BRANDEFENSE COUNTRY REPORT · UNITED STATES 2026

Brandefense United States Cyber Threat Landscape Report 2026

Identity, supplier access and the continuity of essential services

Odin by Brandefense
Research window: 1 January–22 November 2026, by post date
Version 1.0 · Public Research Edition · TLP:CLEAR · 8–22 November 2026

172 of 250
estates had a credential listed for sale when checked

4,605
publication-dated extortion claims in the window

29
source-supported incident and disclosure families, with separate date limits

149
labels associated with publication-dated US extortion records

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Digital services and the US threat context	10
03	National exposure: the selected operating-estate portfolio	15
04	Underground evidence: advertisements, listings and the limits of a claim	25
05	Incident disclosures and targeting by sector	41
06	Hacktivism, DDoS and operational disruption	62
07	Threat actors, listing labels and supported relationships	69
08	The fraud economy: identities, accounts and payment decisions	85
09	Banking and financial-service decisions	93
10	Regulatory response and notification decisions	99
11	Outlook and conditions that would change the assessment	104
12	A 30/60/90-day action plan	108
A	Appendix A. Scope, populations and evidence limits	116
B	Appendix B. Evidence and decision register	120
C	Appendix C. Sources	126
D	Appendix D. Terms used in the report	131
	About this report	133

Board and executives	01 05 11 12
CISO and security leads	03 05 06 10 12
SOC and threat intelligence	04 06 07 B
Fraud and customer protection	04 05 08 09
Legal and communications	05 06 10 12

About this edition

English master edition. No translated edition accompanies this report.

Prepared with AI assistance. Observations, actor claims, official disclosures and analyst judgements remain distinct. The window uses post or publication dates; source-verification dates are listed separately.

US disclosures connect identities and suppliers to data loss and operational disruption, while extortion listings create continuing pressure for validated response and tested recovery.

4,605

US-labelled extortion records; claims rather than confirmed intrusions

80/100

National Atlas headline for the selected portfolio

250

selected operating estates across ten sectors

29

source-supported incident and disclosure families, with distinct date limits

Contents and reading routes

The report moves from leadership decisions to the evidence, then to a programme with accountable owners.

Chapter	Question	First reader
1. Executive summary	Which decisions deserve attention now?	Board and CISO
2. Digital context	Which US service dependencies change the response?	Security leadership
3. National exposure	What does the selected estate portfolio establish?	Identity and infrastructure
4. Underground evidence	What is advertised, and what remains unverified?	Threat intelligence
5. Disclosures by sector	What did original notices actually confirm?	Service and privacy owners
6. Disruption	What separates a claim from operational impact?	Operations and communications
7. Actors	Which attributions and relationships have evidence?	SOC and intelligence
8. Fraud economy	How can information loss affect the next transaction?	Fraud and customer teams
9. Banking	Which financial-service decisions need shared ownership?	Financial security leaders
10. Regulation	Which reporting clock and legal scope apply?	Legal and compliance
11. Outlook	What would change the assessment?	Leadership and planning
12. Action plan	Who acts, and what demonstrates completion?	All owners
Appendices A–D	Where are the scope, evidence, sources and definitions?	Reviewers and practitioners

Leadership route: Chapters 1, 5 and 10–12. **Operations route:** Chapters 3–7 and 12. **Customer and fraud route:** Chapters 5 and 8–10.

Observed means the post, source record or control observation is held. **Claimed** means an advertiser or listing asserts something. **Officially disclosed** means the cited organisation or authority published the stated account. **Analyst judgement** identifies an implication whose limits remain explicit.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which decisions follow from the US evidence, and what should leaders validate first?

4

decisions with accountable owners

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

US disclosures show different routes to harm: supplier-held information, misused identities, website scripts and interrupted operations. Ransompedia records 4,605 US-labelled extortion claims, including 357 publications in the closing period. The selected portfolio has a national Atlas headline of 80/100. Credentials were listed for sale for 172 of 250 estates when checked. Twenty-nine source-supported disclosure families add lessons without forming a national attack census. Validate credible access signals, constrain supplier permissions, prepare accurate notices and prove recovery of an essential service.

This report combines Brandefense observations with original disclosures and official campaign notices. Posts, extortion listings, selected estates, patient records and complaints describe different populations. They cannot be added into a national incident total. An observed advertisement does not establish current access, authentic data or a completed transaction [S1][S2][S3][S4].

The research window starts on 1 January and ends at the available 22 November snapshot. Publication, discovery, access, notification and recovery dates are distinguished. Some in-window disclosures concern earlier activity. The recent section covers 8–22 November without claiming complete coverage of every publication during those days.

1. Extortion pressure extends beyond a small group of labels. The listing snapshot contains 149 group labels. The leading five account for 1,602 of 4,605 records, or 34.8%. The remaining 3,003 carry other labels. These figures describe public assertions. They do not establish successful encryption, independent operating teams or distinct victim organisations [S3].

2. A supplier boundary can determine the incident's real scope. The selected disclosures distinguish a customer-management integration, hosted business applications, legal-service records and a learning platform. A supplier event can affect many customers while remaining one incident at the provider. Scope the actual permissions and affected information before describing an intrusion into every customer's own systems [S19][S22][S23][S24][S8].

3. Information loss and operational disruption require separate decisions. Amgen's July filing concerns cloud-held information and states specific operational exclusions. Stryker's March incident disrupted business operations, with a later restoration milestone. Neither account establishes the same effects at another manufacturer. Continuity exercises should test the service dependency described by the evidence [S12][S14].

4. Identity recovery must cover sessions and application permissions. Official warnings describe device-code lures, malicious application consent and messaging-account recovery. These involve different trust decisions. An account password change may leave another permission or session question unresolved. Identity owners should examine the access mechanism supported by their own evidence [S48][S49][S66][S67].

5. The closing period rewards careful classification. A website-script supplier incident, malware-disruption actions and patching notices provide concrete response tasks. A separate NSA statement attributes internal service degradation to routine maintenance. Concurrent stories do not establish a common actor or a coordinated intrusion [S10][S45][S61][S62][S65].

6. Current listings justify dated account validation. Credentials were listed for sale for 172 of 250 selected estates when checked. The national Atlas headline is 80/100. At least 2,251,336 device associations and 117,106,392 credential-record associations require separate ownership and freshness checks. These are overlapping observations, not confirmed intrusions [S2].

Four decisions for leaders

1. **Assign an owner to each credible intelligence signal.** Require a documented match, account or service relevance, current activity assessment and escalation decision. A claim-only alert can close with a reasoned disposition; corroborated unauthorised activity enters incident response.
1. **Map supplier permissions around essential services.** Identify who can export data, administer identities, change customer-facing scripts or restore operations. Test the emergency restriction and initial-notification route with the supplier.
1. **Use one fact record for several reporting decisions.** Record awareness, materiality, service impact and affected-data assessments separately. Legal, privacy and communications teams should work from those facts while applying the relevant reporting trigger.
1. **Demonstrate recovery with business owners.** Restore an important service using protected data and separate recovery access. Test a usable fallback, reconcile interrupted work and obtain business sign-off before declaring the exercise complete.

The year in numbers

These figures retain their separate populations and periods.

4,605

US-labelled extortion records in the source snapshot [S3]

WHAT IT IS NOT

Confirmed intrusions or distinct victims

3,996

US-labelled listings in the whole of 2025 [S3]

WHAT IT IS NOT

A matched-duration baseline for partial 2026

149

Group labels attached to window records [S3]

WHAT IT IS NOT

Independently verified operating teams

357

Publication-dated records in 8–22 November [S3]

WHAT IT IS NOT

Confirmed attacks starting in that period

250

Selected operating estates in ten sector groups [S2]

WHAT IT IS NOT

A representative national sample or revenue ranking

80/100

National Atlas headline for the selected portfolio [S2]

WHAT IT IS NOT

A breach percentage, intrusion probability or sector ranking

172 of 250

Estates with a credential listed for sale when checked [S2]

WHAT IT IS NOT

Accounts sold, usable credentials or confirmed intrusions

At least 2,251,336

Device associations, including 633,281 employee-device associations [S2]

WHAT IT IS NOT

Unique US endpoints or verified current infections

117,106,392

Historical credential-record associations [S2]

WHAT IT IS NOT

Unique people, active accounts or records first exposed in 2026

29

Source-supported incident and disclosure families [S6][S8][S10][S12][S14][S16][S17][S18][S19][S20][S21][S22][S23][S24][S25][S26][S29][S30][S31][S32][S84][S85][S86][S87][S88][S101][S102][S103][S107][S108][S109][S110][S111]

WHAT IT IS NOT

Twenty-nine independently dated new attacks in 2026

37,866

Distinct retained post records available for case analysis [S1]

WHAT IT IS NOT

Unique offers, people or incidents

248

Estates with passive observations [S2]

WHAT IT IS NOT

A complete assessment of every associated service

The total describes 4,605 publication-dated claim records, including 357 dated within the recent window. A dated listing does not authenticate the alleged incident or establish when unauthorised activity occurred [S3].

KEY TAKEAWAYS

01

Keep posts, listings, disclosures and control observations separate.

02

Validate account and supplier relevance before choosing disruptive containment.

03

Fund recovery and factual notification with accountable owners.

Report map

Begin with the decision you own, then follow its evidence and completion test.

Board and executives	Which service risks justify investment and accepted exceptions?	01 05 11 12
CISO and security leads	Which identities, suppliers and recovery dependencies need validation?	03 05 06 10 12
SOC and threat intelligence	What is claimed, who reports it and what is established?	04 06 07 B
Fraud and customer protection	Which customer and payment decisions need a different check?	04 05 08 09
Legal and communications	What can be said, and which reporting decision has begun?	05 06 10 12

01 Summary
Decisions justified by the available evidence

02 Context
Digital-service dependencies and national-statistic limits

03 Exposure
Selected-estate observations and their proper interpretation

04 Underground
Advertisements, chronology and unverified propositions

05 Disclosures
Source-supported cases with distinct operational and data boundaries

06 Disruption
Availability, operational systems and claim-versus-impact evidence

07 Actors
Source-attributed campaigns, listing labels and supported relationships

08 Fraud
Identity, account, employment and payment opportunities

09 Banking
Financial-service validation and joint response decisions

10 Regulation
Different legal scopes, triggers and notification recipients

11 Outlook
Conditional scenarios and signals that change the assessment

12 Actions
Owners, timing and demonstrable completion

CHAPTER 02

Digital services and the US threat context

THIS CHAPTER ANSWERS

Which features of the US operating environment change a defender's priorities?

93.1%

internet penetration in DataReportal's October 2025 baseline

2.1 A connected population, with a dated baseline 11
2.2 An annual crime report is context, not a 2026 attack total 11
2.3 Shared providers create several kinds of dependency 12
2.4 Local operations and national services require different recovery evidence 12
2.5 Neutrality applies to attribution and policy context 13
2.6 What the public-source sweep establishes 13

CHAPTER 02

Digital services and the US threat context

IN SHORT

The US evidence spans national providers, local services, cross-border platforms and regulated information. A service can depend on a supplier's identity system, browser code or recovery process. National complaint statistics and official warnings describe different populations from this report's posts and listings. Political attribution requires its own source. Map the service, data custodian, supplier permissions and reporting owner before an incident forces those decisions.

2.1 A connected population, with a dated baseline

DataReportal's Digital 2026 report gives 324 million US internet users and 93.1% internet penetration. Those figures describe October 2025, rather than measurements made throughout this report's observation window. Its 417 million cellular connections also describe the end of 2025. Connections are not unique subscribers [S76].

The security implication is an analyst judgement. Customer and employee identities connect banking, education, healthcare, communications and public services. Information obtained in one context can make an impersonation attempt elsewhere more convincing. That does not establish that the second service lost information or that every exposed record was used.

A useful identity review consequently extends beyond the login form. Account recovery, contact-centre verification, contractor onboarding, application consent and payment changes all decide who has authority. A strong sign-in control can coexist with a weaker recovery or integration permission.

Digital access also changes the continuity question. An available homepage is insufficient if a patient order, financial transaction or public notice cannot complete. Business owners should define the function that must continue, the acceptable fallback and the evidence needed to restore normal work.

2.2 An annual crime report is context, not a 2026 attack total

The FBI IC3's 2025 annual report records 1,008,597 complaints and approximately $20.877 billion in reported losses. It was published in 2026 but describes 2025 reporting. Complaints are not a census of all incidents, and reported losses are not a measure of every victim's eventual loss [S5].

Those figures cannot be added to the 4,605 extortion records in this report. The source, year, reporting route and unit differ. A complaint may describe investment fraud, identity misuse or another crime without a ransomware listing. A listing may remain an unverified criminal assertion.

Use the annual report to test the breadth of the response programme. Fraud, customer support, identity operations and law enforcement liaison may need to work together. Do not use it to calculate a 2026 probability of intrusion from an unrelated post or selected-estate population.

Evidence population	Unit	Appropriate use
Country-associated posts	Published messages	Identify a specific claim worth validating
Extortion records	Public criminal assertions	Prepare continuity and disclosure decisions
IC3 complaints	Reports under the FBI's reporting definitions	Understand reported crime and loss categories in the stated year
Breach notifications	Reports meeting a particular legal or regulatory scope	Assess the stated data and affected-person questions
Original disclosures	An organisation's or authority's account	Compare a specific mechanism and response choice
Selected operating estates	Purposive domain-associated observations	Assign validation to the appropriate owner

2.3 Shared providers create several kinds of dependency

The public cases show dependencies in customer-management integrations, legal services, clinical business applications, learning platforms and website experimentation. These are different relationships. The supplier controlling a data export may be different from the supplier that restores the service [S19][S22][S23][S8][S10].

For each essential service, record the identity provider, data custodian, integration administrator and recovery provider. Identify who can stop an export, remove a permission or provide investigation records. A contract contact alone may not know the technical authority required during an incident.

An integration also deserves a separate lifecycle. Its initial approval, credential ownership, actual data access and removal process can outlive the staff member who requested it. Include dormant applications and inherited permissions in a service review, with the business owner deciding which remain necessary.

The cases do not establish one universal supplier entry route. A browser-script flaw differs from a social-engineered contractor session. Both justify a permission review, but the investigation should follow the mechanism actually supported by the relevant evidence.

2.4 Local operations and national services require different recovery evidence

Minnesota's July statement describes malicious activity involving technology at more than 30 community water systems. It explicitly warns that an impacted system does not mean every community experienced water-service disruption. The state had not attributed the activity to a particular actor [S6].

A national provider may need to reconcile orders across many sites. A local utility may need to operate safely while remote monitoring is unavailable. Recovery must therefore demonstrate the relevant business or physical function, rather than treating the return of a management interface as sufficient.

For operational systems, include the process owner in access and restoration decisions. A security change can affect monitoring, alarms or maintenance arrangements. The report's recommendation is to validate intended connectivity and usable fallback procedures, without assuming that every visible device or screenshot establishes physical impact.

2.5 Neutrality applies to attribution and policy context

This report takes no position on the federal administration, political parties, Congress, elections, agency staffing or budgets, tariffs, immigration or foreign policy. State links remain the cited source's assessment. Language, a country label, a persona's chosen name and political rhetoric do not establish nationality or state control.

The FBI and CISA's October election warning concerns phishing and smishing directed at election and campaign officials. It does not establish altered votes, manipulation of results or a successful intrusion against every recipient. The appropriate control questions apply regardless of party or affiliation [S56].

The same discipline applies to water-system activity. A source-attributed national campaign and a state's unattributed incident set can coexist. The report does not resolve that difference by assigning one actor to every local event. A shared device type or date is insufficient evidence.

Policy developments enter the report only where they change a defender's operating decision. Chapter 10 distinguishes rules already in force from a final-rule submission still marked under review. It makes no judgement about whether a government decision was desirable [S40].

2.6 What the public-source sweep establishes

The public-source review covers selected priority organisations and campaigns, with notices from each month of January–November. It includes CISA material, FBI IC3 warnings, DOJ actions, NSA publications, selected regulatory filings and state-submitted notices. English and Russian reporting support discovery and comparison with the original account.

The outcome is a source-supported set of cases and campaign notices, rather than a census of every US organisation or disclosure. Healthcare and life-science cases are prominent because the selected original filings provide unusually specific data and operational boundaries. Their share does not measure the national sector distribution.

The HHS portal view is partial. Its submission dates and affected-person fields are not intrusion dates or a complete calendar-year total. Selected state notices likewise describe particular jurisdictions and resident populations. Missing monthly archive coverage does not establish that no event occurred [S33].

A report reader should use these cases to ask better questions of their own services. The strongest result is a defensible scope decision, with facts, alternatives and an owner. A larger unsupported national total would not improve that decision.

KEY TAKEAWAYS

01

Digital-adoption and annual crime figures keep their earlier measurement periods.

02

Shared providers require service-specific access and recovery decisions.

03

Official attribution and political claims remain tied to their sources.

CHAPTER 03

National exposure: the selected operating-estate portfolio

THIS CHAPTER ANSWERS

Which external signals require account and service validation across the selected portfolio?

172 of 250

estates had a credential listed for sale when checked

3.1 Universe card 16
3.2 The national headline and sector signal counts 17
3.3 Email-authentication observations 18
3.4 DNS, certificates and web controls 19
3.5 Devices, credentials, documents and current listings 20
3.6 From a public observation to an owner decision 23
3.7 What leadership should ask of the portfolio 24

CHAPTER 03

National exposure: the selected operating-estate portfolio

IN SHORT

Credentials were listed for sale for 172 of 250 selected estates when checked. The national Atlas headline is 80/100. The portfolio contains at least 2,251,336 device associations and 117,106,392 credential-record associations. These are overlapping observations, not unique people or confirmed intrusions. Historical records and customer accounts can contribute to the totals. Assign current-listing validation, employee-device investigation and service checks to accountable owners.

