claimed elevated access.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
Rows across tables are not unique people; title and schema totals differ. Root or shell access was not tested.

Evidence card B17 — 16 Nov 2026

syn4pz | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A November 16 poster said an open education-management backup exposed employee, applicant and academic information.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
Open-backup claim and volume unverified; personal, financial and sensitive attributes are not reproduced.

A separate 11 November education offer listed several tables and claimed elevated access. Its table rows are not a count of unique students or staff. Treat the dataset assertion and the access assertion as separate propositions, each with its own investigation outcome.

CASE F

F

Medical-payment payees are a distinct exposure question

Evidence card B16 | 14 Nov 2026 | Forum | Health-related payments

Unverified payee-data claim

CLAIM	A 14 November offer described hospital-payment and medical-claims payee information with bank and payment fields.
CHRONOLOGY	The advertisement falls within the recent window. Its underlying data age and claimed volume were not independently established.
WHAT IS ESTABLISHED	The post describes payment-related fields. A medical-payment description does not automatically establish patient clinical-record exposure.
ALTERNATIVES	An intermediary payment export, a payer or provider record set, a mixed historical collection or a misleading label. The advertisement does not identify the verified source.
LIMITS	No named insurer, hospital or bank intrusion is established. A bank named in payee details is a contextual reference rather than evidence about its systems.
RESPONSE	Separate payee-fraud monitoring from clinical-data response. Reconcile genuinely affected payees through trusted finance or insurance channels and investigate the responsible data holder.

Bottom line

Payment context does not establish clinical records or separate bank incidents.

Evidence card B14 — 10 Nov 2026

SensitiveDarkForum | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A November 10 advertisement described an online financial-services dataset and offered purchase by private message.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
Line count is advertised, not verified affected customers; no transaction or extraction date established.

Evidence card B16 — 14 Nov 2026

WSdatabase | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A November 14 offer described hospital-payment and claims-payee records with bank and payment fields.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
No clinical record content or named bank/hospital compromise established; age unknown.

This case illustrates why a broad label can generate the wrong response team. A payee-integrity concern belongs first with finance and the record owner. Clinical privacy assessment requires evidence of clinical content or another applicable data scope.

4.4 Other retained offers and what they do not establish

The following examples extend the validation questions without adding confirmed incidents. The public evidence register in Appendix B connects each card to the section where it appears. [S2]

Card	Retained theme	Decision boundary
B02	Business-contact collection	Directory membership does not establish access to a listed company's systems
B03	A global card archive explicitly labelled 2023	A 2026 re-upload is not fresh 2026 theft
B05	A request for banking access	Demand does not demonstrate possession or a completed purchase
B07	A reply quoting an archive labelled December 2021	A new reply does not establish a new underlying incident
B09	A catalogue of India-labelled datasets	Menu entries can overlap and are not unique verified incidents
B10	Source-code and secret claims involving an IT-services provider	No link to a separately confirmed incident or customer impact is established
B11	SSL-VPN access advertised for an institution	Access and advertised host counts remain unverified

Card	Retained theme	Decision boundary
B12	IT-support and public-service access claims	The asserted relationship between environments remains unresolved
B13	A bank-related claim with competing scope statements	A seller's quotation of a bank statement is not the original official source
B18	A request for recent data	A request does not establish data possession, intrusion or transaction

Evidence card B09 — 5 Sep 2026

updap | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A seller advertised a broad menu of India-labelled banking, retail, transport and business datasets.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
A menu entry is not a distinct verified incident; recency, provenance and overlap are unknown.

Evidence card B10 — 7 Oct 2026

updap | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A repost described stolen source code and embedded secrets at an IT-services provider.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
This is the poster's claim; no basis here for linking it to a separately confirmed event or customer impact.

Evidence card B11 — 12 Oct 2026

Dark_Alpha | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A seller advertised an SSL-VPN access point and a host count for an India-based institution.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
Target, working access and host count unverified; broad role description only.

Evidence card B12 — 30 Oct 2026

Roxanne | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A seller advertised access involving an IT-support company and another domain described as governmental.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
The claimed relationship between the two environments is unresolved; no access tested.

Evidence card B13 — 5 Nov 2026

scarlettgroup | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A seller's post included a bank statement about a limited supplier-platform incident and made broader competing claims.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
Use the bank's actual official filing for confirmed scope; actor volume and core-system assertions remain claims. Slurs and insults omitted.

Evidence card B18 — 20 Nov 2026

Goofe | Forum | Forum | English paraphrase

ORIGINAL

[Paraphrase: A November 20 buyer asked for recent data associated with two India technology or infrastructure organisations.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
Demand-only signal; no dataset possession, intrusion or completed transaction established.

The B13 distinction matters when a criminal advertisement reproduces an apparently official statement. The organisation's actual disclosure should control any confirmed scope. The seller's broader assertions remain a separate claim even when the two appear in the same post.

An August press account quotes an IT supplier describing claimed employee information as basic and more than four years old. The supplier said it found no credible evidence of affected operational or customer environments. This remains its assessment of that material, rather than a finding about unrelated offers. Older information can still support impersonation. [S121]

4.5 Recent activity: 8–22 November

The recent period includes financial-service, education and medical-payment offers, together with a request for recent data. The dates below describe posts, not independently established intrusion times. Public disclosures and authority notices for the same period are handled separately in Chapter 5.

Date	Card	Observed activity	First validation question
10 November	B14	Financial-service dataset advertised	Which controller and service could produce the claimed records?
11 November	B15	Education tables and elevated access claimed	Are table rows being mistaken for unique people, and is access current?
14 November	B16	Medical-payment payee offer	Is the relevant scope payments, clinical information or neither?
16 November	B17	Education backup claim	Who owns the alleged backup and what do authorised logs establish?
20 November	B18	Request for recent organisation-related data	Is this demand only, with no possession evidence?

A close date match between a post and a public disclosure would justify a comparison. It would not establish that the post describes the same dataset or that the advertiser caused the incident. That linkage requires supporting evidence of its own.

4.6 Additional recent claims retain separate boundaries

Three further recent advertisements illustrate different validation questions. They do not add confirmed incidents or establish that organisations mentioned inside a collection suffered separate intrusions. [S2]

Post date	Observed theme	Evidence boundary
13 November	A professional-services archive offered with client references	The archive and its origin are unverified; client names are not evidence of client-system access
13 November	A contact-data catalogue spanning several claimed categories	Advertised populations may overlap; provenance, institutional ownership and downstream use are unverified
20 November	A workforce-application database offer	Configuration fields do not establish that images were taken, credentials remain active or customer devices were accessed

A 22 November global business-contact catalogue also includes India-related context. It is not an India-only population, and companies inside professional profiles are not established intrusion victims. Repeated telecom and education headlines likewise require a chronology before being treated as new events. [S2]

Additional material includes employee-contact files, government-related document claims and multi-country identity or cryptocurrency-user catalogues. A file label does not establish a new intrusion, an authentic government record or a distinct victim for each company mentioned. Some offers describe editable identity products, which differ from evidence that genuine issuer records were stolen. [S2]

Case Q in §5.11 separately examines a provider-specific diagnostic-services access advertisement. It preserves the difference between advertised administrative permissions and proven access or patient-data exposure. [S2]

4.7 A validation record that supports a decision

Start with the exact proposition that matters to the organisation. Examples are whether an active employee account is implicated, whether a field set matches a supplier export or whether a claimed backup belongs to an owned service. Avoid trying to validate an entire seller narrative at once.

Record who can establish each fact. Identity operations can assess account status. Application owners can identify an export schema. Suppliers can explain delegated permissions. Fraud teams can investigate payment patterns. Communications should receive the resulting scope, rather than an unqualified advertisement title.

Each response should have a closure condition. A historical export already covered by remediation differs from current access requiring containment. A mismatch may close one claim without proving the entire advertisement false. Keep unresolved propositions visible in the incident record.

Do not buy access or use advertised credentials to test a claim. Verification should use owned systems, authorised incident-response processes and appropriate supplier channels. This report's observations establish external leads, rather than permission to access third-party systems.

KEY TAKEAWAYS

01

Current posts can advertise older records, request access or bundle several unverified claims.

02

Bank, supplier and institution names inside a record do not establish separate intrusions.

03

Validate one consequential proposition at a time and record the owner, outcome and closure evidence.

CHAPTER 05

Incidents and targeting examples by sector

THIS CHAPTER ANSWERS

Which supported propositions change a sector owner's response?

11

public-source dossiers with distinct evidence boundaries

5.1 A sector decision table 40
5.2 Supplier distribution requires customer-side validation 41
5.3 Deceptive official-looking messages require a trusted route 42
5.4 Government and energy targeting retains the researcher's attribution 43
5.5 Financial authority can be abused without a bank-wide incident 44
5.6 Named disclosures retain their narrow scope 45
5.7 Recent activity: 8–22 November 47
5.8 Other disclosures and explicit boundaries 49
5.9 Further disclosures from the full-window sweep 49
5.10 Recent reported inquiries retain a separate status 50
5.11 A diagnostic-services access claim 52
5.12 Contractor records and operational scope 53

CHAPTER 05

Incidents and targeting examples by sector

IN SHORT

Official disclosures and campaign research show different problems: update distribution, deceptive attachments, payment authority, customer records and certificate assurance. Some sources confirm an incident; others describe campaigns or warnings without a victim count. The dossiers retain those distinctions. Start with the affected function and the strongest supporting evidence, then assign a proportionate validation, containment or continuity task.

5.1 A sector decision table

The rows connect evidence to a response. They do not rank sectors or measure how often Indian organisations were affected.

Sector	Supported evidence	Boundary	First owner
Technology suppliers	Update-infrastructure access and unauthorised distribution [S56]	No national customer total	Supplier security and endpoint response
Public-facing services	Traffic-notice impersonation delivers Android malware [S44]	No confirmed user or loss total	Fraud and mobile support
Enterprises	Tax-themed phishing in vendor research [S62]	Campaign email volume spans several countries	SOC and endpoint teams
Government and energy	Source-attributed espionage research [S61]	No named victim or national prevalence	Identity and service owners
Finance and executives	Messaging-session theft and impersonation warning [S47]	Intervention counts are not confirmed losses	Fraud, treasury and identity
Lenders and payment providers	Official payment-credential campaign [S43][S41]	No universal attribution of financial incidents	Payment operations and application owners
Banking	Customer records identified in a larger advertised collection [S53]	Origin and wider scope remained under investigation	Privacy and customer protection
Digital trust	Weak global certificate-authority keys reported [S54]	Separate service families retain separate scope	Certificate and service owners
Non-financial payment workflows	Business-record and approval abuse warning [S40]	No national victim count	Finance, data and supplier owners

5.2 Supplier distribution requires customer-side validation

CASE G

EScan's update-distribution incident

Technology supply

Vendor-confirmed scoped incident

CONFIRMED	A supplier advisory describes unauthorised access to regional update infrastructure and distribution of an unauthorised file during a limited interval on 20 January. It reports isolation, rebuilding and credential rotation [S56].
BOUNDARY	The vendor's statement distinguishes infrastructure access from a product vulnerability and says customer data were not accessed. These are the vendor's assertions. No India-wide affected-customer count is established here.
INTERPRETATION	A trusted distribution route can require an incident response even when the affected function is outside a customer's ordinary application inventory. Supplier recovery and customer endpoint assurance are different tasks.
RESPONSE	Identify whether the organisation received the affected update, follow the supplier's scoped guidance and examine relevant endpoint evidence. Retain the update version, affected period and investigation decision before declaring closure.

Bottom line

Validate update delivery and endpoint effects without assuming national impact.

The completion test is specific to the customer's own estate. A general statement that the supplier rebuilt infrastructure does not establish that every downstream installation has been checked. Equally, a supplier incident does not prove that every customer received or opened the file.

5.3 Deceptive official-looking messages require a trusted route

CASE H

H

Traffic-notice impersonation and Android malware

Consumer and public services

Official campaign report

OFFICIAL ACCOUNT	CERT-In's March notice reports traffic-penalty impersonation distributing Android malware. It describes permission requests and false financial screens that can expose authentication-related information [S44].
BOUNDARY	The notice supplies a campaign description, without a verified affected-user total or financial-loss figure. Impersonation does not establish access to the legitimate public-service infrastructure.
INTERPRETATION	Urgency and an official-looking theme can move a user from reading a message to installing an application. The defensive question is whether the service can be verified independently.
RESPONSE	Direct users to the genuine service through a known route. If an installation is corroborated, connect mobile triage, account protection and fraud reporting. Do not ask users to forward sensitive personal material to an unverified contact.

Bottom line

An impersonation campaign does not establish intrusion of the impersonated authority.

Customer operations should be able to explain the legitimate process before a campaign becomes prominent. A warning that merely says to be careful gives the user no decision rule. A trusted route and a clear statement about unsolicited installation requests provide a usable test.

CASE I

I

Tax-themed phishing in a multi-country campaign

Cross-sector businesses

Vendor campaign research

VENDOR ACCOUNT	Kaspersky reports tax-themed phishing affecting Indian and other companies, observed from December 2025. Its January–February email figure covers several countries [S62].

BOUNDARY	The report's campaign label and payload findings are the researcher's. The material does not establish a state sponsor or a count of Indian organisations with confirmed intrusions.
INTERPRETATION	A familiar compliance theme can make an unexpected attachment seem relevant. A national tax reference does not identify the sender's location or prove that every recipient suffered an intrusion.
RESPONSE	Test verification of unexpected tax and accounting messages through a known contact. Review relevant endpoint events and unapproved remote access when a credible alert matches the organisation's records.

Bottom line

Multi-country email counts do not measure affected Indian companies.

5.4 Government and energy targeting retains the researcher's attribution

J

CASE J

Government and energy campaign research

Government and energy

Vendor-attributed campaign

VENDOR ACCOUNT	Acronis describes two India campaigns using cooperation and hydropower themes. It reports government-system communications during 12–22 June and attributes the activity to Mustang Panda [S61].
BOUNDARY	Attribution and espionage intent remain the researcher's assessment. The source does not provide a national incident count or identify a public victim for this package.
INTERPRETATION	A plausible sector document can create a route into a privileged workflow. Abuse of a legitimate cloud service does not implicate the provider or establish access to its underlying platform.
RESPONSE	Relevant owners should review the actual account, endpoint and document-handling evidence. Validate privileged sessions and authorised remote tools. Where an operational service is implicated, involve the service owner before choosing disruptive containment.