3.1 Universe card

Item	Definition
Selected population	250 US-relevant operating estates; 25 selected estates in each of ten sectors
Selection	Purposive service and sector relevance; neither a revenue ranking nor a probability sample
Unit	A primary domain estate associated with an operating organisation or service
Organisational overlap	Parents, subsidiaries, public bodies and university medical systems can share ownership or infrastructure
Exposure snapshot	22 November 2026; all 250 selected estates
Exposure periods	Device, credential and document records are cumulative observations available on that date, rather than 2026-only events; current listings describe the snapshot
Other periods	Mention context: 23 November 2025–22 November 2026; lookalike context: the preceding 30 days
Passive snapshot	22 November 2026; 248 estates with assessed observations
Web-control coverage	155 available results; 93 unavailable results among the assessed estates
Publication	National Atlas headline and anonymous sector signal counts
Interpretation	Associations can overlap across estates, records and people; the portfolio does not estimate national prevalence

A selected estate is not automatically an independent legal entity. International providers can have activity outside the United States, and a shared government domain can support several bodies. The portfolio consequently does not estimate the share of US employers with an active incident [S2].

3.2 The national headline and sector signal counts

The national Atlas headline is 80/100. Higher values indicate greater observed exposure in this selected portfolio. The headline is not a breach percentage, an intrusion probability or a certification of control effectiveness [S2].

Only the national Atlas headline is published. Sector rows show measured signal counts with 25 selected estates per sector. Equal selected counts do not imply equivalent economic size, user populations or technical architecture.

Current credential listings concern 172 of the 250 selected estates

	Current credential listings	Credential listing history	Employee device associations	Document associations
Federal public services	16/25	15/25	22/25	25/25
State and local services	16/25	16/25	22/25	23/25
Banking and financial services	22/25	21/25	25/25	25/25
Insurance and health coverage	18/25	18/25	24/25	24/25
Healthcare and life sciences	13/25	13/25	23/25	23/25
Universities and research	19/25	19/25	25/25	25/25
Technology and communications	22/25	21/25	25/25	24/25
Energy and utilities	9/25	9/25	22/25	24/25
Transport and industrial services	15/25	15/25	25/25	24/25
Retail and consumer services	22/25	22/25	24/25	25/25

Current credential listings by sector (coral). Each cell shows observed estates / selected estates; signals overlap. Source: Brandefense Atlas and Blackhole associations, 22 November 2026. 250 selected estates; cumulative overlapping associations, not confirmed intrusions or unique people [S2].

The listing, employee-device and document columns count estates with each observation. One estate can appear in several columns; these counts cannot be added as affected organisations.

Sector	Selected estates	Estates with current listings	Estates with employee devices	Estates with documents
Federal public services	25	16	22	25
State and local services	25	16	22	23
Banking and financial services	25	22	25	25
Insurance and health coverage	25	18	24	24
Healthcare and life sciences	25	13	23	23
Universities and research	25	19	25	25
Technology and communications	25	22	25	24
Energy and utilities	25	9	22	24
Transport and industrial services	25	15	25	24
Retail and consumer services	25	22	24	25
Total	250	172	237	242

Current credential listings concern 22 estates in each of banking, technology and retail. A listing supports an account-validation task; it does not establish successful access. Lower selected counts in another sector do not establish that sector's national risk level.

3.3 Email-authentication observations

The available observations are summarised below. A published policy describes what the domain requests; it does not demonstrate enforcement for every outgoing message or service [S2].

Observation	Estates	Assessed denominator
DMARC reject policy	169	248
DMARC quarantine policy	41	248
DMARC monitoring policy	32	248
DMARC policy not observed	6	248
SPF record observed	240	248
DKIM key observed	201	248

A reject or quarantine policy can support domain-spoofing protection when legitimate senders and message authentication are configured correctly. A monitoring policy has a different purpose. The messaging owner should validate actual mail flows before changing enforcement [S80].

An SPF record is not proof that every authorised sender is covered. A DKIM key observation does not establish that every outgoing message is signed. A key not observed in this assessment is not proof of absent signing. Preserve those distinctions in remediation tickets and leadership reports.

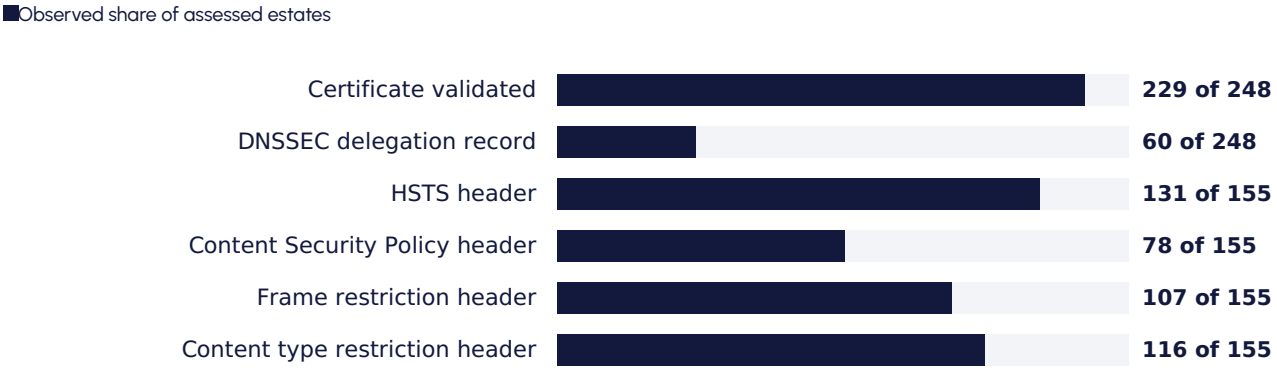
Review the intended use of each estate. Staff mail, transactional messages, delegated marketing and a domain that sends no mail can need different decisions. A policy change should have an approved sender inventory, a delivery test and a rollback owner.

3.4 DNS, certificates and web controls

The observations below retain their own assessed populations. An unavailable result is not classified as an absent control or a confirmed defect [S2].

Observation	Result	Assessed denominator
DNSSEC delegation record observed	60	248
CAA record observed	52	248
Certificate validated	229	248
Certificate result did not validate	5	248
Certificate result unavailable	14	248
Web-control result available	155	248
Web-control result unavailable	93	248
HSTS header observed	131	155
Content Security Policy header observed	78	155

Public web and DNS observations keep their available-result denominators



Source: dated public-control observations, 22 November 2026. Each control retains its own assessed-estate denominator; observations do not establish complete service assurance [S2].

A DS record indicates a DNSSEC delegation record. It does not by itself establish an end-to-end validated signing chain. A public certificate result is also specific to the service and time checked; it does not establish the security of the application [S81].

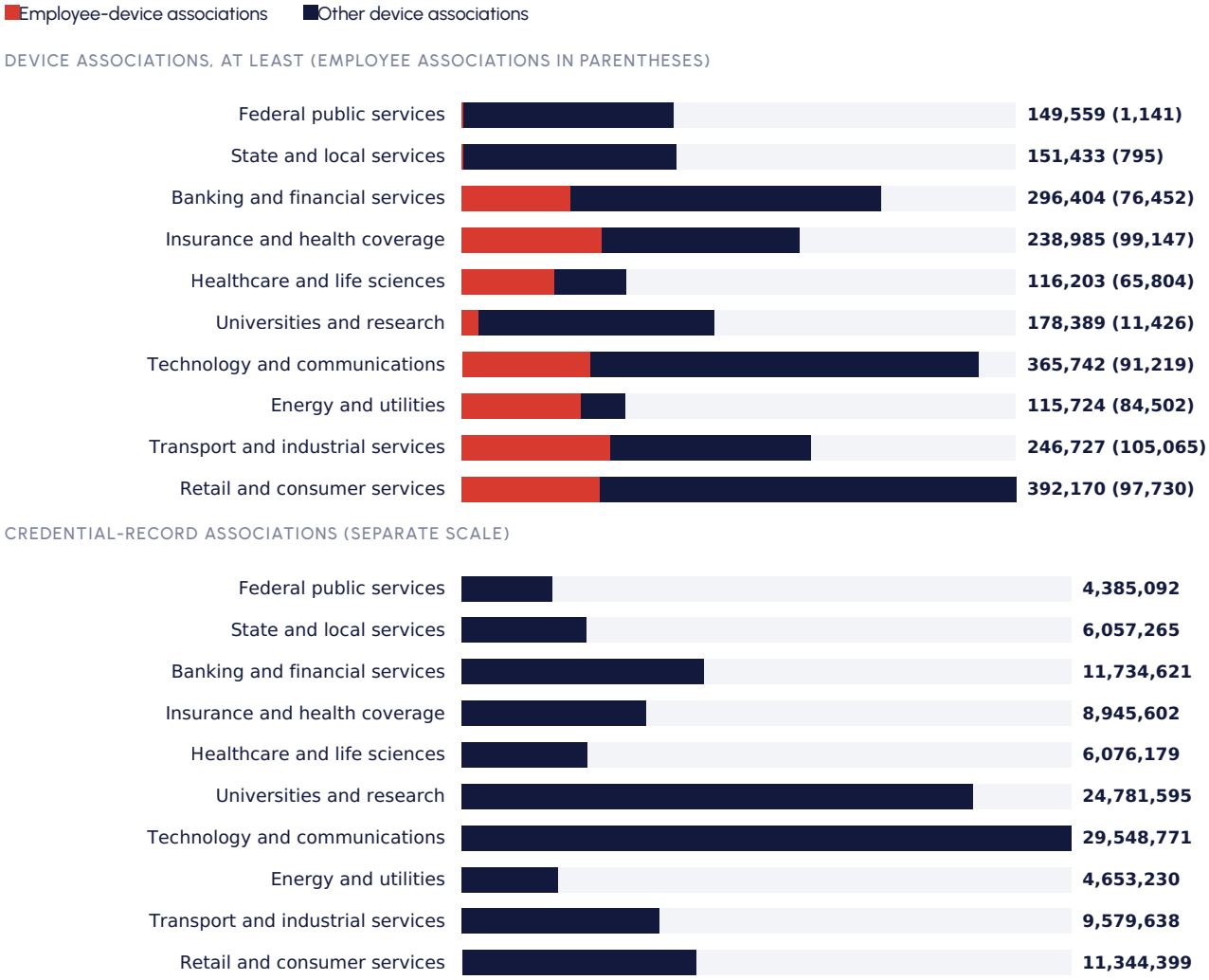
HSTS tells supporting browsers to use HTTPS for the covered host. Content Security Policy constrains the content that a browser can load or execute. A visible header does not demonstrate that every relevant page or policy is effective, particularly where services and intermediaries differ [S82][S83].

For customer-facing scripts, the useful assurance includes what is permitted, who can change it and what happens when a provider changes content. The website-script case in Chapter 5 illustrates why an approved provider relationship still needs a permission and response decision. A header observation alone does not settle that issue [S10].

3.5 Devices, credentials, documents and current listings

The exposure snapshot contains device associations for 247 estates and credential-record associations for all 250. Employee-device associations appear at 237 estates. The table retains each signal's separate unit [S2].

Device and credential associations differ in scale and require separate owners



Source: Brandefense Atlas and Blackhole associations, 22 November 2026. 250 selected estates; cumulative overlapping associations, not confirmed intrusions or unique people [S2].

Sector	Estates with devices	Devices, at least	Employee devices	Credential records
Federal public services	25 of 25	149,559	1,141	4,385,092
State and local services	25 of 25	151,433	795	6,057,265
Banking and financial services	25 of 25	296,404	76,452	11,734,621
Insurance and health coverage	25 of 25	238,985	99,147	8,945,602
Healthcare and life sciences	24 of 25	116,203	65,804	6,076,179
Universities and research	25 of 25	178,389	11,426	24,781,595

Sector	Estates with devices	Devices, at least	Employee devices	Credential records
Technology and communications	25 of 25	365,742	91,219	29,548,771
Energy and utilities	23 of 25	115,724	84,502	4,653,230
Transport and industrial services	25 of 25	246,727	105,065	9,579,638
Retail and consumer services	25 of 25	392,170	97,730	11,344,399
Total	247 of 250	2,251,336	633,281	117,106,392

Device counts are lower bounds. Employee devices are included in the device view and must not be added to its total. Associations not identified as employee devices total 1,618,055; their ownership is not established.

Credential records comprise 56,585,503 breach-database records, 8,232,886 stealer-log lines and 52,288,003 combolist entries. These are historical associations, not unique people or currently usable accounts. A person or record can appear in several populations.

Technology and communications contributes 29,548,771 credential-record associations, while universities and research contributes 24,781,595. Together they account for 46.4% of the portfolio's credential records. Domain use and historical visibility can contribute to these totals; the share is not an intrusion rate.

Retail and consumer services has at least 392,170 device associations, including 97,730 employee-device associations. A login associated with a consumer brand does not establish an intrusion into the provider's corporate estate. Fraud, customer and employee-response owners need different validation paths.

172 of 250

estates with a credential listed for sale when checked

633,281

employee-device associations within the device population

42,235

document associations across 242 selected estates

Current listings require account validation. Credentials were listed for sale for 172 estates at the snapshot. Listing history appears at 169 estates; 169 have both observations. Those populations overlap and do not count completed sales or active sessions.

Establish whether a credible advertised account exists, which service it concerns, whether it remains active and whether prior remediation addressed it. Compare the signal with authorised internal evidence. Containment should follow corroborating activity and business impact.

Documents and lookalikes require contextual review. There are 42,235 document associations across 242 estates. Public documents and repeated material remain possible explanations. A reference does not establish sensitivity, unlawful acquisition or continued access.

The preceding 30-day lookalike context contains 128,171 candidate-domain associations across 240 estates. Similar names can concern unrelated services. A candidate is not a confirmed phishing site, and these counts do not establish distinct malicious campaigns.

Mention context covers 23 November 2025–22 November 2026. Dark-chat mentions concern 206 estates and dark-web mentions concern 214; these estate populations can overlap. Mentions establish visibility, rather than hostile intent or a new 2026 incident. A familiar service can appear in benign links as well as advertisements.

Each account, document or service requires its own validation. A historical credential record is not proof of a currently usable account. A device associated with a consumer service is not automatically an endpoint operated by that provider.

3.6 From a public observation to an owner decision

Observation or signal	First validation	Action trigger	Closure evidence
Unexpected email policy	Confirm domain purpose and authorised senders	Owner confirms an unintended configuration	Approved change and successful delivery checks
Unavailable certificate or web result	Establish the intended service and its actual state	Owner identifies a service or configuration problem	Service validation and documented resolution
Credible credential offer	Match an active account, prior remediation and relevant activity	Corroborated exposure or unauthorised use	Identity investigation, relevant session action and disposition
Employee-device association	Confirm account relationship and managed-device ownership	Evidence of an affected managed endpoint	Endpoint and identity recovery evidence
Document reference	Establish sensitivity and authorised availability	Owner confirms unintended disclosure	Access correction and privacy assessment
Similar-name reference	Establish ownership and actual use	Evidence supports impersonation or abuse	Recorded investigation and authorised response

Do not force every observation into the same response queue. Messaging owners can interpret policy records, service owners can assess availability, and identity teams can validate accounts. Incident command becomes appropriate when the evidence establishes a wider incident or a material service effect.

3.7 What leadership should ask of the portfolio

Ask whether every assessed estate has a responsible owner and whether unavailable observations have a documented disposition. A high count of visible controls does not demonstrate complete protection. A small number of unavailable results does not establish that those estates are insecure.

The most useful assurance is a demonstrated correction or a supported decision that no change is necessary. Keep the observation date, service boundary and validation record together. Recheck after an important migration, supplier change or incident, rather than treating the snapshot as permanent certification.

KEY TAKEAWAYS

01

The selected portfolio does not estimate national prevalence or independent legal entities.

02

Public control observations keep their assessed denominators and service limits.

03

Validate ownership and current relevance before remediation or incident claims.

CHAPTER 04

Underground evidence: advertisements, listings and the limits of a claim

THIS CHAPTER ANSWERS

What is advertised about US-relevant information or access, and what would validate the claim?

4,605

publication-dated extortion claims in the window

4.1 What the retained post evidence establishes 26
4.2 Country-associated post chronology and population boundaries 35
4.3 Extortion publications across the window 37
4.4 Regional context without a national ranking 38
4.5 Group labels and concentration 38
4.6 Sector context 39
4.7 An intelligence disposition that can be defended 39

CHAPTER 04

Underground evidence: advertisements, listings and the limits of a claim

IN SHORT

Retained posts provide examples of advertised information, accounts and access. They do not authenticate an offer or establish a completed sale. The separate extortion snapshot contains 4,605 US-labelled publication-dated claims, spread across 149 group labels. Its October count is 569; November covers only the available period through 22 November. Keep intelligence records separate from confirmed incidents, and validate a credible match against current accounts, service ownership and business impact.

4.1 What the retained post evidence establishes

The retained evidence contains 37,866 distinct in-window posts, including 3,081 dated 8–22 November. This is the evidence set considered for the cases and circulation examples. It is not the complete population of US-related advertising or a representative sample of criminal activity [S1].

Brandefense Blackhole observations establish the retained text and its recorded post timestamp. An advertiser can use a country name to describe customers, records, account eligibility or a desired market. That reference does not establish where an intrusion occurred or who operates an affected system [S1].

The cases below therefore separate the advertised proposition from the defender's validation task. A price is an asking price. A claimed date is the advertiser's account of freshness. Neither establishes payment, delivery, current access or authentic contents.

The public cards withhold organisation identifiers and contact routes. Role labels deliberately fit several bodies. Their purpose is to explain the decision supported by the evidence, rather than make an unverified accusation against an identifiable organisation.

CASE A

A

An analytics archive advertised after claimed access was lost

Unverified claim

Evidence card B01 | 31 Mar 2026 | Forum | A marketing-analytics data business

Bottom line

An archive offer does not establish current access or a new intrusion.

Evidence card B01 — 31 Mar 2026

Anonymous advertiser | Forum | Forum | English

ORIGINAL

Total dumped data: 381 GB. [...] Price: $15,000 [...] access is lost

TRANSLATION

Source English; organisation, personal and contact identifiers omitted where present.

Held

A forum seller advertises an analytics database archive, assigns a March incident date, and explicitly says the entry-point access is lost. The seller describes personal, contact, employment and interest-related fields.

Not established

Authentic contents, extraction date, current access, unique people or a completed sale.

- **Observed.** A 31 March forum post advertises a marketing-analytics archive and says the claimed entry-point access was lost. The advertised 381 GB size and $15,000 price are seller statements [S1].
- **Chronology.** The seller assigns an incident date in March. Some displayed field dates concern 2024, which does not date the whole archive. Similar advertising appears in another retained post.
- **Claimed scope.** The post describes personal, contact, employment and interest-related fields. Its row and email-table figures use different units. They cannot be added or treated as independently verified affected people.
- **Alternatives and limits.** Historical marketing exports, public or commercial leads, mixed-source records, misattribution and fabrication remain alternatives. The offer does not authenticate contents, ownership, extraction date, a completed sale or current access.
- **Response.** Have data and marketing owners compare credible details with authorised exports and retention. Escalate an incident when internal evidence corroborates relevance, and keep any historical-data assessment separate from current account access.

CASE B

B

Privileged hosting access and hosted data offered together

Evidence card B02 | 30 Apr 2026 | Forum | A shared hosting estate

Unverified claim

Bottom line

Validate service ownership and privileged access before inferring tenant impact.

Evidence card B02 — 30 Apr 2026

Anonymous advertiser | Forum | Forum | English

ORIGINAL

Price: $600 with data included (negotiable) [...] Full root access to [hosting control]

TRANSLATION

Source English; organisation, personal and contact identifiers omitted where present.

Held

A seller offers claimed root and hosting-control access with several hosted databases and user records. US relevance comes from the claimed hosted-organisation context, not independently verified server ownership or location.

Not established

Working privileged access, authoritative ownership, current credentials or a completed sale.

- **Observed.** A 30 April UTC forum seller offers claimed privileged hosting access with data for $600. The advertised bundle includes 41 databases and 2,404 user records. These are assertions within the offer [S1].
- **Claimed scope.** The seller describes control of a shared hosting estate. A hosted service, its provider and its customer organisations can have different ownership boundaries. None is independently authenticated by the post.
- **Evidence boundary.** Displayed technical output is seller-supplied material. It is not a validated administrative session or a check performed by this report. No current password, working access or completed sale is established.
- **Alternatives and limits.** The material could describe a genuine shared-host incident, stale administration data, an authorised export misrepresented as illicit access or fabrication. A claim about hosting control is not proof of access to every tenant.
- **Response.** After corroborating a relevant service match, review privileged sessions, tenant separation and stored customer information. Ask the hosting and identity owners to establish which permissions and tenants the evidence actually concerns.

CASE C

C

A loan-application style record alongside an identity-service advert

Unverified claim

Evidence card B03 | 31 Aug 2026 | Forum | A US-labelled consumer financial lead

Bottom line

A displayed financial record does not identify its source or establish a bank incident.

Evidence card B03 — 31 Aug 2026

Anonymous advertiser | Forum | Forum | English

ORIGINAL

Requested_Loan_Amount [value removed] [...] Income_Type [value removed] [...] Account_Type [value removed]

TRANSLATION

Source English; organisation, personal and contact identifiers omitted where present.

Held

A forum post displays one individual-style record containing identity, employment, loan-application and banking fields, followed by a broader identity-document and account advert.

Not established

A validated person, dataset size, current account or incident at a referenced provider.

- **Observed.** A 31 August UTC forum post displays one financial-application-style record with identity, employment, loan and banking fields. It is followed by a broader identity-service advertisement. Personal values are omitted here [S1].
- **Claimed scope.** One displayed record is an example, rather than a dataset size. The field list does not validate a person, a current account or the advertiser's authority to supply either.
- **Chronology.** The post date establishes circulation during the report window. It does not establish when the information was created, collected or obtained. A similarly formatted record elsewhere does not prove common origin.
- **Alternatives and limits.** Older lead-generation material, a broker export, fabricated examples and mixed-source records remain plausible. A bank or employer reference does not establish that the referenced organisation lost the information.
- **Response.** Fraud and privacy owners should compare credible details with authorised lead sources and retention. Review customer verification where relevant, while avoiding disruptive account action based solely on the uncorroborated example.

CASE D

D

A communications-data claim supplies a record total without authentication

Unverified claim

Evidence card B04 | 31 May 2026 | Messaging channel | A communications provider

Bottom line

A claimed record total and update date require independent validation.

Evidence card B04 — 31 May 2026

Anonymous advertiser | Messaging channel | Telegram | English

ORIGINAL

42M+ Records Updated: 28 May 2026

TRANSLATION

Source English; organisation, personal and contact identifiers omitted where present.

Held

A poster names a communications provider, claims a large personal-data population, and presents a May update date alongside negotiation rhetoric.

Not established

Possession, authentic records, unique people, intrusion date, negotiations or completed payment.

- **Observed.** A 31 May Telegram post claims a communications-provider dataset containing more than 42 million records. It gives 28 May as an update date. The record count and date belong to the poster's account [S1].
- **Claimed scope.** The advertisement presents a personal-data population and negotiation rhetoric. The report retains the data claim while omitting the poster's hostile judgements about the organisation.
- **Evidence boundary.** The post alone does not establish possession, authentic files, unique people, an intrusion date, negotiations or a completed payment.
- **Separate public response.** Direct reporting in late May carries the provider's denial that sensitive personal information was exfiltrated. A later spokesperson response limits the impacted environment to business-customer sales tools [S95][S96].
- **What remains unresolved.** Those quoted statements do not expressly confirm unauthorised access or acquisition. The earlier 40 million actor claim and this 42 million-plus seller claim remain separate assertions. Neither establishes identical archives, unique customers, the alleged entry date or payment [S95][S96].
- **Alternatives and limits.** A genuine archive, older customer records, combined sources, misattribution, inflated totals or fabrication remain alternatives. A large displayed number does not settle the underlying proposition.
- **Response.** Communications and privacy owners should compare internally corroborated record fields and retention. Prepare customer-protection communication when relevance is established, using the confirmed data scope rather than the advertiser's population figure.

CASE E

E

A platform-access offer claims reach across identity and business services

Unverified claim

Evidence card B05 | 31 May 2026 | Messaging channel | A US property-services platform

Bottom line

A broad application list is not authenticated administrative control.

Evidence card B05 — 31 May 2026

Anonymous advertiser | Messaging channel | Telegram | English

ORIGINAL

I have access to [a property-services platform] [...] full access to the admin panel

TRANSLATION

Source English; organisation, personal and contact identifiers omitted where present.

Held

An advertiser claims broad access at a US property-services platform, spanning administration, user accounts, identity, payment, support, customer-management and developer services, plus an internal network.

Not established

Current sessions, administrative permissions, extraction, estate-wide control or a completed sale.

- **Observed.** A 31 May Telegram advertiser asks $30,000 for claimed access to a US property-services platform. The offer lists administrative, identity, support, customer-management and developer services, as well as an internal-network claim [S1].
- **Claimed scope.** The advertiser describes broad permissions. Its organisation-size assertions are not adopted as company facts. A list of application categories does not authenticate any account, session, token or administrative role.
- **Evidence boundary.** No working access, extraction, current permission or completed sale is established. The platform reference also does not establish an intrusion into each separate software supplier named by the poster.
- **Alternatives and limits.** Genuine tenant access, exaggerated contractor permissions, stale session material, a misleading demonstration and fabrication remain alternatives. Estate-wide control requires evidence beyond the breadth of the advert.
- **Response.** Identity and application owners should map relevant trusted applications and administrative grants. Investigate current sessions and export activity after corroborating a credible service match, then constrain the permissions actually supported by the evidence.

CASE F

F

A closing-period buyer asks for richer account context

Evidence card B06 | 22 Nov 2026 | Forum | A marketplace-account buyer

Observed buyer request; supply unverified

Bottom line

Buyer demand is not evidence of supply, account validity or a completed transaction.

Evidence card B06 — 22 Nov 2026

Account-material buyer | Forum | Forum | English

ORIGINAL

Order history, added cards & addresses = big advantage Priority: USA, CA

TRANSLATION

Source English; organisation, personal and contact identifiers omitted where present.

Held

A forum buyer requests high-quality marketplace account logs, preferring US and Canadian accounts with order history, stored cards and addresses.

Not established

Available supply, usable accounts, stored payment validity, a purchase or provider intrusion.

- **Observed.** A 22 November forum buyer asks for marketplace account material and prefers US and Canadian accounts with order history, stored cards and addresses. The retained request establishes demand, rather than available supply [S1].
- **Claimed scope.** The buyer expresses a preference for richer account context. No count of supplied accounts is given. The request does not establish valid stored payment details, an authenticated session or a completed purchase.
- **Chronology.** The post appears on the cut-off date and falls in the recent-activity section. Its date stamp does not imply complete coverage of everything posted that day.
- **Alternatives and limits.** A genuine criminal purchase request, a reseller enquiry, a staged advertisement or a scam remain possible. Buyer demand alone does not establish an intrusion into the marketplace provider.
- **Response.** Account-protection and fraud owners should review corroborated unusual sign-ins, stored-payment use, delivery-address changes and account recovery. The decision should follow actual service evidence, rather than the buyer's preference alone.

Further circulation examples: provenance and age

Evidence card B10 — 2 Jan 2026

Anonymous forum poster | Forum | Forum | English

ORIGINAL

[Paraphrase: A seller advertises project and design files attributed to an engineering-services business, with an archive-size claim and a cryptocurrency asking price.]

TRANSLATION

Paraphrase, not a verbatim quote; organisation, personal, technical and contact identifiers omitted.

Held
A dated circulation record and the proposition described above.

Not established
Authenticity, non-public origin, acquisition date, unique people, current access, a completed sale or a confirmed service consequence.

Evidence card B11 — 4 Jan 2026

Anonymous forum poster | Forum | Forum | English

ORIGINAL

[Paraphrase: A poster asserts disclosure of employer analytics records; the stated service also transforms public records, so non-public origin is unresolved.]

TRANSLATION

Paraphrase, not a verbatim quote; organisation, personal, technical and contact identifiers omitted.

Held
A dated circulation record and the proposition described above.

Not established
Authenticity, non-public origin, acquisition date, unique people, current access, a completed sale or a confirmed service consequence.

Evidence card B12 — 4 Jan 2026

Anonymous forum poster | Forum | Forum | English

ORIGINAL

[Paraphrase: A seller claims customer and purchase-related records from a health-products commerce website and gives an asking price.]

TRANSLATION

Paraphrase, not a verbatim quote; organisation, personal, technical and contact identifiers omitted.

Held
A dated circulation record and the proposition described above.

Not established
Authenticity, non-public origin, acquisition date, unique people, current access, a completed sale or a confirmed service consequence.

Evidence card B13 — 5 Jan 2026

Anonymous forum poster | Forum | Forum | English

ORIGINAL

[Paraphrase: A poster labels an insurance archive with a record count and a US/Canada association; some displayed dates predate the post.]

TRANSLATION

Paraphrase, not a verbatim quote; organisation, personal, technical and contact identifiers omitted.

Held
A dated circulation record and the proposition described above.

Not established
Authenticity, non-public origin, acquisition date, unique people, current access, a completed sale or a confirmed service consequence.

Other retained offers concern engineering project files, employment analytics, health-commerce information and insurance records. An engineering file count does not establish affected people or access to a utility client's network. An employment-data assertion can also concern transformed public records. The original claims do not settle provenance or current access [S1].

The response should follow the relevant data owner. An engineering supplier can hold project information without administering a customer's operational systems. A public-record analytics service can describe an employer without establishing that the employer supplied or lost confidential information.

Further circulation examples: units and repeated publication

Evidence card B14 — 18 Jan 2026

Anonymous forum poster | Forum | Forum | English

ORIGINAL

[Paraphrase: A poster claims internal files from a cross-border consumer-finance business; a reply disputes the apparent personal-information scope.]

TRANSLATION

Paraphrase, not a verbatim quote; organisation, personal, technical and contact identifiers omitted.

Held
A dated circulation record and the proposition described above.

Not established
Authenticity, non-public origin, acquisition date, unique people, current access, a completed sale or a confirmed service consequence.

Evidence card B15 — 22 Jan 2026

Anonymous forum poster | Forum | Forum | English

ORIGINAL

[Paraphrase: A January post circulates a claim expressly dated November 2025 and attributes a US subset to an industrial-auction platform.]

TRANSLATION

Paraphrase, not a verbatim quote; organisation, personal, technical and contact identifiers omitted.

Held
A dated circulation record and the proposition described above.

Not established
Authenticity, non-public origin, acquisition date, unique people, current access, a completed sale or a confirmed service consequence.

Evidence card B16 — 23 Jan 2026

Anonymous forum poster | Forum | Forum | English

ORIGINAL

[Paraphrase: A seller advertises a small identity-record package and asserts company-database access; no source organisation or current access is established.]

TRANSLATION

Paraphrase, not a verbatim quote; organisation, personal, technical and contact identifiers omitted.

Held
A dated circulation record and the proposition described above.

Not established
Authenticity, non-public origin, acquisition date, unique people, current access, a completed sale or a confirmed service consequence.

Evidence card B17 — 25 Jan 2026

Anonymous forum poster | Forum | Forum | English

ORIGINAL

[Paraphrase: A hospitality archive offer gives row counts across several files; rows and files do not establish unique affected people.]

TRANSLATION

Paraphrase, not a verbatim quote; organisation, personal, technical and contact identifiers omitted.

Held
A dated circulation record and the proposition described above.

Not established
Authenticity, non-public origin, acquisition date, unique people, current access, a completed sale or a confirmed service consequence.

One internal-file claim is challenged by a thread reply about its personal-information scope. Both statements remain unverified. Another January post expressly circulates a claim dated November 2025. Neither the reply nor the new post independently dates an intrusion [S1].

An identity package is an advertised record offer, rather than a verified affected population. A hospitality archive lists several files whose rows can overlap. Privacy decisions require owner-confirmed information and people, rather than converting files, rows and contacts into interchangeable units.

Further circulation examples: public services and ambiguous quantities

Evidence card B18	30 Jan 2026
Anonymous forum poster · Forum · Forum · English	
ORIGINAL	[Paraphrase: A forum assertion concerns a local public information website; it supplies no validated impact to voting systems, availability or election results.]
TRANSLATION	Paraphrase, not a verbatim quote; organisation, personal, technical and contact identifiers omitted.
Held	A dated circulation record and the proposition described above.
Not established	Authenticity, non-public origin, acquisition date, unique people, current access, a completed sale or a confirmed service consequence.

Evidence card B19	31 Jan 2026
Anonymous forum poster · Forum · Forum · English	
ORIGINAL	[Paraphrase: A B2B-platform claim lists schema fields and an ambiguous quantity; the number does not supply a usable population denominator.]
TRANSLATION	Paraphrase, not a verbatim quote; organisation, personal, technical and contact identifiers omitted.
Held	A dated circulation record and the proposition described above.
Not established	Authenticity, non-public origin, acquisition date, unique people, current access, a completed sale or a confirmed service consequence.

A local public-information website assertion does not establish access to voter-registration or ballot systems, a service interruption or any election consequence. A separate B2B-platform assertion supplies an ambiguous quantity that cannot support a population count. Neither is added to the confirmed disclosure subset [S1].

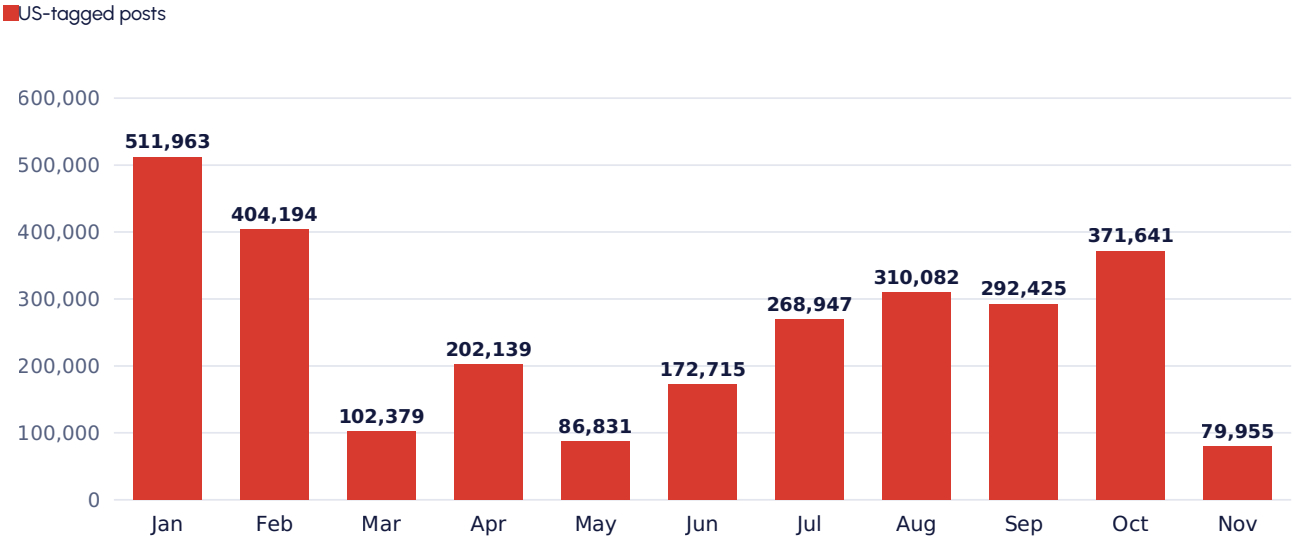
Keep those propositions narrow. Public-service owners can validate hosting and application evidence without adopting a political narrative. Application and data owners can investigate a credible record match without treating a schema field as proof of a working credential.

4.2 Country-associated post chronology and population boundaries

The source records 2,803,271 US-associated posts across the window. Country association is not a finding of criminal content, targeting, residence or a confirmed incident. The monthly population below is separate from the 37,866 retained posts considered for case analysis [S1].

Post month	US-associated posts	Period boundary
January	511,963	Full month
February	404,194	Full month
March	102,379	Full month
April	202,139	Full month
May	86,831	Full month
June	172,715	Full month
July	268,947	Full month
August	310,082	Full month
September	292,425	Full month
October	371,641	Full month
November	79,955	Through 22 November

Country-associated post dates describe source visibility, not national attack activity



Source: Brandefense Blackhole, US-tagged posts, 1 January–22 November 2026; November partial. Separate from 37,866 retained records; not confirmed incidents [S1].