Bottom line

Source attribution and observed scope remain attached to the technical report.

The government and energy relationship is part of the cited research. It does not connect the campaign to every energy-themed access offer in the underground corpus. A shared sector or national reference is insufficient evidence of a shared operator.

5.5 Financial authority can be abused without a bank-wide incident

CASE K

K

Messaging-session theft and executive impersonation

Finance and communications

Official campaign report

OFFICIAL ACCOUNT	The August warning from the Indian Cyber Crime Coordination Centre (I4C) describes malicious files, endpoint malware, messaging-session theft and false executive payment instructions. It refers to an earlier June advisory [S47] [S48].
BOUNDARY	Notifications to potential victims are intervention measures. They do not establish a corresponding number of completed losses, corporate incidents or independently confirmed victims. S48 is the Hindi version of the same I4C warning.
INTERPRETATION	A familiar messaging identity can carry an unauthorised instruction. Sender familiarity and knowledge of an internal role do not establish payment authority.
RESPONSE	Treasury and finance teams should independently verify high-impact instructions. Identity responders should review linked sessions and relevant endpoints when account misuse is corroborated. Record payment review and technical containment separately.

Bottom line

Verify payment instructions independently and review linked sessions.

CASE L

L

Payment credentials and disbursement workflows

Financial services

Official campaign updates

OFFICIAL ACCOUNT	CERT-In describes campaigns against lenders, fintech businesses, payment providers and wallets. Its October notice identifies misuse of valid payment credentials; its November update uses the CRAFTY FALCON designation [S43] [S41].

BOUNDARY	These are authority-reported campaign findings. They do not attribute every Indian financial incident to that label. The authority's AI-assisted description does not establish AI causality in every transaction case.
INTERPRETATION	Authentication of a payment request does not demonstrate that the underlying business instruction is authorised. A trusted system can submit an instruction outside the intended workflow.
RESPONSE	Reconcile payment authority against independent business records. Review provider privileges, environment separation and exceptional transfers. After corroborated misuse, validate the relevant accounts and integrations before returning to normal operation.

Bottom line

Treat the designation as the authority's, with incident-specific validation.

5.6 Named disclosures retain their narrow scope

M

CASE M

State Bank of India's customer-record disclosure

Banking

Scoped public investigation

OFFICIAL ACCOUNT	State Bank of India says alerts arrived on 16 October. Preliminary analysis of approximately 375,000 records identified 3,897 customer records containing personal information. Investigation of authenticity, completeness, source and scope continued [S53].
BOUNDARY	The larger collection is not a confirmed affected-customer total. The bank reported no material impact on core operations. Wider reporting supports naming the disclosed case, without expanding its established scope [S68].
INTERPRETATION	Finding customer records and identifying their source are separate propositions. A customer-facing domain, file label or personal field does not establish the initial access route.
RESPONSE	Privacy and customer-protection owners should assess validated record categories and credible follow-up abuse. Technical responders should preserve the provenance investigation rather than assume the advertised collection originated from the bank's core systems.

Bottom line

Identified customer records do not authenticate the larger advertised population.

A 3 November account quotes SBI's chairman as saying containment, vulnerability assessment and customer contact were completed. Root-cause analysis remained underway. This updates the October matter; it is not a new incident or activity within the closing fortnight. The statement does not authenticate the entire advertised population. [S109]

Reporting separately quotes a communications supplier's denial of connection to the bank-data event. A supplier relationship does not establish a source or an entry route. The denial remains the supplier's statement and does not close the data-origin question. [S130]

CASE N

N

EMudhra's global certificate-key issue

Certificate services

Officially acknowledged certificate issue

OFFICIAL ACCOUNT	eMudhra says eight global TLS intermediate certificate authorities had weak keys generated during an April 2025 ceremony. Its October statement says root-cause investigation continued; a later filing announces an external independent review [S54][S55].
BOUNDARY	The company denies an infrastructure intrusion and customer-data breach. It says Indian digital-signature and eSign services are separate and unaffected. Wider reporting establishes public coverage, without proving theft of customer information [S69].
INTERPRETATION	A certificate-assurance problem can require operational action without establishing customer-data exfiltration. Separate global TLS dependencies from other products instead of applying one headline to every service.
RESPONSE	Certificate owners should inventory the actual chain used by their services, follow relevant trust-store guidance and verify replacement where applicable. Record service-specific decisions and continuity tests while the source investigation develops.

Bottom line

Global TLS certificate scope and India signature services are separate.

The dates matter in both cases. An October disclosure does not make every underlying record or key-generation event an October incident. Preserve the observation, publication and underlying-event dates separately.

5.7 Recent activity: 8–22 November

The closing fortnight contains an incident update, official warnings and a regulatory implementation phase. Publication during the fortnight does not establish that every underlying event began then. The table is not a national incident census.

Ransompedia records 16 listing claims dated 8–22 November, within the 254-record India total [S3]. They are part of that total, not additional incidents. Their publication dates do not establish intrusion dates.

Date	Item	Evidence status	Immediate decision
9–14 November	Virtual-asset service suspension and revised loss estimate	One incident with an earlier 6 November detection [S76] [S77]	Use the controlling update and assess service, wallet and customer-data questions separately
13 November	The Gentlemen ransomware advisory	Official capability warning; no India victim count [S65]	Validate relevant access paths and independent recovery
13 November phase; 14 November notice	Consent Manager registration	Regulatory phase, not an intrusion [S49][S50]	Update the implementation register without starting future duties early
20 November	Business-payment workflow warning	Official categories of incidents, without a public victim total [S40]	Reconcile records, approval authority and provider access

The 4 November financial campaign update and the 5 November payment-system directions precede this recent window. They remain relevant earlier-November context, without being re-dated to the closing fortnight [S41] [S15].

CASE O

Business-record abuse reaches non-financial payment workflows

Business payment workflows

Official incident-category report

OFFICIAL ACCOUNT

CERT-In's 20 November warning describes unauthorised transactions outside the banking and financial-services sector, including service-provider-operated processes. It identifies altered business records and approval relationships [S40].

BOUNDARY

The warning also discusses agentic offensive frameworks in a separate strand. It does not establish that every financial example used AI, nor does it supply an affected-organisation count.

INTERPRETATION	A payment can pass through an expected technical path while lacking genuine business authority. Checking only the payment interface leaves the source record and approval change unexplained.
RESPONSE	Finance, data and supplier owners should independently reconcile authoritative records and high-risk changes. Preserve relevant logs and suspend an affected integration when justified by corroborated evidence. Reopening requires a documented authority and reconciliation test.

Bottom line

Verify the business records underlying an otherwise legitimate payment.

P

CASE P

Unocoin's revised incident assessment

Virtual-asset services

Company-reported incident update

OFFICIAL ACCOUNT	Unocoin's 14 November update estimates approximately US$200,000 lost from three operational hot wallets. It supersedes the preliminary no-loss assessment carried in earlier reporting [S76][S77].
CHRONOLOGY	The operator says suspicious activity was detected on 6 November. Further activity on 9 November led to service suspension. These are phases of one incident, not separate events created by each update.
BOUNDARY	Customer-account and identity-data scope remained under investigation. The operator said it had not found evidence of KYC-document access and that its custody provider's infrastructure was unaffected. The precise mechanism and final scope remained unresolved [S76].
RESPONSE	Use the latest controlling statement when making customer and financial decisions. Preserve the distinction between a reported wallet loss, possible data exposure and provider-system impact. Require service-specific recovery and investigation evidence before treating technical restoration as closure.

Bottom line

Use the controlling revised assessment and preserve unresolved customer-data scope.

5.8 Other disclosures and explicit boundaries

Published	Supported proposition	Limit and response
20 February	A pharmaceutical manufacturer reports unauthorised access to factory server data [S57]	No specific malware or actor established; restrict relevant access and investigate data scope
27 March	An automotive supplier confirms ransomware after a suspected incident the previous day [S58]	Company says core operations were unaffected; do not infer production interruption or final loss
2 April	CERT-In warns about open-source dependency incidents [S45]	Global dependency risk, without an Indian downstream-victim count; validate actual installed components
11 April	English and Hindi reporting relays a courier company's account of contained phishing and impersonation exposure within its parent group [S126][S127]	Data and financial-impact exclusions remain the company's statements; this does not establish data theft or an incident across the entire group
15 October	CERT-In distinguishes agent-evaluation authorisation violations from attacker use [S42]	Separate categories; do not merge them into one criminal campaign
22 October	A cloud provider acknowledges an extortion attempt and samples under review [S60]	Confirmed contact does not confirm the entire claimed dataset or customer impact
28 October	A supplier reports misuse of a foreign subsidiary's mailbox for false payment instructions [S59]	Cross-border subsidiary context; no confirmed intrusion into a bank in India follows

5.9 Further disclosures from the full-window sweep

The following items add distinct service boundaries or later assessments. They are not added to the post or listing counts. The dates are publications unless the row states an event date.

Publication	Supported account	Essential boundary
10 May	A newspaper reports a police inquiry after a complaint about commercial circulation of trade records and quotes officials as matching samples [S107]	Original complaint and final findings were unavailable; no current network entry route or national affected population is established
18 May; October update	HDFC Asset Management Company disclosed a 16 May incident, then reported a completed assessment and unaffected business continuity [S82][S83]	The actor's data-volume claim remains unverified; interim court relief is not final adjudication [S84]

Publication	Supported account	Essential boundary
22 June	Reuters quoted an electronics manufacturer's confirmation of an incident on some systems and no operational impact [S92]	Advertised customer designs and data volumes were not independently authenticated; no customer intrusion follows
26 June	Bajaj Auto confirmed ransomware affecting the parent and technology subsidiary on 23 June [S90][S91]	Key functions were operating normally on 26 June; no shutdown, actor, entry route or data-theft amount is established
27 July; 5 August assessment	Reporting quoted a bank's employee-email access disclosure; a rating agency described one affected account or credential [S93][S94]	The investigation continued; core banking access and the actor's larger volume were not established
25 October	CoinDCX acknowledged a 15.99 million USDT loss on 21 October through deprecated operational wallets [S85] [S86]	The company absorbed the loss and reported active services unaffected; the older 2025 loss is a different event
28 October	A building-materials manufacturer disclosed a 21 September website incident involving unauthorised code and an administrator account [S87]	The company reported containment, no data loss and no business disruption; no ransomware label is inferred
30 October	A lender says it is investigating a potential leak involving a supplier-hosted vehicle-loan platform [S112][S113]	The lender reports its systems and services unaffected; no affected-customer total or authenticated advertised population is supplied

These disclosures show why a product, parent company and subsidiary cannot be treated as interchangeable. They also show why a later assessment should be linked to the earlier incident rather than counted again.

The eScan case also has English and Russian technical research. Those sources describe multi-country infection attempts, rather than a confirmed India customer count. They identify an invalid file signature; the report does not describe a valid vendor-signed malicious package. [S95][S96][S97]

5.10 Recent reported inquiries retain a separate status

The reports below add closing-period visibility. Their source limitations differ from the original disclosures in the preceding sections. They remain attributed reports, with generic organisation roles.

Published	Attributed reporting	What remains unresolved
15 November	Regional reporting describes an industrial-clearances portal inquiry, restoration from backups and a suspected October incident [S102]	Direct primary notice was unavailable; possible data theft was still being examined

Published	Attributed reporting	What remains unresolved
17 November	Moneycontrol reports a bank clarification denying a reported cyber loss and system impact, and says the earlier story was withdrawn [S114]	Attribute the denial and reported correction; the alleged amount is not a verified loss and no new incident is established
17–18 November	Two press accounts quote police describing unauthorised use of a senior public-service official's messaging account and status posts [S134][S135]	No entry route, actor, wider-system access or financial loss is established; verify unexpected contact through a separate trusted route
19 November	Regional reporting describes recovery of encrypted files from one local police computer and quotes a technical authority [S100]	No primary forensic report or national police-network impact is established
21 November	A customer-engagement provider confirmed limited cloud access through a supplier account to Moneycontrol [S99]	The provider-client denominator is not a share of downstream people; a reported client notice was not independently authenticated
21 November	PTI reports a police inquiry into an attempted sale of purported personnel data from a career-registration test platform [S103]	Authenticity, scope and the alleged method remained under examination; the advertised population is not confirmed

An 18 November foreign-customer warning about attempted access to a hosted support system supplies additional supplier context. The cited reporting does not establish successful access, a provider-wide incident or an Indian affected population. It is separate from the customer-engagement provider account above. [S128][S129]

A separate regional healthcare-technology report describes an October complaint and investigation. Its technical impact and ransom amounts remain reported allegations. The report retains that role-based lead without naming a victim or treating an alleged demand as a paid loss. [S98]

The full sweep also records unresolved payment-provider, airline-processor and customer-notification leads. These do not expand the confirmed subset. Discovery dates and recycled historical stories are not treated as new incident dates.

The cases support identity, supplier, data and recovery controls. They do not identify one national entry route or a common operator. Each owner should record what is confirmed, what remains open and which evidence would justify changing the response.

5.11 A diagnostic-services access claim

CASE Q

A diagnostic-services provider access advertisement

Evidence card B19 | 22 Oct 2026 | Forum | Diagnostic services

Unverified access advertisement

CLAIM	A 22 October post advertised server, database and service credentials associated with a private diagnostic-services provider in India. The seller described administrative permissions and connections to other services.
CHRONOLOGY	The post establishes an advertisement date. It does not establish when any access began, whether the credentials remained valid or whether a transaction occurred.
WHAT IS ESTABLISHED	The seller presented a provider-specific access offer. The description includes Windows and database environments, with service credentials claimed rather than independently validated.
ALTERNATIVES	Genuine access, old or revoked credentials, overstated privileges, an unrelated environment or a false listing. The advertisement does not resolve those possibilities.
LIMITS	No patient-record exposure, database extraction or intrusion at connected hospitals, doctors or corporate customers is established. A description of the provider's relationships does not establish access to those partners.
RESPONSE	The provider's identity and diagnostics-service owners should assess genuinely matching accounts through owned evidence. Review delegated access and integration dependencies, preserve logs and plan containment that protects essential diagnostic services.

Bottom line

An advertised provider identity does not establish working access, patient-data exposure or intrusion at a connected hospital.