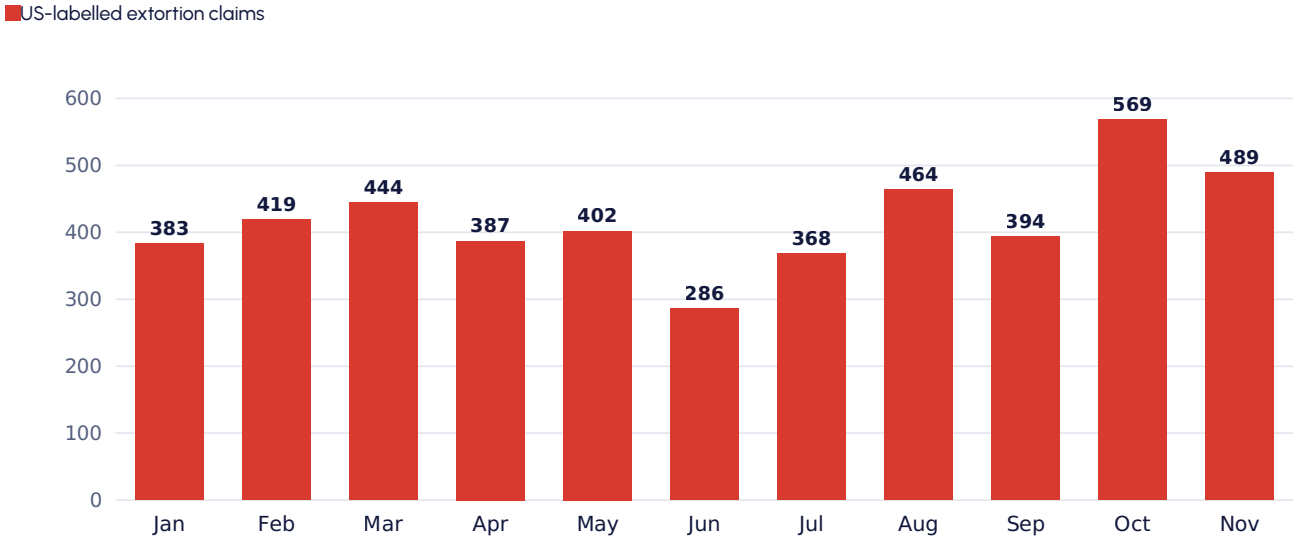
The retained examples are not a representative national sample. Differences between their monthly counts cannot support a claim that attacks increased or decreased by the same amount. A post can also discuss information originating before 2026. Its publication date is not automatically the date of access or data collection [S1].

A newer post can repeat an older offer. Conversely, an old record can still justify a current account review when the service and identity remain relevant. Those are separate questions. Record both the evidence date and the outcome of the current validation.

4.3 Extortion publications across the window

The Ransompedia snapshot contains 4,605 US-labelled claims with publication dates from 1 January through 22 November. These publication dates describe the claims, rather than confirmed intrusion dates [S3].

Monthly extortion publications retain the shortened November period



Source: Brandefense Ransompedia, 1 January–22 November 2026; November partial. Publication-dated country-labelled claims, not confirmed intrusions or distinct victims [S3].

Publication month	Listing claims	Period boundary
January	383	Full month
February	419	Full month
March	444	Full month
April	387	Full month
May	402	Full month
June	286	Full month
July	368	Full month
August	464	Full month
September	394	Full month
October	569	Full month

Publication month	Listing claims	Period boundary
November	489	Through 22 November only
Window total	4,605	1 January–22 November

October has the largest monthly count in this snapshot. That establishes a publication pattern, not the month with the most confirmed intrusions. Disclosure delays, repeated organisation labels and the behaviour of listing operators can affect the pattern. November's shorter duration also prevents a direct full-month comparison [S3].

The same source contains 3,996 US publication-dated listings for the whole of 2025. The two populations have different durations. Their difference should not be presented as a matched year-on-year growth rate or a national ransomware incidence estimate [S3].

The final 8–22 November period contains 357 publication-dated US claims. These are publications during the closing period. The count does not establish 357 attacks starting during those days, 357 independently verified affected organisations or 357 encryption events [S3].

4.4 Regional context without a national ranking

Source country label	1 January–22 November 2026	Whole 2025
United States	4,605	3,996
Canada	392	406
Mexico	108	67
Brazil	206	160
Colombia	74	51

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

Canada and Mexico provide North American service, manufacturing and logistics context. Brazil and Colombia add Americas comparisons across diversified industry and financial services. These are regional reference points, rather than matched populations with equivalent economic size, reporting practices or listing visibility [S3].

The larger US count does not measure a resident's probability of harm or a company's relative security. Country labels can also describe multinational activity. A national resilience ranking would require comparable definitions, populations and independent incident outcomes that these listing counts do not supply.

4.5 Group labels and concentration

The source attaches 149 group labels to the US window population. Qilin accounts for 520 claims, Akira 352, INC Ransom 289, The Gentlemen 261 and Play 180. Together these five labels account for 1,602 of 4,605 claims, or 34.8%. The remaining 3,003 claims carry other labels [S3].

A group label is not a verified person, a stable affiliate or an independent operating team. The source count does not establish that the same initial-access route, malware or negotiation practice applies to every listing under that name. Actor-specific response assumptions need additional evidence.

For a defender, the first question is whether a listing credibly concerns its own service or information. The next questions concern current access, data sensitivity and operational effect. The displayed brand of the claimant does not answer those questions on its own.

4.6 Sector context

The chart groups source industry labels into broad sectors. Each displayed cell covers several source organisation labels. These are listing claims, and the source's industry description is not a verified legal classification. The selected 250-estate portfolio in Chapter 3 is a separate population [S2][S3].

Professional services, healthcare, industry and technology appear in these claims. The categories provide a route to relevant continuity and supplier questions. They do not supply a sector attack rate, a count of confirmed intrusions or a sector Atlas rating.

Professional-service records can concern clients as well as the provider. A manufacturer's event can interrupt delivery without affecting a product already in use. A clinical provider's statement can distinguish business applications from care delivery. Original disclosures in Chapter 5 establish those boundaries more precisely than listing labels alone.

4.7 An intelligence disposition that can be defended

Proposition	What the post or listing establishes	What requires further evidence	Responsible owner
A dataset is advertised	The retained offer and its stated contents	Authenticity, origin, sensitivity and authorised availability	Intelligence and data owner
Account access is offered	An advertiser asserts access	Account match, current permissions and unauthorised activity	Identity and incident response
A credential is described as fresh	The advertiser uses a freshness claim	Actual credential state and relevant session evidence	Identity owner
A company appears on an extortion site	A listing claim exists at a recorded date	Access, encryption, data removal and operational impact	Incident command and business owner
Several posts use a similar persona	The same alias or presentation appears	Human identity, common control or a completed transaction	Intelligence analyst
A public body appears in a disruption claim	The actor asserts an effect	Service availability, duration, cause and actual users affected	Service operations

A disposition can be useful even when it closes without an incident. The record should explain the supported match, the service boundary and the decision. Avoid turning uncertainty into either a breach declaration or a blanket assurance that nothing happened.

Escalation becomes stronger when the organisation can corroborate relevant access, unexpected activity or information outside its intended boundary. Containment should then follow that evidence and the service's operational needs. The action plan in Chapter 12 assigns the resulting identity, supplier and recovery work.

KEY TAKEAWAYS

01

An observed advertisement establishes a claim, rather than authentic data or current access.

02

Extortion publications, group labels and confirmed incidents remain separate populations.

03

Validate a credible match and record the owner, action and evidence supporting closure.

CHAPTER 05

Incident disclosures and targeting by sector

THIS CHAPTER ANSWERS

What did original public notices establish, and what can service owners learn from them?

29

source-supported incident and disclosure families, with separate date limits

5.1 What the confirmed subset means 42
5.2 Healthcare, life sciences and operational services 43
5.3 Integrations and financial information 46
5.4 Clinical business applications and later disclosures 49
5.5 Education and customer-facing suppliers 52
5.6 Public services and public workflows 54
5.7 Additional original disclosures across the window 56
5.8 What these sector examples change 58
5.9 Recent activity: 8–22 November 59
5.10 Follow-up after the headline 60

CHAPTER 05

Incident disclosures and targeting by sector

IN SHORT

The selected disclosures distinguish data access, encryption, supplier interruption, internal information handling and public-workflow abuse. Twenty-nine reporting families support specific defensive lessons. They are not twenty-nine new attacks beginning in 2026 or a national sector distribution. One family concerns a previously disclosed incident, and another concerns internal data handling. Use the original scope to identify the responsible service, validate related access and prepare the appropriate recovery or notification decision.

5.1 What the confirmed subset means

A reporting family groups the notices that the original evidence supports as one provider or organisation event. The website-script case includes a downstream company's response without counting another intrusion into that company's core platform. The education-platform updates likewise remain one provider family.

Twenty-nine families are supported by opened company notices, direct company responses or authority accounts. Twenty-eight appear in this chapter; the water-system family appears in Chapter 6. One is an internal information-handling incident, and one is a 2026 update to a supplier incident already disclosed in 2025. The insurance case spans 2025–2026.

The remaining notices also have different date boundaries. Detection, an actor's communication, materiality and publication can occur on different days. A filing's cover date does not automatically identify the first unauthorised access. Cases retain the date proposition actually supported by the passage.

The selection favours consequential service dependencies and original sources with clear scope. Healthcare and life-science disclosures are prominent. Their share must not be interpreted as the US distribution of attacks, the relative safety of another sector or a measured national trend.

An official disclosure confirms its stated account. It does not automatically authenticate an actor's volume, access route or attribution. Similarly, a stated operational exclusion is not proof that no confidentiality harm occurred. The cases preserve both the established scope and unresolved propositions.

Named cases meet the official-confirmation and wider-reporting rule recorded for this edition. Others use broad roles. Identifying article addresses remain withheld, including addresses embedded in regulator-hosted notices.

5.2 Healthcare, life sciences and operational services

CASE G

G

Stryker's operations and restoration milestone

Healthcare and manufacturing

Company filing; dated recovery milestone

DISCLOSURE	Stryker's April amendment says the company identified an incident on 11 March. It subsequently determined that the disruption materially affected operations and first-quarter financial results. [S12]
CHRONOLOGY	The amendment was filed on 9 April and reports restored manufacturing, commercial, ordering and distribution systems. That is a dated recovery milestone, rather than a fresh November incident.
ESTABLISHED SCOPE	The evidence supports business disruption and restoration. The company's customer updates distinguish product safety from ordering and shipping effects [S13].
ALTERNATIVES AND LIMITS	Early technical assessments can change during investigation. The March updates later identify a malicious file after an earlier no-malware assessment. Neither account authenticates every actor claim or establishes downstream system access.
RESPONSE	Exercise recovery of ordering, manufacturing and distribution together. Reconcile work performed during the interruption, confirm product and service boundaries, and obtain business approval before describing operations as restored.

Bottom line

Recovery must demonstrate the business process, not only the return of individual systems.

CASE H

H

Amgen's information in third-party cloud environments

Life sciences

Company-confirmed data incident

DISCLOSURE	Amgen's 31 July filing says it identified unauthorised activity in third-party cloud environments during July. It confirmed removal of some proprietary information, patient protected health information and other data. [S14]

CHRONOLOGY	The company determined materiality on 29 July. Its filing said the investigation and affected-information assessment continued. The filing date is not the initial access date.
ESTABLISHED SCOPE	The company had not identified impact to products, manufacturing, financial reporting or its ability to meet patient needs as of that filing. Reuters separately reported the disclosure [S15].
ALTERNATIVES AND LIMITS	Data held by a provider can have different access and retention arrangements from core enterprise systems. The notice does not establish one affected-person total, one entry route or every cloud environment's exposure.
RESPONSE	Map sensitive information held by providers and identify who can export it. Review tenant permissions and investigation-record access, while privacy teams prepare field-specific notices based on verified scope.

Bottom line

A data incident can require a substantial response while specified operations remain unaffected.

CASE I

A limited electronic-health-record environment

Healthcare services

Original filing confirms a scoped incident

DISCLOSURE	An electronic-health-record provider reported an approximately eight-hour disruption on 16 March. The filing concerns one of six record environments and the company's belief that an unauthorised party temporarily accessed it. [S16]
CHRONOLOGY	Functionality and access were restored that evening. The company determined materiality on 24 March and filed on 27 March. Those dates describe different decisions.
ESTABLISHED SCOPE	The affected environment held patient information. The filing left access or removal of particular data under assessment and stated that other platforms and environments were not affected.
ALTERNATIVES AND LIMITS	Restored availability does not resolve confidentiality. The source's system boundary also does not establish a complete affected-person population or an intrusion into every healthcare customer.
RESPONSE	Test a clinical fallback for a partial platform outage. Ask the provider for environment-specific data and access evidence, then assess patient notification independently of the restoration milestone.

Bottom line

Service restoration and the patient-data assessment are separate closure decisions.

J

CASE J

A medical manufacturer's network outage

Healthcare and manufacturing

Original filing confirms operational disruption

DISCLOSURE	A medical-device manufacturer reported detection on 25 August. Its 8 September filing describes unauthorised activity and a network outage affecting business applications, manufacturing and order processing. [S17]
CHRONOLOGY	The September account reports substantial distribution restoration and manufacturing resumed at most facilities. It leaves the timing of full recovery uncertain. These are dated statements, not a November status assessment.
ESTABLISHED SCOPE	The disclosure connects an information-system incident to practical manufacturing and shipping effects. It does not establish that every site or product was affected identically.
ALTERNATIVES AND LIMITS	An operating interruption can have different effects on inventory, orders and patient needs. A company-level financial assessment does not provide a general national loss estimate or a common actor link.
RESPONSE	Identify which manufacturing and fulfilment processes rely on central applications. Test a controlled fallback, order integrity and restart sequence with operations, quality and customer-service owners.

Bottom line

An outage exercise should follow an order through production and delivery.

K

CASE K

Impersonation against healthcare personnel

Healthcare services

Company account investigation continuing at filing

DISCLOSURE	A healthcare-management company's September filing describes impersonation of personnel and spoofing of its corporate telephone number. Employees were contacted in attempts to obtain unauthorised system access. [S18]
CHRONOLOGY	The company determined materiality on 22 September and filed the next day. The filing does not establish the initial access date or a complete affected-person total.

ESTABLISHED SCOPE	The company believed private or confidential information had been accessed or acquired. Its stated response included credential resets, remote-tool restrictions, clean-backup restoration and improved monitoring.
ALTERNATIVES AND LIMITS	A familiar displayed telephone number is not proof of the caller's authority. The filing does not establish the scope of every attempted contact or one verified actor for similar calls elsewhere.
RESPONSE	Test independent verification for service-desk and staff requests. Require recorded approval for high-impact recovery and remote access, and investigate relevant sessions when internal evidence corroborates an attempt.

Bottom line

Verify authority through a trusted process, not through the incoming caller's presentation.

5.3 Integrations and financial information

L

CASE L

A customer-management integration at a communications provider

Technology and communications

Original filing identifies an integration boundary

DISCLOSURE	A communications-services company reported unauthorised access through a third-party application integration connected to its customer-management system. The disclosed access occurred on 11–12 June. [S19]
CHRONOLOGY	The company was informed on 13 June and filed on 23 June. Its account says the integration was disabled and the unauthorised access removed.
ESTABLISHED SCOPE	The source identifies customer contact details, fragmented contract and opportunity information, and sales notes. It limits the incident to information accessible through that integration and reports no service interruption at filing.
ALTERNATIVES AND LIMITS	A connected application's permission can expose a meaningful subset without proving access to every customer-management record or the service provider's wider infrastructure. No separate incident at each customer is inferred.
RESPONSE	Review integration permissions, data exports and dormant applications. Test how quickly the platform owner can disable a specific integration while preserving investigation records and customer operations.

Bottom line

The integration's actual permissions define the first investigation boundary.

CASE M

M Internal disclosure through an unapproved AI application

Banking and financial services

Confirmed internal information-handling incident

DISCLOSURE	A regional financial-services company reported an internal incident involving non-public customer information handled with an unauthorised AI-based application. It became aware on 5 May. [S20]
CHRONOLOGY	Materiality was determined on 7 May and the filing followed on 11 May. The incident's cause and full scope were still being investigated at filing.
ESTABLISHED SCOPE	The disclosed information included customer names, Social Security numbers and dates of birth. The company said banking operations, account access, payment systems and core infrastructure were not disrupted.
ALTERNATIVES AND LIMITS	This is not presented as an external attacker intrusion or evidence that every AI application exposes information. The relevant proposition is the company's confirmed unauthorised handling of customer data.
RESPONSE	Give staff an approved route for necessary AI-assisted work. Validate data permissions, retention and acceptable inputs, and make internal disclosures reportable without waiting for an external-attack label.

Bottom line

A material information incident can occur without an attacker or an outage.

CASE N

N A banking investigation and a deletion representation

Banking and financial services

Original amendment: erasure not independently verified

DISCLOSURE	A regional banking company's 30 July amendment says an unauthorised actor accessed parts of its network and removed data. The company was still determining the information's nature and scope. [S21]
CHRONOLOGY	The amendment continues an earlier June filing. It does not establish a new July intrusion merely because an update was published then.

ESTABLISHED SCOPE	The company described efforts to suppress the data, including obtaining the actor's representation that it had deleted information. The representation is something the company received, not independent evidence of erasure.
ALTERNATIVES AND LIMITS	A promise, a removed listing and inaccessible material are different observations. None alone establishes that every copy was destroyed, that no onward transfer occurred or that exposed identities are no longer useful.
RESPONSE	Base privacy and customer-protection decisions on the established disclosure risk. Preserve the negotiation and evidence record through the authorised response process, and continue relevant fraud monitoring after technical containment.

Bottom line

A deletion assertion cannot substitute for an affected-data and customer-risk decision.

CASE O

Financial information at a legal-service provider

Banking and financial services

Original filing: supplier environment distinguished

DISCLOSURE	A financial-services company said it learned on 8 June of ransomware affecting a law firm that provided services to it. The firm's notice described access to company-related borrower information. [S22]
CHRONOLOGY	The company determined materiality on 29 June and filed on 2 July. Those dates do not establish when the provider's unauthorised access began.
ESTABLISHED SCOPE	Borrower information included contact, birth-date and Social Security information. The company reported no evidence of unauthorised access to its own systems and no resulting disruption to its customer services.
ALTERNATIVES AND LIMITS	Legal-service records can remain sensitive even when they are outside production banking systems. One supplier incident should not be counted as an independently verified intrusion into each client.
RESPONSE	Include legal and professional advisers in sensitive-data inventories. Agree evidence access, retention and prompt notice, and test customer verification against the information that the provider actually held.

Bottom line

A professional-services supplier belongs in the data and notification dependency map.

5.4 Clinical business applications and later disclosures

P

CASE P

A contractor session and healthcare business applications

Healthcare services

Company-confirmed session and data incident

DISCLOSURE	A home-healthcare company attributed unauthorised cloud-application access to social engineering of a third-party contractor's user session. Its filing confirms data removal and access to external health-record portals. [S23]
CHRONOLOGY	An actor communication arrived on 15 June. The company determined materiality on 27 June and filed on 2 July. The actor's message is not the initial-access date.
ESTABLISHED SCOPE	The affected material included a stored insurance-billing password file and patient information. The company said the affected systems did not hold Social Security numbers, individual financial accounts or payment-card information.
ALTERNATIVES AND LIMITS	A contractor relationship does not establish that every contractor or application was affected. Credential-file exposure also needs a separate assessment of current validity and connected services.
RESPONSE	Review contractor sessions and the connected applications they can reach. Rotate corroborated exposed secrets, assess associated sessions and permissions, and validate external portal access with the responsible owners.

Bottom line

A session investigation must include connected services and exposed stored credentials.

Q

CASE Q

Hosted applications and a separate extortion demand

Healthcare services

Company-confirmed data removal; demand separately dated

DISCLOSURE	A medical-monitoring company identified unauthorised activity in hosted business applications on 8 June. It received an extortion demand the next day and confirmed that some data had been removed. [S24]
CHRONOLOGY	Materiality was determined on 10 June and the filing followed on 15 June. The demand, detection and filing are distinct events.

ESTABLISHED SCOPE	The company attributed the access to social engineering. Its stated assessment did not identify impact to products, medical-device systems, patient safety, manufacturing, distribution or financial reporting at filing.
ALTERNATIVES AND LIMITS	An actor's demand can describe more information than the company has confirmed. The operational exclusions do not mean no confidentiality harm occurred, and they do not establish current status at every related service.
RESPONSE	Map hosted business data independently from clinical-device operations. Preserve the demand as a claim, establish the confirmed export scope and assign privacy, identity and service decisions separately.

Bottom line

The extortion narrative and the organisation's confirmed scope need separate evidence.

R

CASE R

A clinical supplier's older incident and later confirmation

Healthcare services

2026 follow-up to an incident disclosed in 2025

DISCLOSURE	A clinical-care company's May filing follows an earlier voluntary disclosure from November 2025 about a software-service provider. A 20 May update supplied new information about unauthorised access affecting patient-related systems. [S25]
CHRONOLOGY	The May 2026 confirmation changes what was known about the earlier incident. It does not establish a new intrusion beginning in May.
ESTABLISHED SCOPE	The company reported continuing operations in material respects and an ongoing affected-data assessment. The source does not provide a final patient population.
ALTERNATIVES AND LIMITS	A delayed data review can change notification duties after service restoration. Counting each later notice as another attack would confuse disclosure milestones with independent incidents.
RESPONSE	Keep a supplier incident open for data-scope follow-up after availability is restored. Track changed findings, affected-person decisions and outstanding evidence requests with a privacy owner and review date.

Bottom line

An older incident can create new response work without becoming a new attack.

CASE S

S

Encryption, data removal and manufacturing restoration

Healthcare and manufacturing

Company filing confirms encryption and data removal

DISCLOSURE	A pharmaceutical-supply manufacturer reported initial detection on 4 May. Its amendment says an unauthorised party removed data and encrypted certain systems. [S26]
CHRONOLOGY	The company determined materiality on 7 May. The 20 May amendment reported restored enterprise systems and restarted manufacturing, receiving and shipping processes at all sites.
ESTABLISHED SCOPE	This original account supports both information loss and operational disruption. The stated restoration does not independently establish that the affected-data assessment was complete.
ALTERNATIVES AND LIMITS	An extortion label alone would not establish encryption; this company's own filing does. The report does not infer that the same mechanism applies to other manufacturer disclosures or listings.
RESPONSE	Exercise recovery of applications, production scheduling and receiving together. Validate protected backups, separate restoration access and data integrity, while maintaining an independent privacy and disclosure workstream.

Bottom line

Confirmed encryption and confirmed data removal require complementary recovery and privacy decisions.

CASE T

T

Patient records in a laboratory ordering application

Healthcare services

Item 8.01 notice; scope under investigation

DISCLOSURE	A diagnostic-services company learned on 21 October of unauthorised access to an application used by certain clients for test ordering and results. Its filing says it believed some patient records were accessed. [S29]
CHRONOLOGY	The notice was filed on 22 October under Item 8.01. It is not an Item 1.05 material-incident filing, and the discovery date does not establish when access began.

ESTABLISHED SCOPE	The company reported that business operations and its ability to serve patients had not been materially disrupted. The full access scope remained under investigation in the opened filing.
ALTERNATIVES AND LIMITS	A statement about operational materiality does not settle the confidentiality of patient records. The source does not establish the final affected-person count or data removal merely from access.
RESPONSE	Inventory the practices and interfaces using the affected application. Establish clinical fallback, preserve access evidence and assess patient notification against the confirmed fields and population.

Bottom line

Operational materiality and patient-data exposure answer different questions.

5.5 Education and customer-facing suppliers

U

CASE U

Instructure's education-platform incident and later review

Education suppliers

Provider and federal agency confirmation

DISCLOSURE	Federal Student Aid's May alert confirms unauthorised access involving learning-platform usernames, email addresses, course names, enrolment information and messages. It attributes the incident to the provider's stated account. [S8]
CHRONOLOGY	The agency notice was published on 12 May and updated on 29 May. Instructure's 29 September update says its forensic data review was complete, with remaining institutions to receive their data [S9].
ESTABLISHED SCOPE	The agency distinguished the stated fields from passwords, dates of birth, government identifiers and financial information, for which the provider reported no evidence of exposure. Institutions still needed their own scope assessment.
ALTERNATIVES AND LIMITS	Messages can contain sensitive content beyond a structured field list. Actor claims about institution totals remain claims. A provider event is not an independently verified intrusion into every school's own systems.

RESPONSE	Confirm institution-specific information with the provider. Review integration and recovery permissions, maintain an education-continuity mode and prepare student communications that preserve the established field and date limits.

Bottom line

Institution-specific evidence matters more than an actor's advertised school count.

CASE V

V Optimizely's website-script incident and downstream response

Technology and consumer websites

Provider-confirmed incident; downstream boundaries stated

DISCLOSURE	Optimizely says an unauthorised party exploited a Web Experimentation signup-flow flaw on 16 November and inserted malicious JavaScript into some customer projects. Its summary distinguishes the flaw from stolen customer passwords. [S10]
CHRONOLOGY	The provider reports removal of injected code that day. The public summary carries 18 November corrections and a 20 November shortening. Its guidance should be read in that updated form.
ESTABLISHED SCOPE	The provider limits the affected product to Web Experimentation. Salesforce's own response says it disabled scripts and had no evidence of impact to its platform or subscription services [S11].
ALTERNATIVES AND LIMITS	A malicious script loaded by a visitor is not evidence of access to every customer's internal network. Provider-level remediation does not replace each customer's investigation of its affected pages and visitors.
RESPONSE	Identify affected snippets, pages and exposure periods. Preserve browser, web and payment evidence where relevant, and assess customer impact before re-enabling an integration through the authorised change process.

Bottom line

Trusted third-party browser code needs an inventory, an emergency control and an impact review.

5.6 Public services and public workflows

W

CASE W

A court-service provider's interruption and restoration

Public services

Official service notice and dated restoration update

DISCLOSURE	A judicial authority's October notice says a cybersecurity incident at a provider interrupted a court-notification service. The account identifies unavailable service access and halted production and distribution of notices. [S30]
CHRONOLOGY	The original publication is dated 15 October. A 27 October update says the service was back online. The restoration update is not a second incident.
ESTABLISHED SCOPE	The source establishes a supplier-related service interruption and a subsequent restoration statement. It does not establish access to every court system or the theft of every document involved in a case.
ALTERNATIVES AND LIMITS	A service can return while delayed work still requires reconciliation. The report does not infer a particular actor, ransomware family or affected-person total from the interruption.
RESPONSE	Test alternative notification and deadline-management procedures with the business and legal owners. After restoration, reconcile queued work and document which communications were delivered, delayed or require repetition.

Bottom line

A restored supplier service still needs business reconciliation and accountable sign-off.

X

CASE X

An insurance quotation tool's pre-fill information

Insurance

Submitted organisation notice; access period crosses years

DISCLOSURE	An insurance-services provider's 30 October notice describes suspected abuse of an online quotation tool. Unauthorised users submitted information and may have viewed personal data returned through pre-fill functionality. [S31]

CHRONOLOGY	The notice dates discovery to 3 August 2026 and remediation to 11 August. The described potential-access period begins on 30 January 2025, so the whole event cannot be assigned to 2026.
ESTABLISHED SCOPE	The notice concerns names and driver's licence numbers and says people could be affected without an existing relationship with the provider. It does not establish every applicant or visitor as affected.
ALTERNATIVES AND LIMITS	A convenience feature can disclose information without an internal-network intrusion. A person who never became a customer can still need a notification decision; contractual customer counts are not the relevant denominator.
RESPONSE	Review what public workflows return before identity and authority are established. Test data minimisation, abuse monitoring and notification assessment for applicants and non-customers as well as existing policyholders.

Bottom line

Public workflow responses deserve a privacy review alongside account and network controls.

Y

CASE Y

A school-system notice with a limited network boundary

Education

Submitted original notice; student-store boundary retained

DISCLOSURE	A school system's 6 November notice says unusual activity was identified on 25 September. The investigation found access to files in a small network subsection separate from where student data was stored. [S32]
CHRONOLOGY	The source dates the file access to 25 September and completion of data review to 20 October. The November letter is the notification milestone.
ESTABLISHED SCOPE	The notification identifies names and Social Security numbers among the relevant information. The source's network boundary must remain part of the incident account.
ALTERNATIVES AND LIMITS	An education-sector incident is not automatically a student-record incident. The notice does not establish institution-wide ransomware, the actor's identity or every school's data scope.
RESPONSE	Map staff, student and administrative data separately. Confirm the files and people relevant to the notice, preserve the access record and prepare verification guidance for affected employees or other recipients.

Bottom line

Preserve the affected segment and data-owner boundary in every communication.

5.7 Additional original disclosures across the window

These nine families extend the sector account. Related notices and amendments remain one family each. Disclosure and directory dates do not establish when the underlying intrusions began.

Investment-management cloud files

An investment-management company's notice describes social engineering and access to a limited set of cloud-application files during 29–31 July. Some files held client personal information. The notice expressly excludes client-account access and reports no evidence of recordkeeping or money-movement system access [S84].

Its state-directory reporting date is 11 November. The submitted template leaves the individual data elements and some dates unspecified. Those blanks cannot support a national person count or a claim of trading-account intrusion. The response is to validate affected file permissions, sessions and the information identified for each notice.

Mobility-service information at a provider

A mobility-services company's 10 November notice says a provider alerted it on 9 October after provider credentials were used to access its account. The company severed data connections. On 13 October it determined that personal information had been accessed; no misuse had been identified at the notice date [S85].

The template leaves the specific information category blank. The notice does not establish a company-wide intrusion, a named provider relationship or a link to the other supplier cases. The provider owner should test connection revocation and establish what data remained accessible through the affected account.

Employee accounts at a medical-device company

A medical-device company's submitted notice attributes employee-account access to social engineering and says certain files could be downloaded. On 2 November the company determined that information may have been involved. Its state-directory report date is 13 November; the initial access date is unspecified [S86].

Possible data categories include names, Social Security numbers, birth dates and government-identification information. That list does not mean every category concerned every person. The company revoked access and reported no ongoing unauthorised activity or indication of misuse. The notice does not establish disruption to medical products or patient care.

A medical-components manufacturer's February event

A medical-components manufacturer detected an IT incident around 14 February. Its 24 February signed filing describes effects on billing and delivery-label functions while operations continued in all material respects. It also confirms that files were removed, with the sensitive-data scope still under investigation at that point [S87].

A 5 November notice gives an 11–14 February access period and 28 September review completion. It is an update to the February family, before the recent window. Additional individual data fields remain unspecified. Continuity assurance and the eventual notification scope therefore require separate evidence; neither can be inferred from a restored business function.

A dental-services company's later acquisition finding

A dental-services company detected an incident on 28 August. Its initial filing, signed 1 September, described possible patient-data access without material operational disruption. The later filing, signed 13 October, establishes unauthorised acquisition and says affected patients' protected health information was identified and notifications were being completed [S88].

The later document's 7 October cover date is not its signature date. Its litigation descriptions remain allegations, and no known unauthorised use or damages were reported at that point. Privacy owners should use the later acquisition finding while retaining the company's stated limits on misuse and financial impact.

A legal-information provider's legacy servers

Direct reporting on 3 March carries a US-based legal-information provider's confirmation that an unauthorised party accessed a limited number of servers. The company described mostly pre-2020 business and contact information, including survey and support-ticket material [S101][S102].

The company excluded sensitive identifiers, financial information, active passwords, customer search queries, client or matter information and contracts. It said it had no evidence of compromise of, or impact to, products and services. A report updated on 10 March adds company information [S102][S103].

Those statements do not authenticate every advertised file or establish that each field on the servers was extracted. The actual access date, technical entry route and actor's volume assertions remain unconfirmed. The provider has a global business; no US-only affected population or server count is established.

This is one additional provider-disclosure family, separate from the legal-adviser case above and an older incident in another business division. Data owners should validate legacy-server retention and access, preserve investigation evidence and assess the information actually involved. Older contact records can still require a privacy or impersonation-risk decision.

November marketing-data notice at a bank

Company statements reported on 19 November say suppliers to a bank were targeted by a cyberattack. The bank believed attackers accessed marketing information that might include customer names and email addresses. It did not identify the suppliers or give an access date [S107][S108].

The bank said its services were not disrupted and separated this disclosure from a service fault earlier that week. The contact-data assessment remains a privacy and fraud issue even when payment functions remain available. The statement does not establish intrusion into the bank's own network [S108].

Supplier and customer-protection owners should confirm the affected information and notification route. Review requests that use genuine contact details, preserve the source's provisional language and obtain current supplier evidence. No actor identity or advertised archive volume is adopted here.

November benefit-program email exposure

A separate payment-services company said a supplier incident exposed limited email-address information concerning a small subset of people enrolled in a benefit programme. Its 19 November response excluded payment information and impact to its payment network or card use [S107][S108].

That company said the exposure had been contained and it was working with the provider. This is a dated company assessment, rather than independent proof that every copy disappeared. No affected-person total or supplier identity was supplied in the statements used here.

Another payment provider described an Asia-Pacific supplier incident while excluding its own systems and payment-card data. Its response did not affirm the customer-exposure population alleged by an actor. That narrower response is context, rather than another counted access or exposure family [S107].

The two organisation disclosures do not establish either one shared supplier intrusion or two technically independent attacks. Owners should reconcile provider relationships and actual data fields before combining affected populations. Continue customer verification and factual notification without treating a company logo on a leak site as proof of network compromise.

Federal applications and a dated recovery expectation

An official's on-record remarks reported by DTN on 20 November describe a cyberthreat affecting USDA systems. The same official said no personally identifiable information was involved and no data was lost. Those statements remain the official's dated account [S109].

Nextgov's 19 November report describes an internal 16 November email linking security-response work to application outages. Reported effects concerned loan, payment and administrative functions. The report does not establish the initial access date, actor or data extraction [S110][S111].

The official expected most systems to return by the end of 20 November, with further work over the weekend if needed. That was a recovery expectation. It does not demonstrate completed restoration or verified production readiness by the report's cut-off [S109].

Continuity owners should validate a usable transaction, reconcile queued work and confirm the current service position. Keep this incident separate from maintenance-related statements elsewhere. Similar timing does not establish a shared actor or cause.

5.8 What these sector examples change

The case set supports several different owner reviews. It does not support one assumed initial-access route.

Service boundary	Observed public account	First owner decision
Manufacturing and fulfilment	Disruption can affect ordering, production and shipping	Define the usable fallback and restart evidence
Clinical business applications	Information loss can coexist with stated device-safety exclusions	Separate patient-data and service-continuity assessments
Supplier integrations	An application's permissions can define the disclosed subset	Remove unnecessary access and preserve export records
Professional services	Sensitive client records can be held outside production systems	Include advisers in data and notification maps

Service boundary	Observed public account	First owner decision
Education platforms	Provider and institution responsibilities can differ	Obtain institution-specific data and test continuity
Public workflows	Information can be returned before a customer relationship exists	Review authorisation, minimisation and non-customer notices
Internal information handling	A material disclosure need not involve an external intruder	Provide an approved workflow and an escalation route

These are planning implications from the selected cases. They do not assert that every organisation in the sector uses the same systems or has failed to implement the recommended control.

5.9 Recent activity: 8–22 November

The closing-period picture combines publications, original updates and new source records. Dates below do not silently become intrusion dates. The section uses held posts and public notices dated within the recent window, subject to their recorded verification dates.

Date	Material in scope	Evidence boundary	Immediate owner
8–22 November	357 US-labelled extortion publications [S3]	Claim records, not 357 confirmed intrusions	Threat intelligence and response
10 November	Mobility-service provider notice [S85]	October alert and data-access determination; specific data fields unspecified	Supplier and privacy owners
11 November	Investment-management notice reported to state directory [S84]	July cloud-file access; client accounts excluded	Cloud identity and customer teams
12 November	Gootloader infrastructure-disruption announcement [S61]	Enforcement action; historical victim and loss figures have wider periods	SOC and incident response
12 November	FaceStealer warning and related action [S62][S63]	Fake-meeting campaign; source-attributed state link and global historical figures	Identity, recruiting and engineering
13 November	Medical-device company notice reported to state directory [S86]	November information assessment; initial access date unspecified	Identity and privacy owners
16 November	Website-script incident at a supplier [S10]	Customer-project and visitor-browser exposure, not every customer network	Web application and supplier owners
17–18 November	Federal and state Java patching alerts [S45][S46]	Urgent vulnerability guidance, not a measured US exploitation count	Vulnerability and platform owners

Date	Material in scope	Evidence boundary	Immediate owner
17 November	Official NSA statement on maintenance-related degradation [S65]	No confirmed cyberattack asserted by that statement	Service continuity and communications
18–20 November	Supplier and downstream website-script updates [S10] [S11]	Corrections and investigation updates, not separate incidents	Supplier and customer-impact owners
19 November	Bank and benefit-program supplier statements [S107] [S108]	Two organisation disclosures; access dates and common supplier unresolved	Privacy, fraud and supplier owners
19–20 November	Federal application incident reporting and official cyber-threat acknowledgement [S109][S110][S111]	Reported service effects and a restoration expectation; actor and completed recovery unresolved	Service continuity and incident command
22 November	Marketplace-account buyer request [S1]	Observed demand, not supply, valid access or provider intrusion	Fraud and account protection

The 5 November cold-chain warning precedes the recent window. It remains useful preparation context but is not counted as a closing-period publication [S60].