Evidence card B19 — 22 Oct 2026

Alias omitted | Forum | Forum | English paraphrase

ORIGINAL

[English paraphrase: A seller advertised server, database and service credentials associated with an India-based diagnostic-services provider.]

TRANSLATION

English paraphrase, not a verbatim quotation.

Held
A dated post containing the advertised claim or request.

Not established
No working access, credential validity, patient-record exposure, customer intrusion or completed sale is established.

This access claim is separate from Case F's medical-payment payee offer. One concerns advertised permissions at a diagnostic service; the other concerns a claimed payment record set. Their dates, actors and data descriptions do not establish a common incident. [S2]

5.12 Contractor records and operational scope

R

CASE R

A contractor disclosure requires separate host and operator evidence

Infrastructure and engineering

Scoped contractor disclosure

PUBLIC ACCOUNT	Reuters's 15 July report quotes an infrastructure contractor acknowledging a partial data incident on a third-party-hosted server. The hosting provider described suspicious activity on 29 May and its containment. [S117]
CHRONOLOGY	The host said it learned of an external data claim at the end of June. The May activity, later claim and July disclosure are separate dates within the account, rather than three newly established incidents.
DOCUMENT BOUNDARY	Reuters could not independently authenticate purported project files. A follow-up reports the operator's 15 July clarification limiting the files to non-sensitive facility documents. That remains the operator's assessment as reported. [S117][S118]

ALTERNATIVES AND LIMITS	A scoped contractor-held dataset, an overstated external collection or a mixture of older material remain different propositions. The disclosed host activity does not authenticate the full advertised document set or establish access to an operator's systems.
RESPONSE	Engineering, procurement and incident owners should identify the actual data holder and verified file categories. Obtain the contractor and host chronology, preserve access evidence and separately assess any justified operational concern. A document claim alone cannot settle the operational question.

Bottom line

Contractor data, host activity and operator-system access require separate supporting evidence.

The contractor, hosting provider and project operator are distinct parties. Their statements answer different questions. Do not infer a common scope from their commercial relationship, and require service-specific evidence before changing an operational continuity decision. [S117][S118]

KEY TAKEAWAYS

01

Keep campaign notices, confirmed incidents, source claims and regulatory updates distinct.

02

Preserve each disclosure's dates, affected service and explicit exclusions.

03

Give the relevant service, identity, fraud or data owner a validation task and a reviewable closure test.

CHAPTER 06

Hacktivism, DDoS and the availability question

06

THIS CHAPTER ANSWERS

How should defenders distinguish a political claim, malicious traffic and a verified service impact?

3

questions before an availability statement: service, impact and evidence

6.1 A public statement with a defined boundary 56

6.2 Timeline of reported activity and claim boundaries 56

6.3 Claim versus official reporting 57

6.4 Political rhetoric is evidence about the speaker 57

6.5 A service-status decision that can be tested 58

CHAPTER 06

Hacktivism, DDoS and the availability question

IN SHORT

Politically framed cyber claims require the same evidence discipline as commercial extortion. A claimant's target list does not establish a sustained outage, data theft or the operator's identity. In June, CBSE publicly described coordinated attacks and mitigation, while reporting no detected unauthorised access or data breach. That statement does not identify a hacktivist. Keep the claim, operational measurements and attribution separate, and rehearse an availability statement with the service owner.

6.1 A public statement with a defined boundary

The Central Board of Secondary Education (CBSE) issued a statement on 5 June after attacks against a recently launched online service. It said it had complained to Delhi Police and described mitigation. The authority reported no detected unauthorised access or data breach. Its statement did not attribute the activity to a named group. Press reporting described the same service episode. [S74][S75]

That is useful operational evidence, with a specific limit. The source establishes what the operator reported. It does not establish a connection to any underground post, the nationality of an attacker or a wider campaign. An origin address and an operator's identity are different propositions.

A service team should make the same distinctions in its own incident record. Traffic received, requests rejected, customer transactions completed and downtime each answer a different question. Combining them into a single attack total conceals the business outcome. A traffic figure cannot substitute for a tested customer journey.

6.2 Timeline of reported activity and claim boundaries

The timeline below combines dated public reports relevant to availability and escalation. It does not assign a common actor to the events. The January supplier issue and the June portal issue are separate incident families.

22 Jan 2026	**eScan** Confirms unauthorised activity in update infrastructure; national customer impact is not established
5 Jun 2026	**CBSE** Describes coordinated attacks and mitigation; reports no detected unauthorised access or data breach
22 Oct 2026	**Cloud service provider** Reports an extortion approach; the full claimed dataset remains under validation
13 Nov 2026	**CERT-In** Publishes ransomware guidance; this is an advisory, not a newly confirmed India incident
20 Nov 2026	**CERT-In** Reports abuse of payment workflows beyond financial firms; availability and payment integrity require separate investigation

The dates are disclosure or advisory dates. They do not establish intrusion dates. The 13 and 20 November entries fall within 8–22 November; earlier entries provide context. [S56][S60][S65][S40]

6.3 Claim versus official reporting

The panel shows how to handle an availability claim when the evidence does not support a claimant-to-incident link. Blank attribution is an unresolved question, rather than an invitation to fill in a group name.

Point	Actor claim	Official account	Press reporting
June portal activity	No actor claim is linked to this incident in the verified evidence	CBSE describes coordinated attacks and mitigation [S74]	Reporting relays the operator's statement [S75]
Service outcome	No independently established claimant outage figure	The operator describes its mitigation; no general service-loss measure is established here [S74]	Successful applications and malicious traffic have different units [S75]
Data access	No linked actor evidence establishes data theft	No detected unauthorised access or data breach, according to CBSE [S74]	Reporting does not replace the operator's incident investigation [S75]
Identity and motive	A political label would require its own evidence	No named actor attribution in the cited statement [S74]	No common operator is established by repetition of the statement

A July press account separately relays a government ministry's denial of a current intrusion after documents attributed to a public-sector body were offered underground. The ministry described the material as older or altered. That assessment remains attributed to the ministry; it does not independently authenticate every document offered underground or establish an operator. [S110]

A November financial-loss story has its own correction chronology. Moneycontrol reports a 17 November bank clarification and says the original 13 November story was withdrawn on 15 November. Preserve the reported denial and correction together, rather than carrying an unverified amount into loss totals. [S114]

A future actor claim should be retained as a separate source. Investigators can compare its time and claimed service with operational logs. Similar timing would support further investigation, but would not establish responsibility on its own.

6.4 Political rhetoric is evidence about the speaker

The May 2025 India–Pakistan conflict falls outside this report's observation window. A 2026 post referring to it remains a 2026 statement by its author. Such a reference cannot date the underlying activity or confirm state involvement. Older campaign descriptions should not be imported into the current incident count.

The same standard applies to references to Kashmir, China, Bangladesh, religion, elections, parties or caste. This report takes no position on those subjects. Where an actor invokes one, only the security-relevant claim belongs in the evidence card. Slurs and promotional rhetoric add no defensive value and are omitted.

The language of the summary must remain as careful as the source note. A card labelled as a claim cannot become a confirmed attack in a heading or takeaway. Similarly, a researcher attribution must remain attributed when shortened into a diagram.

6.5 A service-status decision that can be tested

Before an incident, identify the service journey whose failure would matter. Examples include a completed payment, a submitted application or a booking confirmation. Name the owner who can establish whether that journey works and the communication team that can describe the result.

During a claim, preserve four records separately: the claimant's statement, network and application measurements, the service owner's account and any external observation. Document the time covered by each. A brief availability check from one vantage does not establish a sustained national outage.

Containment should follow the operational evidence. Malicious traffic may justify mitigation even when attribution is unknown. A data-theft claim may justify preserving logs while authenticity is assessed. Neither decision requires amplifying the claimant's political message.

After recovery, test the customer journey and document remaining limitations. Reconcile the first public statement with the incident record. If the facts change, issue a correction through the same agreed channel. The completion evidence is a dated service test and an approved account of what is known.

KEY TAKEAWAYS

01

CBSE's June statement describes mitigation and no detected data breach, without a named actor attribution.

02

Actor rhetoric, service impact and attribution remain separate evidence questions.

03

Prepare service-owner tests and status statements before the next availability claim.

CHAPTER 07

Threat actors and supported relationships

07

THIS CHAPTER ANSWERS

Which actor labels are supported, how do they connect to India, and what should those connections change?

254

India-labelled extortion listings in the observation window

7.1 Relationships that the sources support 60
7.2 Extortion is distributed across many labels 61
7.3 Espionage reports need source-specific confidence 64
7.4 Fraud and remote-access campaigns have different objectives 65
7.5 Technique matrix and investigation questions 67
7.6 Advisories and a separate inventory baseline 68

CHAPTER 07

Threat actors and supported relationships

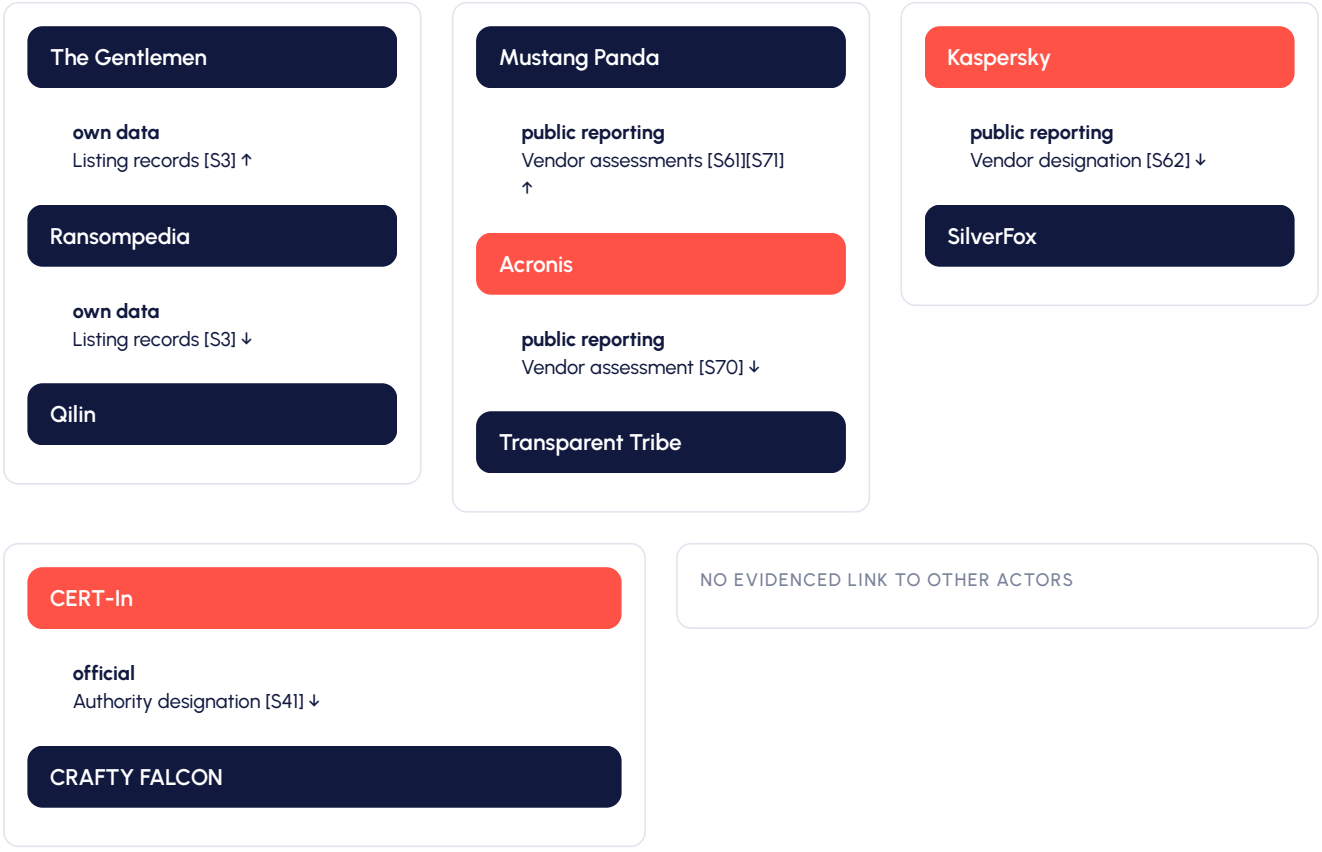
IN SHORT

India-relevant evidence spans extortion listings, vendor-described espionage and financial campaigns reported by CERT-In. These sources support different propositions. A leak-site label identifies a published claim. A technical report may support a campaign attribution while leaving victim outcomes unresolved. CERT-In's CRAFTY FALCON designation belongs to the authority. Preserve those distinctions when routing alerts, and assign each signal to identity, infrastructure, fraud or continuity owners.

7.1 Relationships that the sources support

The relationship map connects a source or observed label to the proposition it supports. It does not connect unrelated personas into a common organisation. No shared operator between the extortion labels, espionage reports and financial campaign is established here.

Own post · Relay · Official statement · Public reporting · Our observation



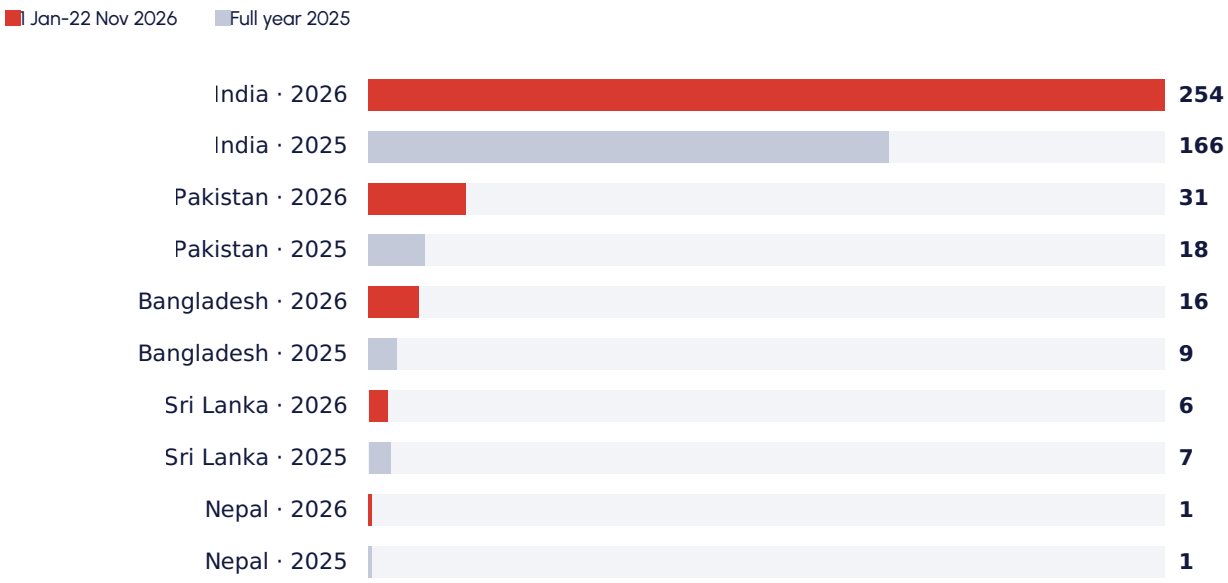
Connection	Evidence type	Supported proposition	Limit
Ransompedia to extortion labels	Own data	Published India-labelled claim records [S3]	Not confirmed encryption, loss or a common affiliate
Acronis to Mustang Panda	Vendor research	Source-assessed campaign links [S61][S71]	Confidence and targeting differ between reports
Acronis to Transparent Tribe	Vendor research	Source-assessed attribution of startup-themed material [S70]	Not confirmation of a named startup intrusion
Kaspersky to SilverFox	Vendor research	Reported tax-themed campaign [S62]	The reported email denominator spans several countries
CERT-In to CRAFTY FALCON	Official statement	Authority designation for a financial campaign [S41]	Not attribution of every financial incident
Seqrite to recruitment and tax lures	Vendor research	Analysed malware-delivery chains [S72][S73]	No national affected-user count

7.2 Extortion is distributed across many labels

Ransompedia records 254 India-labelled listings published during 1 January–22 November 2026. The equivalent counts are 31 for Pakistan, 16 for Bangladesh, six for Sri Lanka and one for Nepal. The countries differ in size, industry and visibility; the table does not rank national security. [S3]

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

India has the largest observed listing count among the five selected regional economies



Source: Ransompedia listing claims [S3]. 2026: 1 January–22 November; 2025: full calendar year. Different periods and source visibility; not a national security ranking.

The leading India labels are shown below. A label can span multiple affiliates or change its operating arrangements. Its presence is useful for matching a claim and preparing continuity decisions, rather than inferring an initial access method.

Label	Listings	Reading
Thegentlemen	36	Published extortion claims under this source label
Lockbit5	14	Source label retained without implying continuity of every operator
Krybit	14	Published claims; victim outcomes need separate confirmation
INC Ransom	11	Published claims; no common affiliate inferred
0apt	10	A source label, not a finding of state affiliation
Qilin	9	Published claims, rather than verified affected organisations
Other labels	160	Remaining claim records across the source's labels
Total	254	Listing records, not a national incident census

The six displayed labels account for 94 of 254 listings, or 37.0%. The remainder is 160 records. No group share is a measure of successful encryption or financial harm. The largest primary industry category is manufacturing, with 51 listings; industry categories in this source differ from the selected-domain sectors. [S3]

The Gentlemen

Extortion listing label | No state attribution made by this report

IN INDIA, 2026

2026

36 India-labelled listing records; CERT-In advisory issued 13 November

CLAIMED TARGETS

India-labelled extortion listing claims; underlying victim outcomes remain unconfirmed

SEEN IN PUBLIC REPORTING

[S3] 36 India-labelled listing records; CERT-In advisory issued 13 November

[S65] 36 India-labelled listing records; CERT-In advisory issued 13 November

OUR ASSESSMENT

Listing records are criminal claims. The advisory does not independently confirm each listed incident.

CONFIDENCE

Confidence attaches to the stated proposition; underlying outcomes require their own evidence.

Qilin

Extortion listing label | No state attribution made by this report

IN INDIA, 2026

2026

9 India-labelled listing records

CLAIMED TARGETS

India-labelled extortion listing claims; no uniform access route established

SEEN IN PUBLIC REPORTING

[S3] 9 India-labelled listing records

OUR ASSESSMENT

Use a matching claim as an investigation and continuity lead; do not infer encryption or an initial access route.

CONFIDENCE

Confidence attaches to the stated proposition; underlying outcomes require their own evidence.

CERT-In issued guidance on The Gentlemen on 13 November. Its publication and the retained listing labels are separate evidence lines. The advisory supplies defensive context without authenticating each India-labelled claim. The report makes no operator-level linkage between the advisory and individual listed organisations. [S65]

7.3 Espionage reports need source-specific confidence

Mustang Panda

Espionage attribution per Acronis | Attribution and confidence belong to Acronis

IN INDIA, 2026

2026
Government/energy research and a separate banking-themed strand

CLAIMED TARGETS

Government and energy research; a separate banking-themed delivery strand

SEEN IN PUBLIC REPORTING

[S61] Government/energy research and a separate banking-themed strand

[S71] Government/energy research and a separate banking-themed strand

OUR ASSESSMENT

June attribution is high confidence per Acronis; April linkage is moderate. Victim outcomes and populations differ.

CONFIDENCE
Confidence attaches to the stated proposition; underlying outcomes require their own evidence.

Acronis's June research describes India government and energy activity, while its April report assesses a banking-themed LOTUSLITE strand. The former carries the vendor's high-confidence attribution; the latter carries moderate confidence. These are different technical reports, rather than a common measured population. [S61] [S71]

For defenders, the useful connection is behavioural. Review whether a document-opening process can launch a script or an unexpected signed program. Examine the library it loads and the identity under which it runs. Treat an approved cloud destination as a service requiring context, rather than proof that traffic is benign.

Transparent Tribe

Espionage attribution per Acronis | Attribution belongs to Acronis

CLAIMED TARGETS

Startup-themed malicious delivery material described by Acronis

IN INDIA, 2026

2026
Startup-themed malicious delivery material

SEEN IN PUBLIC REPORTING

[S70] Startup-themed malicious delivery material

OUR ASSESSMENT

A malicious lure and sample do not confirm intrusion of a named startup or government responsibility.

CONFIDENCE
Confidence attaches to the stated proposition; underlying outcomes require their own evidence.

Acronis attributed startup-themed delivery material to Transparent Tribe with high confidence. That is the vendor's assessment. A lure or sample associated with India does not confirm an intrusion at the organisation it imitates. The report does not assign responsibility to a government. [S70]

A startup or investor should make due-diligence document handling part of endpoint policy. Run unfamiliar files in an approved review environment. If a lure was opened, preserve endpoint evidence and investigate subsequent process activity before determining the incident's scope.

Kaspersky's August release separately includes India in its multi-country HoneyMyte/CoolClient account and uses Mustang Panda as an alias. This is Kaspersky's campaign framing. It does not establish a link to each Acronis case, a named Indian victim or an India-specific affected population. [S105][S106]

7.4 Fraud and remote-access campaigns have different objectives

SilverFox

Campaign designation per Kaspersky | No state attribution made by this report

IN INDIA, 2026

2026
Tax-themed malware campaign spanning several countries

CLAIMED TARGETS

Tax-themed lures aimed at companies in India and other countries, per Kaspersky

SEEN IN PUBLIC REPORTING

[S62] Tax-themed malware campaign spanning several countries

OUR ASSESSMENT

The source's email volume is multi-country and is not a count of affected Indian companies.

CONFIDENCE

Confidence attaches to the stated proposition; underlying outcomes require their own evidence.

Kaspersky's SilverFox research describes tax-themed email and remote-access payloads across several countries, including India. Its reported volume is not an India-only denominator. The source does not establish a state sponsor or count confirmed Indian company intrusions. [S62]

CRAFTY FALCON

Financial campaign designation per CERT-In | Designation belongs to CERT-In/CSIRT-Fin

IN INDIA, 2026

2026

October campaign report updated 4 November

CLAIMED TARGETS

Financial institutions and payment processes described by CERT-In

SEEN IN PUBLIC REPORTING

[S41] October campaign report updated 4 November

[S43] October campaign report updated 4 November

OUR ASSESSMENT

Do not attribute every financial incident or every 20 November workflow category to this designation.

CONFIDENCE

Confidence attaches to the stated proposition; underlying outcomes require their own evidence.

CERT-In's designation is relevant to financial incident handling, but it should not become a catch-all actor name. The 20 November business-workflow notice describes a broader scope. It does not establish that every reported workflow incident and every agent-assisted intrusion has the same operator. [S41][S40]

Seqrite separately analysed recruitment and GST-refund lures. The impersonated institutions are not confirmed intrusion victims. Unapproved remote-management enrolment and scripts launched from attachments are useful investigation leads, regardless of the campaign name. [S72][S73]

Cyber Swachhta Kendra's 6 February notice separately describes an India-targeted espionage campaign using tax impersonation and remote-management software. The impersonated authority is a lure, rather than a confirmed intrusion victim. The notice supplies no named victim, national affected-user total or exploited CVE. [S79]

7.5 Technique matrix and investigation questions

The matrix uses behaviours described in the cited technical reports. The ATT&CK identifiers are analyst mappings checked against current MITRE definitions. A mapping is not a deployed detector or evidence that every behaviour occurred at every target. [S26][S27][S28][S29]

ANALYST MAPPINGS OF SOURCE-DESCRIBED BEHAVIOURS, BY TACTIC

Initial Access	Execution	Persistence
T1566.001 Spearphishing Attachment	T1059.001 PowerShell	T1053.005 Scheduled Task
	T1574.001 DLL	

Analyst mappings of behaviours described in the technical reports [S61][S70][S71][S72][S73], checked against current MITRE definitions [S26][S27][S28][S29]. The source behaviours and analyst mappings are distinct; no deployed detector or shared operator is implied. [S26]

Behaviour	Source context	Investigation question
Spearphishing attachment	Government, energy and startup-themed research [S61][S70]	Did opening an unfamiliar attachment lead to new process activity?
Script execution	Banking, recruitment and tax-lure research [S71][S72][S73]	Which user and parent process launched the interpreter?
DLL sideloading	Mustang Panda-related reports [S61] [S71]	Did a signed program load an unexpected neighbouring library?
Scheduled persistence	Recruitment-themed research [S72]	Who created the task and which account can alter its payload?
Cloud-service command traffic	Government/energy and recruitment reports [S61][S72]	Is the process and account authorised to use that service?
Remote-management enrolment	Recruitment and messaging malware reports [S72][S46]	Does the tool's tenant and controller belong to the organisation?

A matching technique is not actor attribution. Common scripts, libraries and cloud services appear in legitimate administration and unrelated campaigns. Escalate on the sequence, permissions and business context, rather than the name alone.

7.6 Advisories and a separate inventory baseline

The technical campaign reports above do not identify an exploited CVE. They must not be rewritten as vulnerability-led cases. A separate NVD check verified CVE-2025-55182, an older React Server Components remote-code-execution issue. It is a software-inventory example, not a newly established India incident. [S7]

NVD identifies affected React server packages at versions 19.0.0, 19.1.0, 19.1.1 and 19.2.0. The vendor's original fixes were 19.0.1, 19.1.2 and 19.2.1. These address that vulnerability; they are not a statement that those versions satisfy every later advisory. Use a currently supported release and check the applicable framework guidance. [S7][S25]

The practical test is whether an internet-facing service actually includes an affected server package. A client-only application is a different exposure question. Record the installed version, the responsible team and the vendor-supported remediation. Then verify the running deployment, rather than only the build manifest.

KEY TAKEAWAYS

01

Ransompedia lists 254 India-labelled extortion claims, without confirming their operational outcomes.

02

Vendor and authority attributions remain attached to their sources and stated confidence.

03

Hunt the documented process and permission changes before assigning a campaign name.

CHAPTER 08

Fraud, identity and payment authority

THIS CHAPTER ANSWERS

How can identity and business information become an unauthorised payment instruction?

Separate

complaints, transactions, protected funds and confirmed losses

8.1 The supported chain and its limits 70
8.2 Account information is not payment authority 70
8.3 Familiar accounts can distribute untrusted files 71
8.4 Official fraud figures measure different outcomes 71
8.5 Enforcement is case-specific evidence 72
8.6 Payment-card observations retain a narrow scope 72
8.7 Customer support is part of containment 73

CHAPTER 08

Fraud, identity and payment authority

IN SHORT

Official warnings connect deceptive files, stolen messaging sessions, executive impersonation and unauthorised payment workflows. These are different routes to abuse, without a single national loss denominator. Underground offers supply separate claims about accounts and information. Connect customer contact, endpoint evidence, account authority and transaction review under one escalation owner, then verify high-impact requests through a trusted independent route.

8.1 The supported chain and its limits

I4C's warning describes endpoint malware followed by messaging-session theft and false payment instructions [S47]. CERT-In separately describes payment-credential misuse and altered business records [S43][S40]. These sources establish related defensive problems, without establishing one shared operator.

The following is an **analytical model** for response planning. It does not claim an observed transaction chain between the report's underground posters, malware operators and recipient accounts.

Stage	Possible abuse	Defensive interruption
Context obtained	Personal, commercial or account information supplies credibility	Validate provenance and minimise unnecessary disclosure
Trusted identity misused	A familiar messaging or email account carries a false instruction	Verify the request through an independently known channel
Business authority changed	A beneficiary, record or approval relationship is altered	Reconcile against an independent authoritative record
Payment attempted	An apparently valid technical request reaches a payment service	Check business authority, transaction context and exceptions
Further contact follows	The same context supports another request	Retain the incident link and update customer guidance

Each transition needs evidence. An advertised identity file does not prove an unauthorised message was sent. A message does not establish a completed transfer. A suspicious transfer does not by itself identify the source of personal information.

8.2 Account information is not payment authority

An advertisement can offer access, request account stock or promote a lookup service. Those propositions differ. A request to buy an account is not proof of possession, and a seller's stated price is not an observed transaction.

For an owned account alert, determine whether the identity belongs to an employee, customer, contractor or unknown person. Validate current status and earlier remediation. A valid identity may still lack authority for the requested change or transfer.

Financial and customer-service teams should therefore test the entire decision. Can a person who knows a realistic name, balance-related fact or invoice reference obtain a high-impact change? Does the operator rely on a new number supplied in the same message?