A late law-enforcement information-service story remains outside the confirmed subset. Original official confirmation was not established in the source review. The report neither names its alleged victim nor converts the story into a confirmed national-system incident.

A separate service-fault report is not joined to any information-access disclosure without evidence. Concurrent customer complaints do not establish a common intrusion or a shared supplier incident.

5.10 Follow-up after the headline

A public statement can change as investigators review data and restore services. Track the original notice, each material update and the proposition that changed. A later field list, an access finding or a recovery milestone can justify different work without implying a new intrusion.

The company's assessment should also remain dated. A September statement about recovery does not certify November status. A source's future financial expectation is not adopted here as a final outcome. Service owners should obtain current evidence relevant to their own dependency.

KEY TAKEAWAYS

01

The twenty-nine reporting families preserve different event, detection and disclosure dates.

02

Supplier, internal-handling and core-system incidents require different owner decisions.

03

Recent publication and restored availability do not resolve every affected-data question.

CHAPTER 06

Hacktivism, DDoS and operational disruption

06

THIS CHAPTER ANSWERS

How should defenders separate political claims, availability loss and physical-process consequences?

4

propositions requiring separate evidence

6.1 Claims need an independent service measure 63
6.2 Timeline of official operational-system material 64
6.3 Case Z: water-system technology and actual service effects 65
6.4 Claim versus established reporting 65
6.5 Different operational technologies require different questions 66
6.6 DDoS readiness and operational fallback 67
6.7 Neutral handling of political rhetoric 67

CHAPTER 06

Hacktivism, DDoS and operational disruption

IN SHORT

An actor's announcement, an unavailable website, access to operational technology and a physical consequence are different propositions. Official water-system reporting establishes real technology impact while preserving uncertainty about attribution and individual service effects. Other advisories distinguish observed modifications from reconnaissance and possible future harm. Prepare availability mitigation and operational fallback, involve process owners, and communicate only the impact your own evidence supports.

6.1 Claims need an independent service measure

A DDoS announcement can establish that a persona made a claim. It does not independently establish which user function failed, for how long or why. An unavailable homepage can also reflect maintenance, a software fault or another unrelated operational problem.

A useful service measure follows the user transaction. For a public body, that may be submitting a form. For a financial service, it may be completing a payment. For a utility, it may be maintaining safe operation while a management connection is unavailable.

Keep the evidence for the actor's claim and the service's actual condition separate. Matching dates are a reason to investigate, not proof that the claimant caused the outage. Attribution can remain unresolved while the service owner activates agreed mitigation.

The retained underground evidence is bounded by the population described in Chapter 4. No national DDoS total or success rate is inferred from its advertisements or politically framed messages [S1].

An unverified network-device disruption claim (B20)

Evidence card B20 30 Apr 2026

Anonymous poster Forum Forum English

ORIGINAL

i was able to hit them off [...] directly tied to [a government agency]

TRANSLATION

Source English; device, domain, agency and persona identifiers omitted.

Held
A forum poster says they disrupted two purported routers and associates them with a US government agency. The supplied material consists of copied scan/HTTP response text, not independently verified outage evidence.

Not established
Agency ownership, an independently observed attack or outage, outage duration, provider compromise or public-service impact.

A 30 April forum poster claims to have disrupted two purported US-hosted network devices and associates them with a government agency. The supplied scan and HTTP response text establishes what the poster supplied, rather than independently observed ownership or an outage [S1].

A redirect to an agency website does not establish agency ownership. Copied successful-response text does not establish an attack, its timing, outage duration or a public-service effect. Provider labels also do not establish compromise of the provider's own infrastructure.

Possible alternatives include a configured redirect, unrelated or test devices, copied older material, or an unsupported association. Network owners should compare existing asset records and independent availability telemetry before declaring a compromise or service interruption.

6.2 Timeline of official operational-system material

The timeline records notice dates. It does not turn each warning into a new incident or link every event to one operator.

3 Jun 2026	**NSA and partners** Publish automatic tank-gauge guidance describing unattributed malicious changes [S58]
22 Jul 2026	**CISA and partners** Update a source-attributed PLC campaign advisory and defensive guidance [S72]
30 Jul 2026	**Minnesota IT Services** Distinguish confirmed technology impact from water-service disruption and preserve attribution uncertainty [S6]
30 Jul 2026	**FBI and EPA**

Describe reports from at least seven states and some operational effects [S7]

19 Aug 2026	**NSA and partners** Describe PLC reconnaissance and capability development, with physical effects remaining conditional [S59]
5 Nov 2026	**Federal coauthors** Warn about refrigeration and cold-chain controller targeting [S60]
17 Nov 2026	**NSA** Attributes temporary degradation of some internal systems to routine maintenance [S65]

6.3 Case Z: water-system technology and actual service effects

- **Disclosure.** Minnesota's 30 July statement reports malicious activity involving technology at more than 30 community water systems. It distinguishes confirmed technology impact from a water-service interruption at every community. [S6]
- **Chronology.** The state was responding to July activity. A separate FBI and EPA warning describes reports from at least seven states and some operational effects [S7]. These sources do not establish one common actor across every incident.
- **Established scope.** The state says most confirmed cases involved remote monitoring or control technology. It had not attributed the activity to a particular actor and reported no active statewide request to change drinking-water use at that time.
- **Alternatives and limits.** Similar timing or equipment does not establish common control. A national warning can describe effects elsewhere without proving the same effect at every Minnesota system, and no contamination conclusion follows.
- **Response.** Validate intended external connections with operational owners. Test safe manual operation, protected remote access, equipment configuration and recovery, then communicate the service and public-health facts established by each utility.

A national warning and a local utility account can have different denominators. Do not assign every effect described by a national notice to every local system. Likewise, a state's unresolved attribution should not be replaced by an analyst's inference from another advisory.

6.4 Claim versus established reporting

The first row compares an actual retained assertion with its evidence limits. The other rows are analytical examples, rather than quotations attributed to a particular actor. The source column preserves what each account establishes.

Point	Claim or broad implication	Official account	Defender interpretation
Two devices are linked to an agency and successfully disrupted	A forum poster makes both assertions	No official corroboration is established; supplied redirects and response text do not prove ownership or outage [S1]	Reconcile asset ownership and independent availability evidence; keep the claim unverified
An outage is a cyberattack	A claimant or observer may associate an interruption with hostile activity	NSA's 17 November statement attributes temporary internal degradation to routine maintenance [S65]	Measure the service fault and preserve the stated cause; a confirmed attack is not established
Every affected utility lost water service	A technology-impact total can be read as a service-outage total	Minnesota expressly separates these propositions [S6]	Check the individual utility's operating and public-health evidence
Similar equipment establishes one actor	Related timing and devices may suggest a common campaign	Minnesota says a common actor across every incident was not established [S6]	Keep relationship and attribution questions open
Capability development establishes physical damage	Scripts or reconnaissance can suggest future capability	NSA's August notice describes reconnaissance and capability development [S59]	Validate exposed equipment and preparations without inventing a realised consequence
A cold-chain warning is a recent US incident total	Global targeting can be read as confirmed local losses	The 5 November advisory describes targeting and potential effects [S60]	Review relevant controllers; do not calculate US inventory loss from the warning

Do not divide an actor's claimed targets by an authority's affected-system count to calculate a success rate. The units and coverage can differ. A claim, a site, a utility, an attempted connection and a confirmed incident are not interchangeable observations.

USDA's separate November account illustrates the importance of dates. An official acknowledged a cyberthreat and gave a restoration expectation on 20 November. That does not establish completed recovery, nor does it link the incident to another agency's maintenance-related degradation [S109][S110].

6.5 Different operational technologies require different questions

The June tank-gauge guidance describes malicious modification of internet-exposed systems. It does not give a national victim total or identify a state actor. Its source wording should remain separate from the July source-attributed PLC campaign [S58][S72].

The August PLC publication describes reconnaissance and capability development against US installations. Potential physical consequences remain conditional. The report does not convert the presence of scripts, monitoring pretexts or an exposed interface into evidence that a process was damaged [S59].

The cold-chain warning addresses temperature and refrigeration controllers across a global setting. It is relevant to food, healthcare and other temperature-sensitive services. The defensible action is to identify intended connections and safe operation, rather than announce a quantified US loss unsupported by the source [S60].

For each relevant system, identify who approves remote access, what the operator sees when connectivity fails and which settings must be restored. A network diagram without a process owner cannot settle the safety decision.

6.6 DDoS readiness and operational fallback

Decision	Accountable owner	Evidence to prepare
Which user function must remain available?	Business service owner	Essential transaction and acceptable degraded mode
Who can activate network-provider mitigation?	Network operations	Current contact, authority and activation test
How will administrators retain protected access?	Infrastructure and identity	Tested management route and recovery credentials
Which external operational connections are intended?	Process and maintenance owners	Approved connectivity and supplier-access map
What can continue manually and safely?	Operations and safety	Demonstrated procedure, staffing and operating limits
How will customers receive factual updates?	Communications and incident command	Independent status route and approval process

Test the fallback under realistic constraints. The normal messaging system, remote-maintenance provider or identity service may also be unavailable. A procedure that relies on the failed dependency is not a usable continuity mode.

After recovery, reconcile both data and work. Orders, alarms, notices and operational records can accumulate during an interruption. Business owners should verify what was delayed, repeated or omitted before closing the service issue.

6.7 Neutral handling of political rhetoric

The report records politically framed activity only for its security relevance. It omits slurs, intimidation and recruitment appeals. An actor's stated motive does not establish that a particular government decision caused the activity or that a state controlled the claimant.

A federal attribution remains the issuing authority's assessment. It is not extended to unattributed local cases merely because the equipment or timing appears similar. The same readiness controls should apply regardless of a victim's political affiliation or the issue invoked by a claimant.

KEY TAKEAWAYS

01

A claim, outage, operational-system change and physical consequence need separate evidence.

02

Official water reporting preserves local impact and attribution limits.

03

Test provider mitigation and safe fallback with service and process owners.

CHAPTER 07

Threat actors, listing labels and supported relationships

THIS CHAPTER ANSWERS

Which actor assessments have evidence, and which relationships remain unresolved?

149

labels associated with publication-dated US extortion records

7.1 A relationship map with typed evidence 70
7.2 Ransomware and extortion in regional context 72
7.3 Group labels are useful leads, rather than incident verdicts 73
7.4 Identity-focused campaigns with different trust decisions 77
7.5 Router interception and supported attribution 77
7.6 Covert infrastructure and separate state-attributed campaigns 78
7.7 A technique matrix from an official ransomware advisory 79
7.8 Verified vulnerability examples 80
7.9 Recent deception and infrastructure disruption 81
7.10 Earlier enforcement and recovery announcements 82
7.11 Criminal personas and source-attributed state links 82
Campaign follow-ups: botnets and forum infrastructure 83
Perimeter-device persistence: patching and eviction are different 83

CHAPTER 07

Threat actors, listing labels and supported relationships

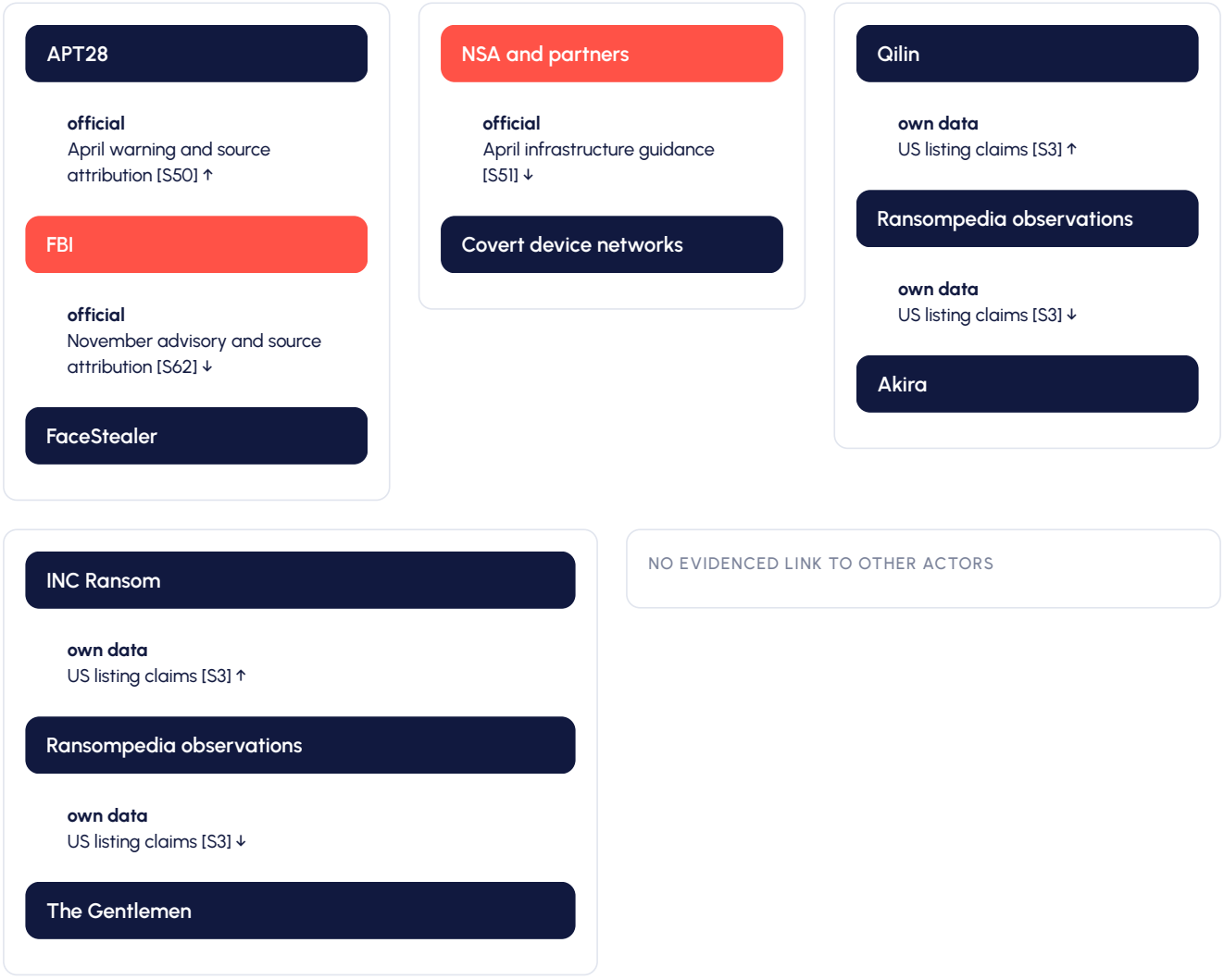
IN SHORT

Listing labels, official campaign attributions and observed advertisements answer different questions. Ransompedia records claims under many labels. Federal advisories describe identity deception, edge-device abuse and operational-system activity, with geography and attribution stated by their authors. Shared timing or a defensive control does not link those populations. Use each supported campaign description to choose a relevant validation task, while keeping the response useful when attribution changes.

7.1 A relationship map with typed evidence

The map shows the main source-supported relationships; the table adds two further evidence links. It does not show a coalition, a single operating organisation or a common incident joining all the groups.

Own post Relay Official statement Public reporting Our observation



Connection	Evidence type	What it establishes	What it does not establish
Ransompedia to extortion labels	Own data [S3]	Recorded publication-dated claims under those labels	Successful intrusion, shared affiliates or completed payment
FBI and partners to router activity	Official statement [S50]	The source's APT28 attribution and described behaviour	A new 2026 incident at every US router owner
NSA and partners to covert device networks	Official statement [S51]	The issuing authorities' assessment of infrastructure use	Malicious intent for every user or one operator across all networks
FBI to FaceStealer	Official statement [S62]	The source-attributed campaign and deceptive meeting pattern	A US-only loss total or common membership across every alias
DOJ to the Handala persona's websites	Official statement [S55]	Domain seizures and the authority's stated attribution	Independent authentication of every persona claim
Public disclosures to response decisions	Original reporting [S8][S10] [S12][S14]	Stated service and information boundaries	A common criminal operator across those cases

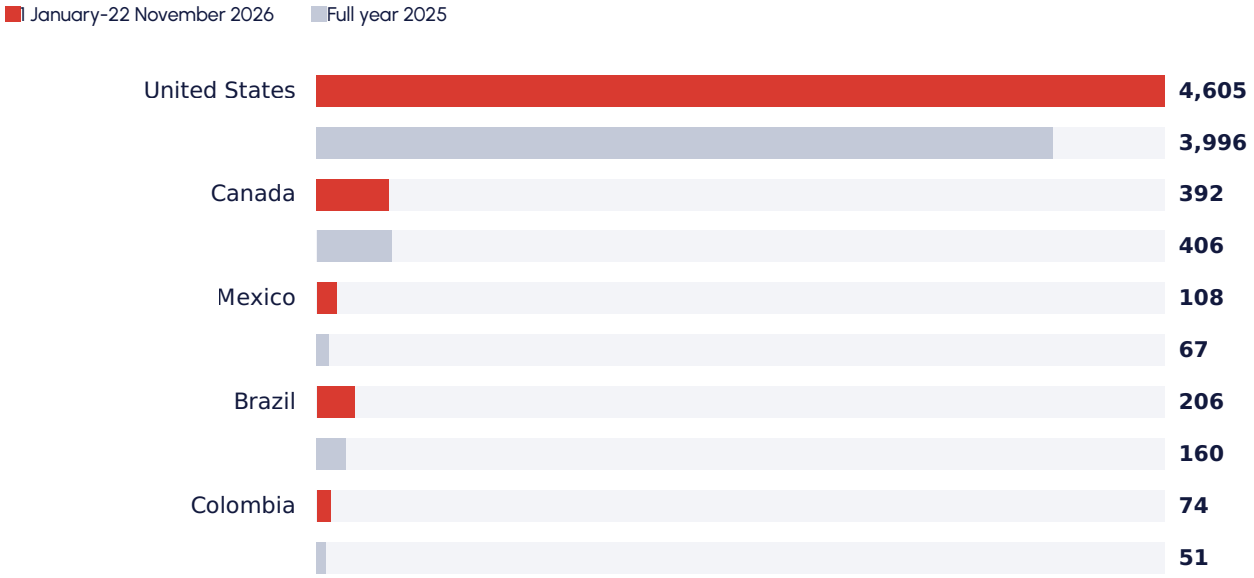
No own-data edge links the listing population to the state-attributed campaigns. A shared tool, language, victim sector or publication day is insufficient to establish that relationship.