Use synthetic information in the exercise. The successful control rejects the unauthorised request, records why it was rejected and provides a legitimate recovery path. An exercise that locks out the real user without a safe alternative is incomplete.

8.3 Familiar accounts can distribute untrusted files

CERT-In's June warning describes malicious scripts sent through already-affected messaging accounts, presented as invoices or statements [S46]. The sender's familiar profile does not make an unexpected file safe. The notice does not provide an India-wide affected-user count.

After a credible match, review the endpoint and linked account sessions together. A restored endpoint does not establish that an unauthorised linked session has ended. A changed account password does not establish that unapproved remote software has been removed.

Finance and executive-support teams need an independent verification route that remains available during an account incident. Record genuine contact details before the incident. A replacement contact supplied by the suspicious sender cannot serve as independent verification.

8.4 Official fraud figures measure different outcomes

The Ministry of Home Affairs reports more than Rs 11,158 crore saved across more than 3.28 million complaints through 30 June 2026. That measure is cumulative from the financial-fraud system's 2021 launch, not a 2026-only loss or recovery total [S18].

The same reply reports a separate financial-year population covering 2023/24–2025/26. It distinguishes complaints, registered cases, reported money, amounts under lien and refunds [S18]. Those units should remain separate in a leadership dashboard.

Measure	What it can show	What it cannot establish
Complaint	A report entered a defined system	A proven offence or unique victim
Registered case	A formal investigation record	A conviction or one transaction
Reported amount	The value reported under the stated definition	A final adjudicated loss
Amount under lien	Funds subject to a protective restriction	Money already returned to the person
Refunded amount	A reported return of funds	Every loss recovered or no remaining harm
Funds described as saved	The system's stated intervention measure	A sum to add to lien and refunded amounts

Prompt reporting can support intervention. It does not guarantee recovery. Customer operations should provide the trusted national reporting route described by the authority and connect the report to the organisation's own fraud process [S18].

8.5 Enforcement is case-specific evidence

The Enforcement Directorate's March release concerns an ongoing investigation of investment, job, QR-related and phishing fraud. It alleges approximately Rs 641 crore moved through accounts and entities in that case [S63]. The investigation spans earlier activity.

That amount is not India's 2026 fraud loss, a profit estimate for the underground corpus or evidence of convictions. The report omits personal names. Investigative allegations remain the authority's allegations.

For a business, the useful response is to preserve the customer's contact chronology, payment instructions and relevant transaction evidence. Fraud and security teams should share a case reference and exchange their findings. Separate queues should not prevent one team learning that the other's suspicion was disproved.

8.6 Payment-card observations retain a narrow scope

SCOPE OF THE CARD FIGURES

Payment-card figures describe only the retained post population. They do not measure national card exposure, active cards, card theft or fraud loss.

The retained posts contain four distinct India-labelled payment-card records in the India-labelled forum posts, including expressly dated 2023 recirculation. Their appearance in the reporting window does not establish fresh 2026 theft, current issuance or usability [S6].

This edition does not establish a national issuer census or an estimate of payment-card fraud. A card-related assertion does not identify the system from which information originated. It cannot establish an incident at a bank, merchant or processor without supporting evidence.

An issuer should use its authorised exposure and fraud process to determine current validity and proportionate protection. Relevant questions include previous replacement, account status and transaction evidence. A public status label alone should not determine a blanket reissue decision.

8.7 Customer support is part of containment

Give concerned users a trusted way to verify contact and report suspected misuse. Explain the genuine payment process and the information the organisation will request. Avoid collecting additional sensitive documents through a route supplied in a suspicious message.

The incident team should brief staff on what is confirmed, what remains uncertain and what action a customer can take now. A warning should not promise that a criminal no longer holds information or that payment causes deletion.

Track whether reports reached the appropriate owner, whether a transaction was reviewed and whether the customer received a clear disposition. These measures show operational response. The volume of warnings distributed does not demonstrate an equivalent number of prevented losses.

KEY TAKEAWAYS

01

Accurate personal or business information does not authenticate a payment instruction.

02

Keep complaints, protected funds, refunds and alleged proceeds in separate units.

03

Connect account, endpoint, transaction and customer-support decisions through one accountable escalation route.

CHAPTER 09

Banking and financial-services deep dive

09

THIS CHAPTER ANSWERS

Which banking decisions require identity, transaction and supplier evidence together?

30

selected banking domains, not a banking-system census

9.1 The selected portfolio has a limited denominator 75
9.2 A bank disclosure is stronger than an advertisement, within its scope 76
9.3 Customer-side and institution-side evidence differ 76
9.4 Provider access extends the decision boundary 77
9.5 Regulatory scope follows the entity and activity 77
9.6 Four workflows to exercise 77
9.7 Board reporting should measure completed decisions 78

CHAPTER 09

Banking and financial-services deep dive

IN SHORT

Banking evidence must distinguish customer information, employee access, payment authority and provider incidents. The selected portfolio contains 30 banking domains, while a public bank disclosure retains unresolved source and scope questions. Official campaign notices add payment-workflow risks without confirming an intrusion at every institution. Validate the account and business instruction, establish the affected service, and give identity, fraud, privacy and supplier owners a shared decision record.

9.1 The selected portfolio has a limited denominator

The selected portfolio contains 30 banking domains within the wider 250-domain portfolio. It is a purposive service sample. It is not a list of all licensed banks, a ranking by size or a representative estimate of banking-system security.

RBI's official bank directory supplies current website context, including `.bank.in` addresses [S24]. The domain relevant to a historical record can differ from a current primary website. No current-domain result should be described as every past and present service of that bank.

The banking cohort has 2 of 30 selected estates with a credential listed for sale when checked. It has 9,174 recorded device associations, including 17 employee-associated records, and 259 credential records. The device and credential figures are cumulative and can overlap; they are not 2026-only counts or verified current intrusions. [S30]

Banking measure	Result	Boundary
Current credential-offer estates	2 of 30	Account ownership and validity require validation
Device associations	9,174	Not unique people or proven current infections
Employee-associated device records	17	Source association does not establish employment
Credential records	259	Not unique accounts or working passwords

The banking view covers all 30 selected estates. Device associations occur at 28, and employee-associated records occur at 6. There are 9,157 other device associations; their owners are not established. These results retain the current-domain boundary. [S30]

One of the four distinct card samples in §8.6 has an issuer label matching this banking cohort. The other three have no named issuer. The label does not establish current issuance, usability or an intrusion into bank infrastructure. [S6]

The table has no banking rating. Public disclosures, the narrow forum-card population and extortion listings retain their own units and are not added to these association counts.

The following propositions require different supporting evidence.

Proposition	Appropriate evidence	Decision boundary
Customer information appears in an advertised collection	Validated record categories and a scoped disclosure	Does not by itself identify the source system
A current employee identity is misused	Owned identity, session and endpoint records	Service-domain association alone does not establish employment
A payment instruction lacks authority	Independent business records and transaction review	Successful authentication is not sufficient business approval
A provider reports an incident	Affected service, tenant and data scope	Does not establish an intrusion at every customer
Card information appears in retained material	Authorised issuer validation	Does not identify an issuer-infrastructure incident

9.2 A bank disclosure is stronger than an advertisement, within its scope

Case M preserves State Bank of India's preliminary record finding and unresolved source and scope [S53]. The customer-record finding and the stated operational exclusions answer different questions. Neither identifies how every record originated or excludes later customer misuse.

For a bank handling comparable evidence, assign several questions to different owners. Privacy assesses the identified categories and notification implications. Customer protection investigates credible follow-up contact. Technical responders establish whether any current identity, session or system access is implicated.

Do not start with a universal password-reset or reissue instruction. First establish which secret, account or service the evidence concerns. A proportional response can differ for a historical customer record, a usable employee session and an unauthorised transaction.

9.3 Customer-side and institution-side evidence differ

An external record associated with a banking service can concern a customer device, an employee identity, a contractor or another relationship. It does not establish ownership of the device or access to the bank's internal infrastructure.

For an employee identity, review active status, privilege, recent sign-ins, session grants and recovery methods. For a customer, connect account-protection and fraud evidence through established support processes. For an unknown relationship, document the uncertainty before choosing containment.

Use consistent dispositions: confirmed and contained, previously remediated, historical, unrelated, unresolved or escalated. Retain the date and supporting evidence. A count of open alerts without dispositions does not demonstrate whether exposure remains actionable.

The same distinction applies to a technically valid transaction request. CERT-In's payment notice describes misuse of valid credentials from trusted infrastructure [S43]. The receiving service still needs confidence that the underlying business instruction has genuine authority.

The narrow payment-card population in §8.6 includes older recirculated material [S6]. It does not establish current issuer exposure or the source of the information. Keep that population separate from institution-access evidence and customer transaction findings.

9.4 Provider access extends the decision boundary

A banking-software supplier's October filing describes misuse of an employee mailbox at a Canadian subsidiary to send false payment instructions. It reports no company-account outflow or product-platform impact at the time [S59]. This is cross-border supplier context, not a confirmed intrusion into a bank in India.

The useful lesson concerns authority over a customer's payment decision. Can the recipient independently verify a changed instruction? Can the supplier identify the affected account, preserve the message chronology and communicate the actual service scope?

Avoid inferring platform access from the supplier's product category. An email-account incident and an application-platform incident require different evidence. Equally, an operational exclusion in the first filing remains time-bounded and should be revisited if a later source expands the scope.

9.5 Regulatory scope follows the entity and activity

RBI's July digital-payment directions apply to commercial banks under their stated definition. Small finance banks, payments banks and local area banks have separate category directions [S13]. A selected sample containing several institution types cannot use one undifferentiated compliance row.

The payment-authentication directions have a general compliance date of 1 April 2026, with specific provisions and exemptions. They generally require two distinct factors for domestic transactions; applicable non-recurring cross-border card provisions have their own timing [S14].

These requirements do not guarantee that an authorised-looking instruction is genuine. The operational test remains whether identity, device, payment and business records support the transaction. Do not describe the framework as a universal ban on SMS authentication.

For a SEBI-regulated activity, reporting and system scope require a separate assessment. The August reporting alignment describes initial, intermediate and final information stages [S21]. Shared technology does not automatically give every legal entity the same regulatory route.

9.6 Four workflows to exercise

Account recovery. Use synthetic customer and staff identities. Test whether accurate personal facts can authorise a high-impact change. A passed exercise rejects an unauthorised request while preserving a usable recovery route for the legitimate person.

Payment changes. Start with a plausible supplier or executive message. Require an independently known contact route and review any exception. Record whether the receiving operator could override the control and who approved that decision.

Provider incident notice. Begin with an incomplete alert: an account was accessed, data scope is uncertain and the affected tenant is still being identified. Test whether legal, fraud and security can preserve their different questions without losing the reporting chronology.

Session containment. After a corroborated identity incident, demonstrate review of sessions, recovery routes, delegated permissions and relevant endpoints. Closing only the password-reset ticket does not establish that the associated access has ended.

9.7 Board reporting should measure completed decisions

Ask how many credible signals lack an owner, which high-impact instructions required exceptions and whether a critical provider supplied usable incident scope. Track the completion of recovery and customer-verification exercises.

Keep customer fraud, employee identity and institution-access outcomes separately labelled. A decline in externally visible material cannot establish that every internal incident is contained. A successful restore cannot establish that affected people no longer face impersonation.

The board should receive owned exceptions as well as completed actions. Identify the affected service, the unresolved question, the interim protection and the date for review. That record supports a decision without pretending that incomplete evidence provides a precise national banking score.

KEY TAKEAWAYS

01

Preserve the selected-domain and historical-domain limits before interpreting banking evidence.

02

Customer records, employee access, payment authority and provider incidents require different validation.

03

Demonstrate recovery, independent payment verification and complete session containment through accountable owners.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which duties apply now, and which remain future implementation phases?

6 / 24 hours

separate early reporting stages in the applicable cyber and securities frameworks

10.1 Current instruments and their scope 80
10.2 CERT-In's six-hour requirement needs a practical clock 81
10.3 Personal-data duties are phased 81
10.4 Financial reporting follows the regulated entity 82
10.5 Shared systems do not erase scope distinctions 82
10.6 Sanctions and exclusions require the actual provision 83
10.7 A joint reporting exercise 83

CHAPTER 10

Regulatory and national response

IN SHORT

Current CERT-In and sector duties must remain separate from future personal-data breach requirements. Entity type, activity, awareness and detection can change the applicable route. MeitY's November Consent Manager phase did not activate every obligation in the personal-data framework. Record the governing instrument and trigger for each duty, preserve the event chronology, and rehearse an initial report while some facts remain uncertain.

This chapter is a planning aid, not legal advice. The table records selected duties from the official texts read. It does not determine the legal scope of every organisation in the research universe.

10.1 Current instruments and their scope

Instrument	Applicable scope	Operational requirement	Decision owner
CERT-In directions under section 70B	Listed entities and incident categories	Report applicable incidents within six hours of noticing or being informed; maintain the required contact and records [S10]	Incident lead and legal
RBI commercial-bank digital-payment directions, 2026	Commercial banks within the stated definition; category exclusions apply	Board-approved governance, security review, product assessment and provider oversight [S13]	Bank security and management
RBI payment-authentication directions, 2025	Payment-system providers and participants, subject to specific provisions and exemptions	General compliance by 1 April 2026; distinct-factor and applicable dynamic-authentication requirements [S14]	Payment operations and compliance
RBI NBFC cybersecurity directions, 2026	Tiered and chapter-specific NBFC applicability	Relevant incident reporting within six hours of detection; recipient exceptions include housing finance companies [S51]	Regulated-entity incident function
RBI non-bank payment-system directions, 2026	Authorised non-bank payment-system operators, with phased applicability	Current requirements for large and medium operators; small-operator phase begins 1 April 2028 [S15]	Payment operator and management

Instrument	Applicable scope	Operational requirement	Decision owner
SEBI Cybersecurity and Cyber Resilience Framework (CSCRF) reporting alignment, August 2026	Applicable regulated entities under the framework	Email reporting within six hours and portal reporting within 24 hours; progressive reporting stages [S21]	Securities incident function
DPDP Act and Rules commencement	Provisions commence in separate phases	Distinguish current machinery and registration from later core duties [S11][S12][S49]	Privacy and legal

The RBI commercial-bank definition excludes small finance banks, payments banks and local area banks. Their separate category directions need their own review [S13]. An organisation's marketing description is not a sufficient scope determination.