7.2 Ransomware and extortion in regional context

The four peers provide Americas context. Canada and Mexico share North American business dependencies with the United States. Brazil and Colombia add regional industrial, financial and digital-service contexts. They are not matched national populations or equal-coverage controls [S3].

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

Listing counts describe five different country-labelled populations



Unmatched periods and country populations; not a national risk ranking. Source: Brandefense Ransompedia, 1 January-22 November 2026; November partial. Publication-dated country-labelled claims, not confirmed intrusions or distinct victims [S3].

Country	2026 window	Full-year 2025	Interpretation
United States	4,605	3,996	Publication-dated source records
Canada	392	406	Country label in the same source
Mexico	108	67	Country label in the same source
Brazil	206	160	Country label in the same source
Colombia	74	51	Country label in the same source

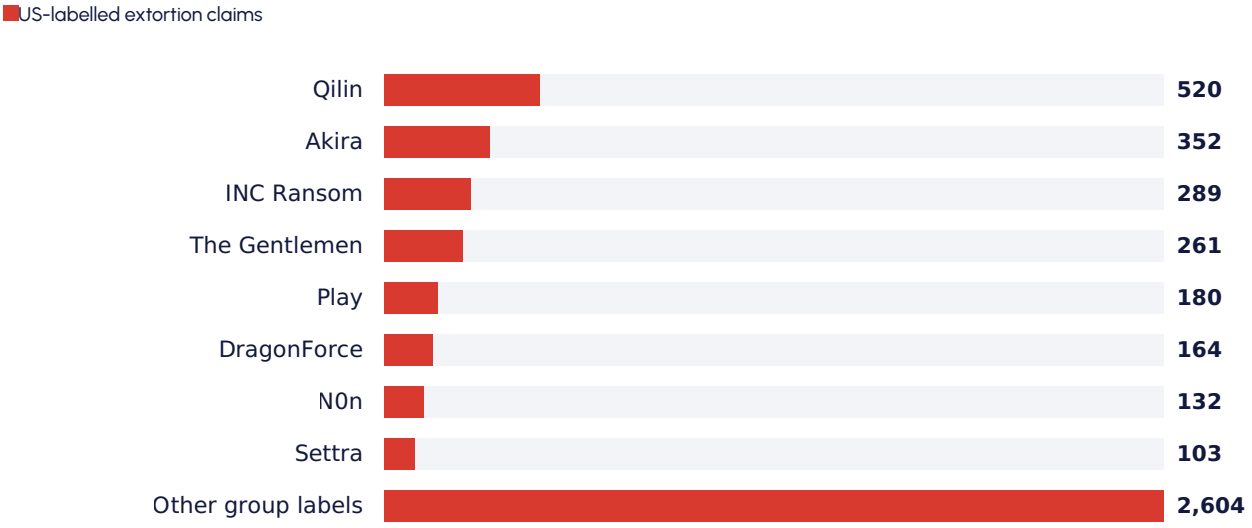
The 2026 window is partial, while 2025 is a complete year. The table does not provide matched-period growth rates or population-adjusted risk. Country size, business composition and source visibility differ. A multinational listing also requires care about which operating entity is relevant.

The US population contains 4,605 publication-dated records under 149 group labels. The recent window contains 357 publication-dated records [S3].

7.3 Group labels are useful leads, rather than incident verdicts

The leading five labels account for 1,602 records, or 34.8%. Other labels account for 3,003, or 65.2% [S3].

The leading five labels account for 34.8% of publication-dated US listings



Source: Brandefense Ransompedia, 1 January–22 November 2026; November partial. Publication-dated country-labelled claims, not confirmed intrusions or distinct victims [S3].

Group label	Listings	Share	Decision implication
Qilin	520	11.3%	Include extortion and recovery in exercises without assuming an entry route
Akira	352	7.6%	Validate a matching claim against the relevant service and accounts
INC Ransom	289	6.3%	Preserve the difference between listing and confirmed incident
The Gentlemen	261	5.7%	Do not infer a shared operator from a criminal label

Group label	Listings	Share	Decision implication
Play	180	3.9%	Maintain a recovery plan that remains useful if attribution changes
Other labels	3,003	65.2%	Prepare for a broad claim population

Qilin

Extortion listing label | No state attribution made in this report

IN THE UNITED STATES, 2026

1 January–22 November

520 publication-dated US listing claims in the snapshot

CLAIMED TARGETS

US-relevant organisations as labelled in the source; identities withheld

SEEN IN PUBLIC REPORTING

[S3] 520 retained listing claims; outcomes and operator identities remain unverified

OUR ASSESSMENT

Investigate a credible match and prepare proportionate continuity action. The label does not establish successful encryption, an initial-access route or a single independent operating team.

CONFIDENCE

High for the retained count; incident outcomes unverified

Akira

Extortion listing label | No state attribution made in this report

IN THE UNITED STATES, 2026

1 January–22 November

352 publication-dated US listing claims in the snapshot

CLAIMED TARGETS

US-relevant organisations as labelled in the source; identities withheld

SEEN IN PUBLIC REPORTING

[S3] 352 retained listing claims; outcomes and operator identities remain unverified

OUR ASSESSMENT

Investigate a credible match and prepare proportionate continuity action. The label does not establish successful encryption, an initial-access route or a single independent operating team.

CONFIDENCE

High for the retained count; incident outcomes unverified

INC Ransom

Extortion listing label | No state attribution made in this report

IN THE UNITED STATES, 2026

1 January–22 November

289 publication-dated US listing claims in the snapshot

CLAIMED TARGETS

US-relevant organisations as labelled in the source; identities withheld

SEEN IN PUBLIC REPORTING

[S3] 289 retained listing claims; outcomes and operator identities remain unverified

OUR ASSESSMENT

Investigate a credible match and prepare proportionate continuity action. The label does not establish successful encryption, an initial-access route or a single independent operating team.

CONFIDENCE

High for the retained count; incident outcomes unverified

The Gentlemen

Extortion listing label | No state attribution made in this report

IN THE UNITED STATES, 2026

1 January–22 November

261 publication-dated US listing claims in the snapshot

CLAIMED TARGETS

US-relevant organisations as labelled in the source; identities withheld

SEEN IN PUBLIC REPORTING

[S3] 261 retained listing claims; outcomes and operator identities remain unverified

OUR ASSESSMENT

Investigate a credible match and prepare proportionate continuity action. The label does not establish successful encryption, an initial-access route or a single independent operating team.

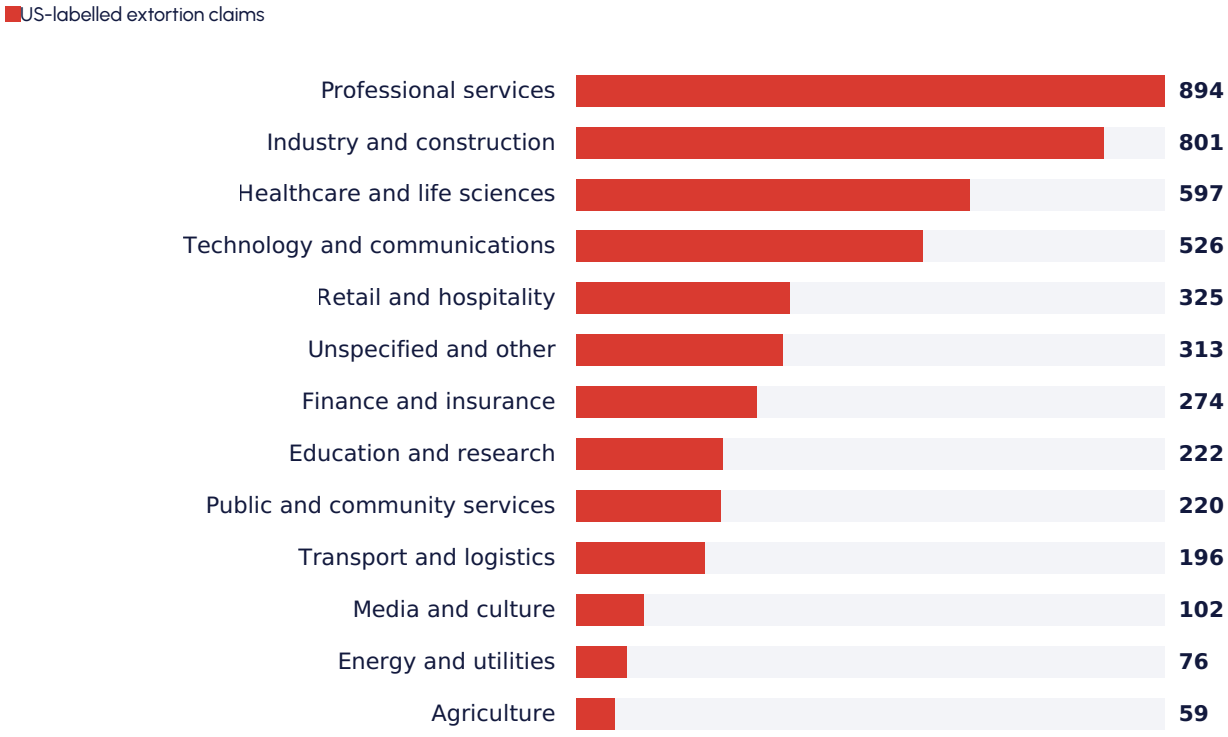
CONFIDENCE

High for the retained count; incident outcomes unverified

The listing label helps an intelligence team track a public assertion. It does not determine which account to contain or which business process to restore. Those decisions need the organisation's evidence and service map.

The source's industry labels also describe recorded claims. The public sector chart groups related labels and preserves the listing unit. It is not a distribution of independently confirmed intrusions or a national sector attack rate [S3].

Extortion claims span several broad business and public-service sectors



Source: Brandefense Ransompedia, 1 January–22 November 2026; November partial. Publication-dated country-labelled claims, not confirmed intrusions or distinct victims [S3].

7.4 Identity-focused campaigns with different trust decisions

The FBI's January QR-phishing warning describes activity attributed by the source to Kimsuky. Its examples concern 2025 activity involving foreign-policy and academic communities. The January publication is relevant context, not a count of new 2026 US victims [S47].

The FBI and CISA's March messaging warning attributes a global account-phishing campaign to Russian intelligence services. It distinguishes individual-account access from the security of the applications' encryption. Their June update adds attempts to obtain backup recovery keys [S48][S49].

A new recovery key can invalidate an older key for future backup downloads under the source's account. It cannot undo an already downloaded copy. Identity recovery should therefore assess current sessions, linked devices and relevant backup exposure, rather than equating a changed password with complete closure.

The May device-code warning describes a phishing service first observed in April. The September consent-phishing warning describes malicious application permissions that can survive a password change until the relevant permission or token is revoked. These are distinct mechanisms, not evidence that every use of MFA fails [S67][S66].

For each mechanism, the operational question is which authority the user approved. Was it a sign-in, device authorisation, application permission or recovery action? Investigate that decision and the evidence it produced. The incident label alone will not identify the remaining access path.

7.5 Router interception and supported attribution

The FBI and partners' 7 April notice attributes router DNS-hijacking activity to Russia's GRU, using APT28 and other aliases. It describes activity since at least 2024, including US and global victims, and the theft of credentials and authentication tokens [S50].

That is the source's attribution. The report's country-associated posts do not independently reproduce it. The advisory does not supply a US-only count of newly affected organisations in this report's 2026 window.

APT28

As identified in the FBI source

Source-attributed espionage campaign | Attributed by the FBI to Russian military intelligence

IN THE UNITED STATES, 2026

7 April

FBI warning describes router-related activity beginning in 2024

CLAIMED TARGETS

Credentials and traffic in the reported campaign; no US 2026 victim count supplied

SEEN IN PUBLIC REPORTING

[S50] FBI router warning and its stated attribution

OUR ASSESSMENT

Validate router support, configuration and account evidence. The source attribution is not an independent attribution by this report or a confirmed incident at a selected estate.

CONFIDENCE

High for the official publication; attribution remains the source's

The defender response joins device lifecycle and identity recovery. Infrastructure owners should validate intended DNS settings and supported equipment. Identity owners should assess relevant session and token evidence if interception is corroborated. Neither task requires publishing the addresses of affected routers.

7.6 Covert infrastructure and separate state-attributed campaigns

NSA and partners' April publication describes covert device networks used by actors the source calls China-nexus. Some infrastructure can also carry legitimate traffic. A shared network observation does not establish the intent of every connection or a single operator across the network [S51].

The August QTFY warning and October NSA/FBI advisory describe distinct source-attributed activity and infrastructure. Their historical scope extends beyond 2026. They do not provide a national incident total or establish that every industry label maps to the same operating cluster [S52][S53].

Covert device networks

Several actor sets described by NSA and partners

Source-described supporting infrastructure | China-nexus description belongs to the cited agencies

IN THE UNITED STATES, 2026

23 April

Joint guidance describes infrastructure used by multiple actor sets

CLAIMED TARGETS

Network devices used as supporting infrastructure; device ownership and ultimate victims differ

SEEN IN PUBLIC REPORTING

[S51] NSA and partner guidance; the report does not combine these actors into one operator

OUR ASSESSMENT

Review supported devices, administrative exposure and unexpected changes. A shared infrastructure category does not establish direct collaboration between the named actor sets.

CONFIDENCE

High for the guidance and its published scope; no independent state attribution

Investigate behaviour and service context before blocking shared or reassigned infrastructure. Retain the source's exact attribution proposition and date. Do not infer state control from a language label, a residential address or a criminal persona's name.

7.7 A technique matrix from an official ransomware advisory

The matrix selects technique identifiers explicitly named in the 20 October SafePay advisory. It describes the authors' reported campaign behaviour across several continents and historical periods. It is not a set of detections measured in this country corpus [S57].

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Credential Access	Lateral Movement	Collection	Exfiltration	Impact
T1110 Brute Force	T1021.001 Remote Services: Remote Desktop Protocol	T1560.001 Archive Collected Data: Archive via Utility	T1048 Exfiltration Over Alternative Protocol	T1486 Data Encrypted for Impact
	T1021.006 Remote Services: Windows Remote Management			T1490 Inhibit System Recovery

Technique identifiers and tactic labels as listed in the FBI and CISA SafePay advisory of 20 October 2026 [S57]. This is a response reference, not detections or prevalence at selected US estates. [S57]

Tactic	Technique	Defensive review
Credential Access	T1110, Brute Force	Review anomalous authentication and approved access controls
Lateral Movement	T1021.001, Remote Desktop Protocol	Validate remote logons, account authority and intended destinations
Lateral Movement	T1021.006, Windows Remote Management	Review remote administration against approved operational activity
Collection	T1560.001, Archive via Utility	Investigate unusual data preparation in its user and service context
Exfiltration	T1048, Exfiltration Over Alternative Protocol	Review unusual transfers alongside the relevant account and host evidence

Tactic	Technique	Defensive review
Impact	T1486, Data Encrypted for Impact	Test detection and restoration for important information
Impact	T1490, Inhibit System Recovery	Protect recovery access and validate backup integrity

Legitimate administration and archiving tools are not malicious solely because the advisory names them. Their use needs contextual evidence. The report supplies validation tasks, not an untested production detector or an offensive procedure.

The August Gunra notice adds a separate source-described example of backup and archive deletion affecting primary and recovery locations. It is a global warning, with activity predating 2026. The planning implication is to test the independence of recovery capability [S71].

7.8 Verified vulnerability examples

The examples below were checked against NVD and the relevant vendor guidance. They do not establish exploitation or vulnerable versions in the selected estate portfolio [S41][S43][S74].

Record	Affected scope	Remediation scope
CVE-2026-1731	BeyondTrust Remote Support 25.3.1 and earlier; Privileged Remote Access 24.3.4 and earlier [S41][S42]	Apply the relevant BT26-02 patch or supported fixed release; Remote Support 25.3.2 and later. The narrative recommends Privileged Remote Access 25.1.1 or later [S42]
CVE-2026-114938	Oracle's November matrix lists Java SE and GraalVM branches; distribution and processor conditions matter [S43][S44] [S78]	Apply the appropriate distribution update. For Ubuntu 24.04, fixed packages are OpenJDK 17 `17[.]0[.]21[.]1+2-1~24[.]04[.]1` and OpenJDK 21 `21[.]0[.]13[.]1+2-1~24[.]04[.]1` [S79]
CVE-2023-50224	Legacy TP-Link router and access-point variants; the April source associates the record with router activity [S50][S74] [S75]	Match hardware and region. TL-WR841N V11 has a US 260415 update; EU V11 and V12 have 211209 and 230317 updates. Several older variants remain partly patched [S75]

In package versions above, `[.]` denotes a literal period.

NVD records a CISA Known Exploited Vulnerabilities catalogue addition on 13 February for CVE-2026-1731 [S41]. That recorded status supports prompt vendor-scoped remediation. It does not establish exploitation at any selected estate or supply a monthly catalogue total.

The BeyondTrust advisory's table also uses a broader Privileged Remote Access 25.1 line. The more specific 25.1.1 narrative recommendation is retained here. Older self-hosted branches can require an upgrade before the patch applies. Follow the vendor's current product-specific instructions [S42].

The Java example needs more than the word Java in an inventory. Oracle's matrix lists affected Java SE builds including 17.0.21.0.3 and 21.0.13.0.3. Red Hat describes processor and code-path conditions, while Ubuntu provides distribution-specific fixed packages [S44][S78][S79].