SEBI's 2025 implementation extension also had stated exclusions. It did not extend the same date to every regulated category [S16]. Research analysts' 2026 master circular points to the framework and successive clarifications rather than creating one standalone duty for every company [S52].

10.2 CERT-In's six-hour requirement needs a practical clock

The directions identify reportable incident categories in an annexure and specify the relevant entity groups. The trigger is noticing an applicable incident or being informed of it [S10]. A criminal advertisement, by itself, does not establish every element of that trigger.

The operational problem is to make the determination quickly. Record the first alert, validation performed, information received and decision owner. Do not use a later press-release date as the organisation's awareness time.

The directions also require a designated point of contact and ICT logs retained securely for a rolling 180 days within Indian jurisdiction. Time synchronisation has stated traceability and geographical qualifications [S10]. Infrastructure owners should validate the actual service coverage and applicable text.

An incident exercise should establish who can approve an initial submission outside ordinary office hours. The team should know where the necessary service description and contact details are held. The exercise should not assume a complete forensic report can be produced immediately.

10.3 Personal-data duties are phased

The commencement notification separates immediate provisions, a one-year phase and an eighteen-month phase. Most substantive provisions in sections 3–17 belong to the eighteen-month phase. Section 6(9) and the related section 27(1)(d) instead belong to the one-year phase [S11]. The Rules have a corresponding staged schedule [S12].

MeitY's 14 November update says Consent Manager registration took effect on 13 November 2026. It identifies 13 May 2027 for other key duties, rights and inquiry or penalty procedures [S49]. The November event is therefore a phase change, not full commencement of all breach duties.

Future Rule 7 describes notice to affected individuals and an initial Board intimation without delay. Further details follow within 72 hours of becoming aware of the breach, or a longer period allowed on written request [S12]. That future process must not replace current CERT-In or sector reporting.

Future safeguards also concern access control, monitoring, resilience and processor contracts [S12]. Organisations can prepare the underlying capabilities now without misrepresenting their legal commencement. Record current requirements and future implementation milestones separately.

The distinction changes the exercise design. One scenario should test a current reportable cyber incident. Another should test readiness for the later personal-data process. The same chronology may support both, but their triggers, recipients and status remain different.

10.4 Financial reporting follows the regulated entity

The NBFC directions specify relevant six-hour reporting after detection and identify an exception for housing finance companies continuing to report to NHB [S51]. Chapter-specific applicability matters. This is not a universal six-hour rule for every business in India.

The November non-bank payment-system directions distinguish operator sizes and implementation dates. Duties in the wider unregulated linked ecosystem are subject to mutual agreement [S15]. Do not assume a provider's regulated status automatically makes every customer subject to the same direction.

For securities entities, the August reporting alignment uses the Financial Stability Board's Format for Incident Reporting Exchange. It allows an initial submission, intermediate updates and final closure [S21]. That structure recognises that important facts may remain unknown at the first report.

The progressive stages do not establish that a SEBI report automatically satisfies a separate CERT-In duty. Legal and compliance should record each applicable route, submission owner and timing. Preserve the difference between an initial alert and a final closure determination.

10.5 Shared systems do not erase scope distinctions

SEBI's technical clarifications address entities subject to more than one regulator. They describe exclusivity and equivalence principles for applicable systems, shared components and equivalent controls [S22]. Scope therefore requires an assessment of the actual service and audit coverage.

A group company may share identity or hosting with a regulated business. That relationship does not make every system identical for reporting purposes. Map the legal entity, activity, service and provider before deciding which framework applies.

For a provider incident, ask for a dated account of the affected service, access, data categories and containment. Distinguish facts from estimates. A controller or regulated customer should preserve its own determination rather than merely copy a provider's generic statement.

NCIIPC's critical-information-infrastructure role is a further institutional context [S23]. The selected sector cells in this report do not confer legal designation. Operational owners and legal counsel should identify applicable obligations through the competent channels.

10.6 Sanctions and exclusions require the actual provision

This report does not apply a universal fine figure to an advertisement, listing or public disclosure. Liability depends on the provision, commencement, entity and facts. A source claim about information possession does not establish an offence by the alleged victim.

The DPDP commencement phases are particularly important when discussing penalties. A notification about registration or institutional machinery does not itself demonstrate that every later substantive and penalty procedure is already operative [S11][S49].

Keep statutory duties, supervisory directions and contractual commitments in separate rows. A provider contract can require rapid notice while the legal assessment follows another trigger. A public status statement is a further communication with a different purpose and approval owner.

Where facts remain uncertain, record why a particular duty applies or does not apply, what information is missing and when the decision will be revisited. An undocumented assumption that another party already reported is insufficient closure evidence.

10.7 A joint reporting exercise

Use a realistic provider alert: a valid identity was misused, the affected data population is incomplete and a business service remains operational. Ask the team to distinguish account access, data access, transaction integrity and service continuity.

Exercise prompt	Required decision	Completion evidence
External claim arrives	Does owned evidence establish a relevant incident?	Dated validation and escalation decision
Applicable incident is noticed	Which current technical reporting duty starts?	Trigger time, recipient and approved owner
A regulated payment service is involved	Which entity and activity determine the sector route?	Scope determination and reporting calendar
Initial facts are incomplete	What can be submitted and updated now?	Bounded initial report and missing-information list
Personal information is implicated	Which current and future processes must remain distinct?	Privacy assessment and implementation register
Provider gives new evidence	Which earlier statements need correction?	Versioned update and reassessed decisions

Run the exercise with security, legal, privacy, finance, communications and the provider. A passed exercise produces timely decisions with acknowledged uncertainty. It does not pretend that every factual question is resolved at the first meeting.

KEY TAKEAWAYS

01

Preserve the trigger, recipient and scope of each current reporting duty.

02

The November personal-data phase does not replace current cyber or financial-sector reporting.

03

Test staged reporting, shared-system scope and provider evidence with the actual accountable functions.

CHAPTER 11

Outlook and conditional planning

11

THIS CHAPTER ANSWERS

Which preparations follow from the evidence, and what would change the assessment?

6

bounded judgements with an evidence-based revision signal

11.1 Key judgements 86
11.2 Evidence that changes priority 87
11.3 Conditional scenarios 87
11.4 What the evidence cannot project 88
11.5 Leadership review 88

CHAPTER 11

Outlook and conditional planning

IN SHORT

The strongest planning priorities concern identity, payment authority, supplier assurance and independent recovery. Official notices and source claims support different conclusions, while incomplete measurements cannot establish national prevalence. The scenarios below are planning assumptions, not forecasts of attack dates or losses. Give each a signal, accountable owner and closure test, and revise the response when new evidence resolves a material uncertainty.

11.1 Key judgements

Confidence attaches to the proposition in each row. It does not certify every assertion by a source or describe an actor's overall capability.

Judgement	Confidence	Basis and limit	Revision signal
Ransomware readiness remains a cross-sector priority	High for the planning need	Listing visibility and an official warning; no national attack probability [S3][S65]	A validated affected service or failed recovery exercise
Identity containment should include sessions and authority	High as a defensive implication	Messaging-session and payment-credential warnings; not a universal entry route [S47][S43]	Corroborated active session, privilege or payment misuse
Payment security requires business-record integrity	High for the control need	November workflow warning; no public victim total [S40]	A verified beneficiary, record or approval change
Supplier assurance extends beyond a restored provider	High as a planning implication	Update-distribution and certificate-assurance cases; customer scope differs [S56] [S54]	Affected local installation, chain or tenant identified
Public record claims will require provenance checks	Medium	Bank disclosure and retained offers; no sale-frequency forecast [S53]	Matching owned records or a revised official disclosure
Reporting readiness must preserve implementation phases	High for the cited timetable	Current cyber duties and later personal-data phases [S10][S49]	A new applicable official instrument or entity-scope change

These judgements support preparation, without estimating a particular organisation's likelihood of an incident. They should not be converted into sector ratings or a national security score.

11.2 Evidence that changes priority

A current identity match. A credible advertisement becomes a different response problem when owned records confirm an active account or unauthorised session. Identity operations should then preserve the evidence and activate proportionate containment. A historical, remediated account requires a documented closure.

A business-record discrepancy. A payment warning becomes urgent when reconciliation identifies an unauthorised beneficiary or approval change. Finance should establish which instructions depended on the altered record. Technical authentication alone cannot close the business-authority question.

A supplier-specific scope. An incident notice becomes actionable when a provider identifies the affected tenant, update, certificate chain or data population. Procurement should obtain the supporting account and named technical contact. A generic assurance statement cannot establish the local outcome.

A corrected official account. A later disclosure can expand or narrow the affected service and population. Preserve the earlier statement and the reason for revision. Do not silently retain a superseded headline or treat a continuing investigation as proof of no impact.

A verified service effect. An actor's availability claim becomes materially different when the service owner confirms that an essential task fails. Correlate user impact, provider information and access evidence. The outage still does not establish data theft or an actor identity.

A new legal phase. An official commencement or amended sector instrument changes the duty register when it actually applies. Legal should record the source, entity scope, trigger and operational owner. A news headline about the framework does not replace that assessment.

11.3 Conditional scenarios

The following are planning assumptions. They are not measured response intervals, claims that the scenario will occur, or findings that the recommended controls are already implemented.

If this occurs	Planning response	Completion evidence
An active privileged identity is corroborated in an access claim	Activate identity and endpoint response	Sessions, privilege and related endpoint disposition
A payment instruction conflicts with independent business records	Pause the affected decision through approved procedures	Reconciliation, authorised approval and transaction review
A provider reports possible customer-record access	Convene privacy, supplier and incident owners	Service scope, affected categories and reporting decision
An update or certificate dependency is confirmed locally affected	Follow applicable trusted guidance and assess the local installation	Version or chain evidence, tested remediation and investigation decision
A DDoS claim coincides with service degradation	Activate mitigation and business fallback owners	Essential user task works or a bounded incident status is issued
A credible customer report describes impersonation using real facts	Use independent verification and assess transaction exposure	Customer-protection decision and linked fraud record

The organisation should decide who may authorise a temporary restriction and who can reopen the service. Those decisions should follow the actual business and safety context. A generic instruction to disconnect every system can create a separate operational problem.

11.4 What the evidence cannot project

Post volume does not supply an attack probability. A larger advertised dataset does not establish more newly affected people. Ransomware listings do not establish a national encryption or loss total. Unequal source visibility prevents a country security ranking.

Public cases also reflect disclosure practices. A sector with detailed filings can be more visible than a sector with limited public reporting. That difference does not establish its underlying incident rate or control quality.

The selected organisation universe cannot support a nationally representative exposure estimate. Related services can share ownership and dependencies. A current-domain measurement also cannot represent every historical domain associated with an institution.

Use successive evidence only after establishing comparable scope and dates. A new snapshot may change triage priorities, but movement in a summary figure does not demonstrate that a particular account was contained. Completion requires the relevant owner's evidence.

11.5 Leadership review

Review the assumptions when a material source, service or legal scope changes. Ask which proposition became stronger, which alternative was excluded and which decision must now change. Preserve the dated basis for that revision.

The useful leadership output is a short list of owned decisions: contain an identity, correct payment authority, scope a provider event, restore a service or update reporting readiness. Keeping an unresolved question explicit is preferable to supplying unsupported certainty.

KEY TAKEAWAYS

01

Prepare for the mechanisms and consequences supported by the evidence.

02

Attach a revision signal and accountable owner to each planning judgement.

03

Change the response when current evidence changes the proposition, without turning visibility into predicted national loss.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

What should accountable teams demonstrate over the next 90 days?

20

conditional actions with reviewable completion evidence

12.1 Thirty, sixty and ninety days 91

12.2 What each role owns 93

12.3 A reviewable leadership scorecard 94

12.4 How Brandefense can help 95

CHAPTER 12

Action plan

IN SHORT

Begin with alert ownership, payment authority, current reporting duties and service dependencies. Then test provider notice, account recovery and customer verification. Close the programme with independent restoration and a joint incident exercise. These are planning targets, not legal deadlines. A corroborated material incident enters response immediately, without waiting for its place in the calendar. Give every action an accountable owner and a specific completion artefact.

12.1 Thirty, sixty and ninety days

The actions are conditional on the organisation's services and regulatory scope. Use synthetic information and approved procedures for exercises. Preserve actual findings and exceptions, including a failed test that requires further work.

1Days 1–30		
Establish one route for credible identity, provider and public-claim alerts	OWNER CISO and SOC	COMPLETION EVIDENCE Successful routing test with a named backup owner
Validate account ownership, freshness, active status and earlier remediation	OWNER Identity and incident response	COMPLETION EVIDENCE Dated disposition for relevant alerts
Reconcile authority for high-impact payment-record and beneficiary changes	OWNER Finance and data owners	COMPLETION EVIDENCE Independent record and approved exception trail [S40]
Map critical services to identity, data, payment and communication dependencies	OWNER Business service owners	COMPLETION EVIDENCE Service map, provider contact and minimum fallback
Record applicable current cyber and sector reporting triggers	OWNER Legal and compliance	COMPLETION EVIDENCE Entity-specific duty register and awareness chronology [S10] [S21]

Approve separate wording for claims, disruption, data access and unresolved scope

OWNER

Communications and incident lead

COMPLETION EVIDENCE

Bounded templates with next-update responsibility

2Days 31–60

Test provider notice with incomplete tenant and data information

OWNER

Procurement, privacy and SOC

COMPLETION EVIDENCE

Timed evidence exchange and owned information gaps

Test executive and supplier payment instructions through independent verification

OWNER

Treasury and finance

COMPLETION EVIDENCE

Synthetic unauthorised instruction rejected and recorded [S47]

Exercise customer and staff recovery against realistic personal facts

OWNER

Identity and customer operations

COMPLETION EVIDENCE

Safe legitimate recovery and rejection of impersonation

Review linked sessions, delegated permissions and recovery methods after a validated incident

OWNER

Identity and application owners

COMPLETION EVIDENCE

Session and privilege closure record

Reconcile production, test and provider payment authority

OWNER

Application security and payment operations

COMPLETION EVIDENCE

Access inventory and tested business-authority checks [S43] [S41]

Establish local relevance of critical update and certificate dependencies

OWNER

Endpoint and certificate owners

COMPLETION EVIDENCE

Version or trust-chain inventory and scoped action [S56] [S54]

Test legitimate public-service and payment verification guidance

OWNER

Fraud and customer support

COMPLETION EVIDENCE

Staff exercise and findable trusted contact route [S44]

Validate mail authentication and certificate changes against service dependencies

OWNER
Messaging and infrastructure

COMPLETION EVIDENCE
Tested change, rollback plan and approved exceptions

Rehearse availability degradation at a complete user journey

OWNER
Operations and service owners

COMPLETION EVIDENCE
Essential task and fallback work during an authorised test

Update future personal-data implementation milestones separately from current duties

OWNER
Privacy and legal

COMPLETION EVIDENCE
Phase-specific readiness plan with source dates [S11][S12] [S49]

3Days 61–90

Restore a critical service using protected recovery access

OWNER
Infrastructure and business continuity

COMPLETION EVIDENCE
Isolated restore, integrity check and business acceptance

Exercise payment abuse, provider notice and reporting together

OWNER
Incident lead, finance, legal and provider

COMPLETION EVIDENCE
Timely decisions, staged report and reconciliation result

Review access and retention for sensitive customer and workforce records

OWNER
Data owners and privacy

COMPLETION EVIDENCE
Documented retention decisions and permission review

Present completed tests and unresolved exceptions to management

OWNER
CISO and management

COMPLETION EVIDENCE
Decisions with accountable owners and review dates

12.2 What each role owns

Management and the board. Ask which essential business task can continue during identity or provider failure. Require evidence from a real exercise and an owner for each unresolved exception. A threat-volume chart does not demonstrate that a payment decision or recovery procedure is safe.

CISO and incident lead. Keep the proposition and evidence type explicit. A source claim, a confirmed access event and a verified service consequence can coexist without proving the same thing. Coordinate identity, fraud, privacy and service owners around one chronology.

Security operations. Preserve the alert time, account or service relationship, validation performed and disposition. Check known remediation before escalating historical material again. Relevant new evidence should change the response, while a duplicate advertisement should not create an artificial incident total.

Identity and application teams. Test account status, privilege, sessions, delegated permissions and recovery paths. For payment-integrated applications, verify business authority as well as authentication. A valid service credential should not alone authorise an otherwise unsupported beneficiary or approval change.

Finance, treasury and fraud. Own the independent verification of high-impact instructions and the reconciliation of authoritative records. Preserve the payment decision and the reason for any exception. Share transaction findings with the technical responders without assuming every suspicious contact originated in an institution's systems.

Infrastructure and certificate owners. Establish whether a supplier advisory concerns the actual local version or trust chain. Follow the applicable guidance and verify the resulting service. Keep remediation separate from the investigation of earlier unauthorised access or data exposure.

Customer operations. Give people a trusted route to verify contact and report suspicious instructions. Use clear scripts based on confirmed categories. A user who quotes accurate information can still be an unauthorised requester; staff should know what independently establishes authority.

Legal, privacy and procurement. Determine applicable current duties and future phases for the actual entity and service. Preserve awareness and detection times, provider statements and staged updates. An agreement that requires notice is useful only if the contact and evidence exchange work in practice.

12.3 A reviewable leadership scorecard

The following are recommended completion measures. They are not measured control performance in Indian organisations.

Measure	Evidence leadership should request	Exception to record
Alert ownership	A credible signal reaches its owner and receives a dated disposition	Missing owner or incomplete validation
Payment authority	A high-impact change is checked against independent records	Override or unresolved record discrepancy
Provider readiness	A critical supplier supplies usable incident scope in an exercise	Tenant, contact or data-map gap
Identity containment	Relevant sessions and privileges are reviewed after a validated incident	Persistent or unexplained access
Reporting readiness	Current obligations and future phases remain distinct in the exercise	Unresolved entity scope or trigger

Measure	Evidence leadership should request	Exception to record
Service recovery	An essential task works after an isolated restore	Dependency or integrity failure
Customer protection	Staff verify a realistic request through a trusted route	Unsupported assurance or unsafe information request

An exception should identify the affected service, interim protection, accountable owner and review date. Do not convert a failed exercise into a passed control because a remediation ticket exists. Leadership can accept a bounded risk, but should see the evidence and the remaining uncertainty.

The review should also identify which earlier assumption changed. A newly verified identity match, corrected provider scope or enacted legal change can alter priorities. Record that basis rather than using the latest public headline as the reason for a broad programme change.

12.4 How Brandefense can help

Bring representative owned domains, critical services and actual response questions to a Brandefense discussion. Use this report's cases to test how an external signal reaches the appropriate identity, fraud, service or privacy owner.

Ask which evidence supports the finding, which dates and populations it covers, and what permits closure. A demonstration should help the organisation assess a workflow; it does not establish that the organisation has already been assessed in this report.

Request a Brandefense demo

KEY TAKEAWAYS

01

Establish alert ownership, payment authority and current reporting scope by day 30.

02

Test provider, identity, customer and service decisions by day 60.

03

Demonstrate restoration and present owned exceptions to management by day 90.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

How can readers trace a finding without confusing claims, observations and outcomes?

4

appendices covering scope, evidence, sources and terms

Appendix A. Sources, scope and confidence 97

Appendix B. Public evidence-card register 101

Appendix C. Sources 103

Appendix D. Glossary 107

Appendix A. Sources, scope and confidence

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

A.1 Window and timestamp meaning

The primary window is 1 January–22 November 2026 by the date of a post or publication. Recent activity means 8–22 November. The cut-off includes material available when checked on 22 November, rather than every publication that may appear later that day.

A post date establishes circulation, not an intrusion date. A company's detection, investigation and disclosure dates can differ. Where the source supplies several dates, the case preserves their roles. A later assessment of one event is linked to that event rather than added as a new incident.

Population	Time meaning	Main limit
Country-related posts	Post time within the primary window [S1][S2]	Source association does not establish targeting or an incident
Recent retained material	Post time during 8–22 November [S9]	The final day remains a snapshot of available material
Extortion listings	Publication date within the primary window [S3]	Listing claims are not confirmed outcomes
Selected estates	Dated portfolio and control observations [S4][S5]	A primary domain does not describe every service or historical domain
Official statistics	The period stated by the issuing authority	Publication in 2026 does not convert a 2025 statistic into 2026 data
Public incident disclosures	Event, awareness and publication dates as stated	An initial statement can be superseded by a later assessment

A.2 Brandefense Blackhole post evidence

The report uses retained dark-web and messaging material supplied through Brandefense Blackhole. Posts, advertisements, source accounts and alleged incidents are distinct units. One post can contain a global menu, several target assertions or a request with no possession claim.

The detailed forum dossiers describe held advertisements and their evidence boundaries. The broader source contains different languages and platforms. Results from one retained subset are not extrapolated to the whole Indian underground or to national incident prevalence.

Public post cards use stable B identifiers and English paraphrases. They omit victim identifiers, sensitive sample material and contact details. Paraphrases are explicitly labelled. They are not represented as the actor's exact wording or as confirmation that advertised records are authentic.

The six Chapter 4 dossiers and Case Q in §5.11 are selected for distinct decision value. They cover payment archives, mobility services, supplier access, finance-related documents, education backups, medical-payment payees and diagnostic-services access. They are not a random sample or seven confirmed breaches. [S2]

A.3 Selected organisation universe

The 250-estate portfolio is purposive. It covers national and regional public bodies, financial organisations and major service, industrial, research and healthcare organisations. It is not an official top-250 ranking or a representative national survey. [S5]

An estate may belong to a wider group, share a supplier or operate alongside legacy domains. The report does not assume statistical independence between rows. In particular, a current primary bank domain does not represent every historical domain associated with that bank. [S24]

No unavailable exposure count is replaced with zero. The validated exposure signals cover the 250 selected estates on 22 November 2026. Device and credential records are cumulative, regardless of capture date. Only the national Atlas headline is published. [S30]

A.4 Control results

Email, DNS, certificate and web-control observations describe visible configuration, with their assessed populations stated beside the results. They do not demonstrate complete security, malicious intent or an intrusion. Unavailable evidence remains distinct from an observed missing control. [S4]

DMARC policy is not a measure of phishing success. An observed DKIM record supports a narrower proposition than signing every message. A DNSSEC delegation record does not establish every validation path. A valid certificate does not establish application integrity or safe authorisation.

A.5 Payment-card scope

The card figure describes payment-card records in the retained post corpus. It does not measure national card exposure, card theft or fraud loss. Four distinct India-labelled samples were observed in the India-labelled forum posts, including historical recirculation. Their appearance does not establish valid current issuance, usability or fresh 2026 theft. [S6]

The figure is not added to credential records, customers in public disclosures or financial-fraud complaints. No bank's intrusion status can be inferred from a card label alone. Issuer response requires its own authorised validation and fraud evidence.

A.6 Ransomware and regional comparison

Ransompedia supplies the 254 India-labelled extortion listing records and the four comparator counts. Publication dates determine the window. A listing is a criminal claim, rather than independent confirmation of encryption, exfiltration, payment or business interruption. [S3]

The 2025 figures cover 1 January–31 December 2025. Historical totals describe available source history when checked on 22 November 2026, rather than complete national incident histories. The chart data records each country's earliest and latest retained record dates. The partial 2026 window and full 2025 calendar year are not equal observation periods. [S3]

The four peers are Pakistan, Bangladesh, Sri Lanka and Nepal. They provide neighbouring South Asian financial, trade and public-service contexts. Their different populations, economic structures and visibility prevent a national security ranking from the observed counts.

Multiple listings can refer to the same organisation, and one label can involve multiple affiliates. The report therefore uses listing records as its published unit. It does not equate the 254 records with 254 unique organisations or assume that the labels prove a common operator.

A.7 Public incidents and campaign coverage

The public register distinguishes company disclosures, authority campaign notices, vendor technical research, attributed press reports, advisory-only context and excluded leads. Those categories do not share a national incident denominator. An advisory is evidence of a warning, rather than a newly confirmed victim.

Official-source review covered CERT-In, financial regulators, government and parliamentary publications, cybercrime authorities and available police reporting. Public archives and original notices were not uniformly available.

The resulting coverage is a bounded source review. It does not establish that every Indian cyber incident or every public report has been found. Unavailable original notices remain unresolved, and a search result alone is not treated as a read primary statement.

Case dossiers can bundle several propositions. A confirmed extortion approach, an unverified data-volume claim and a company's operational statement may coexist in one case. The evidence for one does not automatically validate the others. Updates and related notices are linked rather than summed as separate victims.

A.8 Public naming and source links

A victim organisation is named only where official confirmation and wide reporting support the incident proposition, with an entry in the public naming register. That entry does not approve unrelated claims, all advertised data or alleged incidents at the organisation's customers.

Other organisations use roles broad enough to fit several bodies. Unverified national-service claims receive the same protection as commercial claims. Actor aliases may be used where they have no contact value. Aliases do not establish a real identity or a common operator.

Where an article URL would identify a withheld victim, Appendix C supplies a neutral publisher root and an article-withheld notice. The precise source mapping remains in the private evidence record. A working publisher homepage does not independently substantiate the incident account.

A.9 Confidence, alternatives and forecasts

Confidence attaches to a proposition. A dated post supports confidence that an advertisement was observed, without establishing confidence in its alleged origin. An official statement supports what the issuer reported, while its stated preliminary scope may remain unresolved.

Source attributions remain attributed to their authors. A vendor's campaign grouping does not establish responsibility for a separately observed criminal post. Similar target sectors, dates or tools are insufficient to draw an operator-level connection.

The outlook contains conditional planning scenarios. Each states a signal, an alternative explanation or limit and a decision that could change. The report does not infer attack probabilities, national losses or control effectiveness from advertisement or listing counts.

A.10 Technical references and source checks

Every external source used in the public text has a dated record in Appendix C. The entry distinguishes a substantive statement from an index or an attributed press account. Historical sources retain their original period.

The specific India-focused campaign sources do not identify an exploited CVE. The separate React example was checked against NVD and the vendor's affected and original fixed versions. It is a software-inventory baseline, rather than a newly established India incident. [S7][S25]

The behaviour matrix uses analyst mappings checked against current MITRE definitions. A technique mapping is an aid to investigation. It does not establish that every capability of a malware family was exercised or that a deployable detection has been validated. [S26][S27][S28][S29]

Appendix B. Public evidence-card register

The cards below contain dated, role-based English paraphrases. They describe held claims, requests or circulation, with the limits printed on each card. No private post identifier or source contact is published.

Card	Date	Venue	Alias	Language	Section
B01	2026-01-31	Forum	INS	English paraphrase	4.3 Case A
B02	2026-02-04	Forum	AYYUBI	English paraphrase	4.3
B03	2026-02-17	Forum	Mckay	English paraphrase	4.3
B04	2026-03-04	Forum	Eliphas	English paraphrase	4.3 Case B
B05	2026-03-18	Forum	krisko383	English paraphrase	4.3
B06	2026-03-23	Forum	vexin	English paraphrase	4.3 Case C
B07	2026-04-16	Forum	Antelope	English paraphrase	4.3
B08	2026-08-21	Forum	updap	English paraphrase	4.3 Case D
B09	2026-09-05	Forum	updap	English paraphrase	4.4
B10	2026-10-07	Forum	updap	English paraphrase	4.4
B11	2026-10-12	Forum	Dark_Alpha	English paraphrase	4.4
B12	2026-10-30	Forum	Roxanne	English paraphrase	4.4
B13	2026-11-05	Forum	scarlettgroup	English paraphrase	4.4
B14	2026-11-10	Forum	SensitiveDarkForum	English paraphrase	4.3 and 4.5
B15	2026-11-11	Forum	protowisher	English paraphrase	4.3 and 4.5
B16	2026-11-14	Forum	WSdatabase	English paraphrase	4.3 Case F

Card	Date	Venue	Alias	Language	Section
B17	2026-11-16	Forum	syn4pz	English para-phrase	4.3 Case E
B18	2026-11-20	Forum	Goofe	English para-phrase	4.4 and 4.5
B19	2026-10-22	Forum	Alias omitted	English para-phrase	5.11 Case Q

Appendix C. Sources

Own-source entries have no public dataset download. External entries give the opened source or a neutral publisher root where a victim-identifying article URL is withheld. Verification dates describe the source check, rather than a claim that an investigation has reached its final conclusion.