CISA and New York DFS issued 17–18 November alerts about this Java record, including runtimes bundled in applications, containers and appliances. The notices support urgent inventory and remediation. They do not themselves establish a US exploitation count [S45][S46].

The router example likewise does not justify installing a firmware image for another hardware revision or region. A model-family label can hide materially different support and remediation options. Replace an unsupported variant when the vendor provides no applicable correction [S75].

7.9 Recent deception and infrastructure disruption

The FBI's 12 November FaceStealer warning describes fake video meetings, previously recorded victim videos and a false technical-fix pretext. The FBI attributes the activity to North Korean state-sponsored hackers. Its loss figure covers a global eighteen-month period, not US-only activity in 2026 [S62].

FaceStealer

Campaign name used in the FBI advisory

Deceptive meeting and cryptocurrency-theft campaign | North Korea attribution stated by the FBI

IN THE UNITED STATES, 2026

12 November

FBI publishes campaign warning with historical international activity

CLAIMED TARGETS

People with cryptocurrency or investment access; international historical figures are not US-window losses

SEEN IN PUBLIC REPORTING

[S62] FBI advisory; its aliases are not automatically one operating team

OUR ASSESSMENT

Use a separate trusted channel to validate unexpected meetings. Require independent approval for sensitive downloads, signing or value transfers, and examine relevant device and session evidence after a suspicious interaction.

CONFIDENCE

High for the advisory and its stated actions; no independent attribution

The response is a verification rule: an unexpected meeting does not authorise software installation or an improvised system repair. Recruiting, investment and engineering teams should use a trusted support route. If a user followed the pretext, investigate endpoint and account evidence together.

DOJ's 12 November Gootloader action concerns infrastructure disruption. Its historical computer, victim and loss totals extend back to 2018 and across countries. The announcement does not become a count of computers newly infected in the final fortnight [S61].

The March SocksEscort and September Sality actions likewise describe infrastructure interventions involving older global activity. They are useful reminders that an enforcement announcement and a victim's recovery are different milestones. Neither announcement establishes that every associated device was remediated [S69][S70].

7.10 Earlier enforcement and recovery announcements

Microsoft's 14 January account describes coordinated US and UK legal actions and international measures disrupting RedVDS. It reports approximately $40 million in US fraud losses since March 2025. That period crosses the prior year; the figure is not adopted as a 2026 national loss total [S89].

A 12 January Dutch prosecution notice reports an arrest following a May 2025 international malware-service action involving US authorities. The announcement concerns a suspect and an investigation. It supplies enforcement follow-up, rather than a new 2026 US incident count [S90].

DOJ's 26 January ATM-jackpotting release announces additional charges, rather than sentencing. Its 87 charged defendants are people, not attacks or victim organisations. Charges remain allegations. A separate 21 January sentencing notice describes physical ATM access and malware, without supplying an attack period [S91][S94].

A 22 January technical account describes recovery of attacker-held data attributed to 12 US organisations. The incident-response company had already disclosed a dozen-victim recovery in November 2025. This is historical recovery context, rather than 12 new 2026 incidents or proof that all production systems were restored [S92][S93].

These examples explain why a recent publication can change defensive understanding without adding a new incident. Keep legal action, charging, conviction, data recovery and business restoration as distinct milestones. A company's technical account is also distinct from a federal agency's confirmation.

7.11 Criminal personas and source-attributed state links

DOJ's March domain-seizure release attributes associated websites and activity to Iran's Ministry of Intelligence and Security. Its account discusses a medical-technology attack claim. The company's operational disclosure is separately sourced; the report does not authenticate every persona statement from the seizure alone [S55][S12].

The October remote-worker action describes alleged schemes whose conduct substantially predates the announcement. DOJ's state-linked description is its attribution, and charges remain allegations unless adjudicated. Employer counts from separate actions are not added as unique victims [S54].

The FBI's October virtual-asset theft attribution concerns a global exchange event. A November DOJ action reports frozen assets and authority to seize or restrain part of them. Frozen, seized, forfeited and returned funds are different quantities, and overlapping figures must not be summed [S64][S63].

Actor aliases in retained advertisements describe public personas, rather than verified individuals or contact routes. Repeated wording can support a repost assessment. It does not establish file identity, a completed sale or one human author. Keep the proposition and its evidence together [S1].

Campaign follow-ups: botnets and forum infrastructure

DOJ announced a four-botnet infrastructure disruption on 19 March. Its 21 May follow-up describes a complaint unsealed after a Canadian arrest and related seizures supporting DDoS-for-hire services. Charges remain allegations [S97][S98].

The March device figures describe worldwide cumulative activity across four botnets, with a US subset. The May KimWolf figures overlap that campaign. Devices, attack commands and service platforms cannot be added together or converted into new US victim organisations.

Contemporaneous reporting on 28 January documented federal seizure banners replacing a cybercrime forum's sites. No separate original FBI or DOJ announcement is cited. The later February relay does not date another action or establish arrests, recovered records or lasting prevention [S99][S100].

For defenders, these notices support reviewing unmanaged devices, egress anomalies and provider mitigation readiness. An enforcement announcement does not demonstrate that every affected device was cleaned or that a customer service has recovered.

Perimeter-device persistence: patching and eviction are different

CISA and the UK NCSC announced firewall-backdoor analysis and updated federal civilian guidance on 23 April. The agency bulletin describes persistence through firmware patching and ordinary device reboots. It supplies no affected-agency count or country attribution [S104].

Cisco's advisory places initial compromise before fixed releases made available in September 2025. The April publication therefore does not establish a new April intrusion. Current vendor guidance includes revisions through 19 May, rather than only the original announcement [S105].

Cisco Talos attributes the activity to the cluster it tracks as UAT-4356. That remains the vendor's attribution. The report does not infer data removal, operational disruption or a government-wide incident from an implant's capabilities [S106].

For confirmed compromise, the vendor favours reimaging and upgrading, with recovery of trusted configuration and associated secrets. Arrange evidence-preserving investigation and vendor support before disruptive changes. A patch-inventory entry alone does not demonstrate that existing access was removed [S105][S106].

KEY TAKEAWAYS

01

Listing labels and official campaign attributions describe separate evidence populations.

02

Techniques and vulnerabilities require source, period and product-specific scope.

03

Shared tools, dates or language do not establish a common operator.

CHAPTER 08

The fraud economy: identities, accounts and payment decisions

THIS CHAPTER ANSWERS

How can advertised information and misused authority affect the next customer or business transaction?

3

decisions: verify identity, validate authority and protect the transaction

8.1 An advertisement is not a measure of the economy 86
8.1a Account-service advertising in the retained evidence 87
8.2 An analytical model of follow-on harm 89
8.3 Customer knowledge is different from authority 90
8.4 Employment and supplier identity 90
8.5 Payment-card material has a narrow scope 90
8.6 Cargo and payment instructions 91
8.7 Deceptive meetings and the technical-fix pretext 91
8.8 Closure evidence for fraud-related signals 92

CHAPTER 08

The fraud economy: identities, accounts and payment decisions

IN SHORT

Underground advertisements describe products that personas claim to supply. Official warnings describe ways criminals misuse identities, application permissions, employment relationships and shipment instructions. These populations do not measure a national market or completed sales. Payment-card observations are a narrow additional view. Connect credible signals to account recovery and transaction controls, and require independent verification before changing access, payment details or delivery instructions.

8.1 An advertisement is not a measure of the economy

The retained material contains offers and assertions whose authenticity requires separate validation [S1]. A service name can describe a claimed source, an account type, a customer subset or a passing reference. It does not establish that the named provider's own systems were accessed.

A persona offering a verified account may be advertising an existing account, a proposed registration service, borrowed identity material or a fabricated product. The post alone does not establish possession, current validity, lawful ownership or a completed transaction.

The useful question is which business decision the product could influence if the claim were genuine. Contact data may support impersonation. Credentials may support attempted sign-in. Company documents may support fraudulent onboarding. These are conditional possibilities, not observed downstream outcomes for every advert.

Keep an asking price separate from transaction value. A price can concern a batch, a service period, a region or a negotiated product. It cannot establish the total value of the market, seller revenue or the victim's financial loss.

8.1a Account-service advertising in the retained evidence

Evidence card B07 — 28 Feb 2026

Account-service advertiser | Forum | Forum | English

ORIGINAL

[Paraphrase: A forum poster solicits use of a claimed aged US bank account for receiving funds associated with fake checks, wires and transfers.]

TRANSLATION

Paraphrase, not a verbatim quote; provider, contact and personal identifiers omitted.

Held
A dated advertisement or solicitation; its asserted account or recovery service.

Not established
Genuine supply, lawful authority, current account access, tested tool behaviour, completed transactions or a provider incident.

Evidence card B08 — 28 Feb 2026

Account-service advertiser | Messaging channel | Telegram | Russian and English

ORIGINAL

[Paraphrase: A bilingual Russian/English advert offers aged seller accounts associated with US identities, newly registered business accounts, withdrawal services and claimed insider screenshots.]

TRANSLATION

Paraphrase, not a verbatim quote; provider, contact and personal identifiers omitted.

Held
A dated advertisement or solicitation; its asserted account or recovery service.

Not established
Genuine supply, lawful authority, current account access, tested tool behaviour, completed transactions or a provider incident.

Evidence card B09 — 28 Feb 2026

Account-service advertiser | Messaging channel | Telegram | English

ORIGINAL

[Paraphrase: An advertiser markets an account-checking service, claims performance and authentication behaviour, and lists several subscription prices and discounts.]

TRANSLATION

Paraphrase, not a verbatim quote; provider, contact and personal identifiers omitted.

Held
A dated advertisement or solicitation; listed subscription asking prices.

Not established
Genuine supply, lawful authority, current account access, tested tool behaviour, completed transactions or a provider incident.

A February forum solicitation offers a claimed aged US account as a receiving service. A separate bilingual advertisement combines seller accounts, US-associated identities and account-recovery assertions. Neither establishes genuine supply, lawful authority, a completed transfer or an incident at a financial or marketplace provider [S1].

A checking-tool advertisement lists subscription asking prices, including $70 per day and $800 per month. The report does not adopt its performance or authentication claims. These prices do not establish sales, seller revenue or a market average [S1].

The useful response crosses several functions. Account protection can assess credible login activity, fraud teams can examine transaction behaviour, and trust teams can review recovery authority. Accurate identity details do not by themselves authorise a withdrawal or account change.

8.2 An analytical model of follow-on harm

The following sequence is an **analytical model**. It is not a demonstrated transaction chain linking the personas or incidents in this report.

Stage	Possible use	Evidence needed before escalating	First owner
Information advertised	Select a plausible person or business pretext	Credible match to owned information or a relevant service	Intelligence and data owner
Identity impersonated	Persuade staff or a customer to trust a request	Message, call or account evidence supporting the attempt	Fraud and customer operations
Authority requested	Change recovery, consent, payee or delivery details	Recorded request and independent verification result	Identity or transaction owner
Access or transaction attempted	Use granted permissions or changed instructions	Relevant sign-in, application or transaction records	SOC and business operations
Harm established	Remove information, divert funds or interrupt service	Corroborated effect and a scoped affected population	Incident command and legal

The model helps assign responsibility without inventing actor relationships. A shared advertised data category does not establish that one seller supplied another, that a buyer used the material or that a particular payment followed.

A useful case record should consequently identify both the external signal and the internal decision. The latter determines whether an alert remains an investigation lead or becomes evidence of an incident requiring containment.

8.3 Customer knowledge is different from authority

A person can know genuine customer details and still lack authority to change an account. The insurance quotation-tool notice illustrates why non-customers can also appear in an affected population. The financial-services cases show information held outside a bank's core systems [S31][S22].

Customer teams should test recovery and payment-change requests against an established verification process. Do not improvise a weaker route because a caller sounds informed or cites a real transaction. Provide staff with a safe escalation path when normal checks cannot be completed.

Warnings should tell recipients what action to take. An established contact route is more useful than an actor name. Avoid asking a customer to verify a suspicious message by replying to it or using a telephone number supplied only within that message.

A confirmed disclosure also does not mean every later scam used those records. Fraud operations should compare timing, fields and behaviour while retaining alternative explanations. The response can improve even when a precise criminal data lineage remains unresolved.

8.4 Employment and supplier identity

DOJ's October remote-worker action describes alleged use of false identities and facilitation arrangements connected by the source to North Korea. The underlying alleged conduct substantially predates the October announcement. Charges do not establish guilt, and overlapping employer populations are not added here [S54].

The defensive lesson concerns identity and access governance. Validate the person, work location and approved device arrangement through proportionate, lawful processes. Recheck changes in recovery, equipment custody or privileged access. Nationality, accent or an applicant's name is not evidence of misconduct.

Procurement should apply the same authority question to a provider. Who is entitled to request a new integration, change a payout account or collect an identity document? A known commercial relationship does not automatically validate every message appearing to come from it.

8.5 Payment-card material has a narrow scope

SCOPE OF THE CARD FIGURES

These figures cover a limited set of post-based payment-card observations [S4]. They do not represent all cards observed by Brandefense, national card theft, active cards or fraud losses.

This limited population contains 1,739 distinct US-labelled card-number observations in 175 posts, with 1,981 appearances. These observations do not authenticate active cards, cardholder residence or completed payments [S4].

A post's country or issuer label is not independently authenticated by the advertisement. A status word such as live is a poster's or service's assertion, rather than proof of an authorised successful charge. No card-related observation establishes an intrusion into the issuing institution [S4].

A payment provider should validate relevance and currency through its authorised fraud process before deciding a disruptive response. The report does not recommend cancelling every account associated with an old or unverified advertisement. Issuer and customer evidence should determine the scope.

8.6 Cargo and payment instructions

The FBI's April cargo warning describes impersonation of brokers and carriers through spoofed messages, deceptive sites and misused accounts. Its activity period begins before 2026. It is a campaign warning, not a national cargo-theft count for this report's window [S68].

The relevant control is the authority to change a movement or payment instruction. Establish an independent route for confirming changed destinations, carriers or settlement details. A reply within the same disputed message thread may preserve the attacker's access to the decision.

This review should include operations and finance. The person who spots an unusual collection instruction may not own supplier payments. Give both functions a shared escalation route and preserve the original instruction and verification result.

8.7 Deceptive meetings and the technical-fix pretext

The November FaceStealer warning explains why a recognisable face or familiar account is insufficient verification. The FBI describes previously recorded victim videos and false technical problems used to persuade a recipient to follow a harmful fix. The report does not reproduce those instructions [S62].

Set a clear rule for unexpected support actions during interviews, investment discussions and external meetings. Stop the improvised repair and use an established support channel. A staff member should not need to decide whether a convincing video is synthetic before refusing an unapproved installation.

When an action was followed, investigate the endpoint and the accounts accessible from it. Repository access, customer information and financial authority can have different owners. Do not assume that changing the meeting account's password answers every question about the device or connected services.

8.8 Closure evidence for fraud-related signals

Question	Evidence that supports closure	Limitation to preserve
Did the signal concern an owned account or customer?	Documented match and relevance assessment	A brand reference alone is insufficient
Was authority independently verified?	Trusted-channel confirmation and approval record	Correct personal details do not establish authority
Did access or a transaction occur?	Relevant service or transaction records	An advertisement or claimed status is not proof
Was the affected route corrected?	Tested recovery, consent or transaction control	A policy document alone does not demonstrate the control
Does residual customer risk remain?	Scoped privacy and fraud assessment	Restoration does not erase disclosed information

KEY TAKEAWAYS

01

Advertising, asking prices and official loss reports describe different quantities.

02

Verify authority independently when recovery, payments or delivery details change.

03

Connect endpoint, identity and customer evidence before closing a fraud-related incident.

CHAPTER 09

Banking and financial-service decisions

09

THIS CHAPTER ANSWERS

Which financial-service responses need joint ownership across security, fraud, operations and legal teams?

25

selected financial estates, rather than independent licensed banks

9.1 The financial portfolio and its limits 94
9.2 Several financial cases, several distinct questions 95
9.3 Customer-account and employee-account evidence 96
9.4 Transactions and payment changes 96
9.5 Supplier-held records and notification readiness 97
9.6 Continuity and reporting clocks 97
9.7 A financial-service closure record 98

CHAPTER 09

Banking and financial-service decisions

IN SHORT

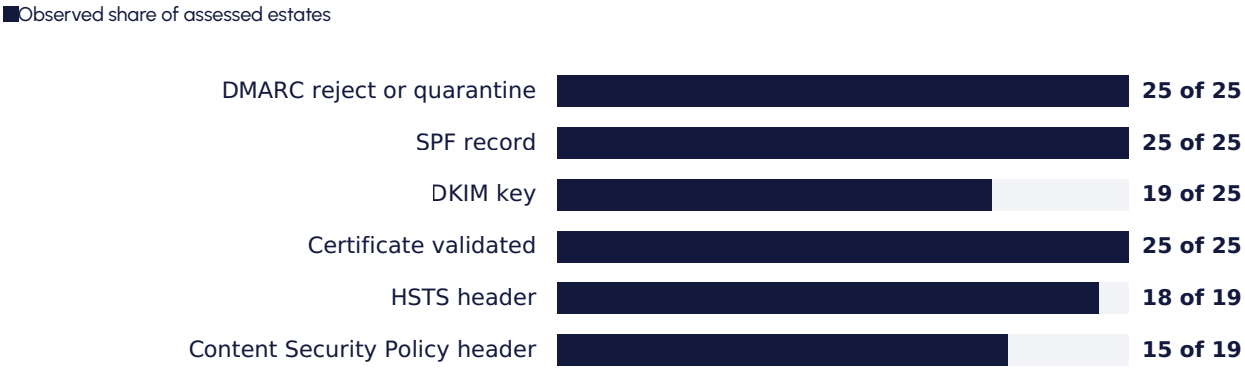
Financial services face account, supplier, information-handling and continuity questions that do not share one denominator. The selected portfolio contains 25 financial estates, and its passive observations remain separate from the narrow payment-card material. Original filings show why data materiality and operational disruption are different decisions. Validate credible account signals, test supplier and transaction authority, and rehearse reporting and service recovery with the relevant business owners.

9.1 The financial portfolio and its limits

The financial group contains 25 selected operating estates. It includes banking, payments, investment and market-related services. It is not a list of independent licensed banks or every US financial institution. Parent, brand and subsidiary relationships can overlap [S2].

Financial-estate observation	Observed estates	Assessed denominator
DMARC