S1: Brandefense Blackhole country-related post observations, 1 January–22 November 2026. Own-source evidence; no public dataset address. Verified on 22 November 2026.

S2: Brandefense Blackhole retained forum material, 1 January–22 November 2026. Own-source evidence; no public dataset address. Verified on 22 November 2026.

S3: Ransompedia extortion listings, India and four regional comparators, 1 January–22 November 2026. Own-source evidence; no public dataset address. Verified on 22 November 2026.

S4: Brandefense control observations for selected India estates, 22 November 2026. Own-source evidence; no public dataset address. Verified on 22 November 2026.

S5: Brandefense selected 250-estate India organisation portfolio, 22 November 2026. Own-source evidence; no public dataset address. Verified on 22 November 2026.

S6: Brandefense Blackhole India-labelled card samples in the India-labelled forum posts, checked 22 November 2026. Own-source evidence; no public dataset address. Verified on 22 November 2026.

S7: NIST National Vulnerability Database, CVE-2025-55182. Open source. Verified on 22 November 2026.

S9: Brandefense Blackhole recent-material snapshot, 8–22 November 2026. Own-source evidence; no public dataset address. Verified on 22 November 2026.

S10: CERT-In directions under section 70B, 28 April 2022. Open source. Verified on 23 November 2026.

S11: DPDP Act commencement notification, GSR 843(E), 13 November 2025. Open source. Verified on 22 November 2026.

S12: Digital Personal Data Protection Rules 2025, GSR846(E). Open source. Verified on 22 November 2026.

S13: RBI Commercial Banks Digital Payment Security Controls Directions 2026. Official issuer. Verified on 23 November 2026.

S14: RBI Authentication mechanisms for digital payment transactions Directions 2025. Official issuer. Verified on 23 November 2026.

S15: RBI non-bank PSO Cyber Resilience and Digital Payment Security Controls Master Directions 2026. Official issuer. Verified on 23 November 2026.

S16: SEBI CSCRF implementation extension circular 2025/96. Open source. Verified on 22 November 2026.

S17: MHA Assistance to States to Tackle Cyber Incidents, 24 March 2026 written parliamentary reply. Open source. Verified on 22 November 2026.

S18: MHA National Cybercrime Response Mechanism, 22 July 2026 Rajya Sabha reply. Open source. Verified on 23 November 2026.

S19: TRAI Yearly Performance Indicators 2025–26, released 5 October 2026. Open source. Verified on 22 November 2026.

S20: CERT-In annual report index. Open source. Verified on 22 November 2026.

S21: SEBI Alignment of Cyber Incident Reporting Portal with FIRE Format. Open source. Verified on 22 November 2026.

S22: SEBI Technical Clarifications to CSCRF 2025/119. Open source. Verified on 22 November 2026. Abbreviation expansion checked on 23 November 2026.

S23: PIB Curbing Cyber Frauds in Digital India: NCIIPC role paragraph. Open source. Verified on 22 November 2026. Abbreviation expansion checked on 23 November 2026.

S24: RBI Websites of Banks in India. Official issuer. Verified on 23 November 2026.

S25: React original CVE-2025-55182 advisory and updated remediation guidance. Open source. Verified on 22 November 2026.

S26: MITRE ATT&CK current technique definition. Open source. Verified on 22 November 2026.

S27: MITRE ATT&CK current technique definition. Open source. Verified on 22 November 2026.

S28: MITRE ATT&CK current technique definition. Open source. Verified on 22 November 2026.

S29: MITRE ATT&CK current technique definition. Open source. Verified on 22 November 2026.

S30: Brandefense Atlas selected portfolio exposure observations, 22 November 2026. Own-source evidence; no public dataset address. Verified on 22 November 2026.

S40: CERT-In CIAD-2026-0062 business payment workflows. Open source. Verified on 22 November 2026.

S41: CERT-In CIAD-2026-0058 CRAFTY FALCON. Open source. Verified on 22 November 2026.

S42: CERT-In CIAD-2026-0049 AI agent incidents. Open source. Verified on 22 November 2026.

S43: CERT-In payment and disbursement API campaign. Open source. Verified on 22 November 2026.

S44: CERT-In RTO/eChallan Android campaign. Open source. Verified on 22 November 2026.

S45: CERT-In open-source supply-chain notice. Open source. Verified on 22 November 2026.

S46: CERT-In WhatsApp attachment malware. Open source. Verified on 22 November 2026.

S47: I4C Boss Scam warning. Open source. Verified on 23 November 2026. Abbreviation expansion checked on 23 November 2026.

S48: I4C Boss Scam Hindi edition. Open source. Verified on 23 November 2026.

S49: MeitY Consent Manager phase. Open source. Verified on 22 November 2026.

S50: MeitY Consent Manager Hindi edition. Open source. Verified on 22 November 2026.

S51: RBI NBFC Cybersecurity Framework Directions 2026. Official issuer. Verified on 23 November 2026.

S52: SEBI Research Analyst master circular. Open source. Verified on 22 November 2026.

S53: SBI exchange disclosure. Official issuer (21 October 2026 exchange filing). Verified on 23 November 2026.

S54: eMudhra official statement. Open source. Verified on 22 November 2026.

S55: eMudhra KPMG independent-review filing. Open source. Verified on 22 November 2026.

S56: eScan security advisory updated January 27. Open source. Verified on 23 November 2026.

S57: Manufacturing incident disclosure. Open source (article URL withheld). Verified on 22 November 2026.

S58: Automotive supplier incident disclosure. Open source (article URL withheld). Verified on 22 November 2026.

S59: Supplier subsidiary email incident disclosure. Open source (article URL withheld). Verified on 22 November 2026.

S60: Cloud provider extortion disclosure. Open source (article URL withheld). Verified on 22 November 2026.

S61: Acronis Mustang Panda India government/energy research. Open source. Verified on 22 November 2026.

S62: Kaspersky SilverFox India campaign research. Open source. Verified on 22 November 2026.

S63: ED cyberfraud money-laundering investigation. Open source. Verified on 22 November 2026.

S65: CERT-In The Gentlemen ransomware advisory. Open source. Verified on 22 November 2026.

S68: Independent SBI coverage. Open source. Verified on 22 November 2026.

S69: Independent eMudhra coverage. Publisher site. Verified on 23 November 2026.

S70: Acronis Transparent Tribe startup-themed campaign. Open source. Verified on 22 November 2026.

S71: Acronis LOTUSLITE banking-themed campaign. Open source. Verified on 22 November 2026.

S72: Seqrite ShadowRecruit recruitment campaign. Open source. Verified on 22 November 2026.

S73: Seqrite GST refund phishing Remcos campaign. Open source. Verified on 22 November 2026.

S74: CBSE coordinated portal attacks official statement. Open source. Verified on 22 November 2026.

S75: Independent reporting of CBSE portal attacks. Open source. Verified on 22 November 2026.

S76: Unocoin security incident update superseding earlier assessment. Open source. Verified on 22 November 2026.

S77: Independent reporting of Unocoin service suspension. Open source. Verified on 22 November 2026.

S79: Cyber Swachhta Kendra SyncFuture espionage advisory. Open source. Verified on 22 November 2026.

S82: HDFC AMC initial cyber-security disclosure. Open source. Verified on 22 November 2026.

S83: HDFC AMC later assessment and injunction update. Open source. Verified on 22 November 2026.

S84: PTI reporting of HDFC AMC interim court relief. Open source. Verified on 22 November 2026.

S85: CoinDCX October wallet activity official update. Open source. Verified on 22 November 2026.

S86: Independent reporting of CoinDCX revised October loss disclosure. Open source. Verified on 22 November 2026.

S87: Listed building-materials manufacturer website incident filing. Open source (article URL withheld). Verified on 22 November 2026.

S90: Bajaj Auto ransomware response update. Open source (filing URL withheld; exchange update, 26 June 2026). Verified on 23 November 2026.

S91: Independent reporting of Bajaj Auto ransomware disclosure. Open source. Verified on 22 November 2026.

S92: Reuters report quoting an electronics manufacturer incident statement. Open source (article URL withheld). Verified on 22 November 2026.

S93: Rating-agency assessment of a bank employee-account incident. Open source (article URL withheld). Verified on 22 November 2026.

S94: Press account quoting a bank employee-email incident statement. Open source (article URL withheld). Verified on 22 November 2026.

S95: Kaspersky Russian primary eScan supply-chain analysis. Open source. Verified on 22 November 2026.

S96: Kaspersky English primary eScan supply-chain analysis. Open source. Verified on 22 November 2026.

S97: Independent eScan update compromise reporting. Publisher site. Verified on 23 November 2026.

S98: Regional report of healthcare technology incident complaint. Open source (article URL withheld). Verified on 22 November 2026.

S99: Customer engagement provider confirms limited cloud access. Open source (article URL withheld). Verified on 22 November 2026.

S100: Regional report of police computer ransomware recovery. Open source (article URL withheld). Verified on 22 November 2026.

S101: Lok Sabha written answer on government cyber incidents. Open source. Verified on 22 November 2026.

S102: Regional reporting of industrial clearances portal inquiry. Open source (article URL withheld). Verified on 22 November 2026.

S103: Police investigate alleged career test-platform data sale. Open source (article URL withheld). Verified on 22 November 2026.

S105: Kaspersky August 2026 HoneyMyte/CoolClient campaign statement. Open source. Verified on 22 November 2026.

S106: Securelist CoolClient driver and campaign technical research. Open source. Verified on 22 November 2026.

S107: Reported trade-data complaint and police inquiry. Open source (article URL withheld). Verified on 22 November 2026.

S109: SBI says root cause analysis of data breach underway, steps up cybersecurity checks. Open source. Verified on 22 November 2026.

S110: Attributed denial of a public-sector information claim. Open source (article URL withheld). Verified on 23 November 2026.

S112: Lender investigates supplier-platform data scope. Open source (article URL withheld). Verified on 22 November 2026.

S113: Independent account of lender supplier-platform inquiry. Open source (article URL withheld). Verified on 22 November 2026.

S114: Recent bank cyber-loss claim correction. Open source (article URL withheld). Verified on 22 November 2026.

S117: Reuters account of contractor data disclosure and hosting-provider response. Open source (article URL withheld). Verified on 22 November 2026.

S118: Operator clarification of contractor-document scope. Open source (article URL withheld). Verified on 23 November 2026.

S121: IT supplier response to employee-information claims. Open source (article URL withheld). Verified on 22 November 2026.

S126: Courier-company account of a contained parent-group event. Open source (article URL withheld). Verified on 22 November 2026.

S127: Hindi account of courier parent-group incident scope. Open source (article URL withheld). Verified on 22 November 2026.

S128: Customer warning about attempted support-system access. Open source (article URL withheld). Verified on 22 November 2026.

S129: Short report of a customer support-system warning. Open source (article URL withheld). Verified on 22 November 2026.

S130: Supplier response to an unresolved bank-data source claim. Open source (article URL withheld). Verified on 22 November 2026.

S134: Public-service messaging-account misuse reported by press. Open source (article URL withheld). Verified on 22 November 2026.

S135: PTI account of a public-service messaging-account warning. Open source (article URL withheld). Verified on 22 November 2026.

S136: RFC 4033, DNS Security Introduction and Requirements. Open source. Verified on 22 November 2026.

S137: RFC 6797, HTTP Strict Transport Security. Open source. Verified on 22 November 2026.

Appendix D. Glossary

Term	Plain meaning
Actor claim	An assertion by a seller or claimant that has not become an independently established outcome
Advertisement	A post offering data, access or a service; it does not establish a completed transaction
Atlas	Brandefense's exposure rating product; the national headline describes the selected portfolio
Backdoor	Software designed to provide remote access outside the intended administrative process
BFSI	Banking, financial services and insurance
Blackhole	Brandefense's source of retained underground and messaging evidence
CFCFRMS	India's financial-cyberfraud reporting and response system; its reported measures have distinct meanings
Crore	Ten million; amounts in this report retain their stated rupee unit and source period
Credential	Information or a token used to authenticate an account or service
Credential-market listing	An offer of a credential associated with a domain; ownership and validity require validation
CSCRF	Cybersecurity and Cyber Resilience Framework [S22]
Disbursal	Release of money through a payment or lending process
DLL sideloading	A program loads an unintended library, potentially giving that library the program's privileges
DMARC	A domain's policy for handling mail that fails its authentication and alignment checks
DKIM	A mail-signing standard that lets receivers check a message's signature
DNSSEC	DNS Security Extensions: signatures that help verify the origin and integrity of DNS data [S136]
Estate	The selected domain and service boundary used for an organisation-level observation
Extortion listing	A public criminal claim used to pressure an organisation; it is not independent incident confirmation

Term	Plain meaning
FIRE	The Financial Stability Board Format for Incident Reporting Exchange
Hot wallet	A wallet with signing capability available to an operational online service
HSTS	HTTP Strict Transport Security: a policy directing browsers to use secure connections for a site [S137]
I4C	Indian Cyber Crime Coordination Centre [S47]
KYC	Know-your-customer identity checks
NBFC	A non-banking financial company, with duties depending on its regulatory category
NCIIPC	National Critical Information Infrastructure Protection Centre [S23]
NCRP	India's National Cyber Crime Reporting Portal
PSO	Payment system operator; applicable duties depend on the operator's type and category
Ransompedia	Brandefense's source of ransomware and extortion listing records
RMM	Remote monitoring and management software; controller and permission context determine authorised use
SPF	A domain's statement of which systems may send mail for it
Supplier boundary	The systems, accounts and responsibilities belonging to a service provider rather than its customer
TLP:CLEAR	Information designated for unrestricted sharing, subject to other applicable obligations
USDT	A digital token; a reported token amount is not silently converted to realised rupee loss
Workflow integrity	Confidence that records and approvals underlying a business action are authorised and accurate

About this report

Prepared by Odin by Brandefense. This English master follows the Brandefense Country Report series structure and separates own-source observations, actor claims, source-attributed reporting and analytical judgements. This is the English master edition.

The cut-off is 22 November 2026, with recent activity highlighted for 8–22 November. Material published later on the cut-off day can fall outside the available snapshot. The report does not claim a complete census of cybercrime affecting India.

Recommendations specify tasks that an organisation can validate against its own systems, policy and legal status. They do not assert whether a named or anonymised organisation has implemented a control. Readers should apply each finding within its stated source population and evidence boundary.

© 2026 Brandefense. All rights reserved.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO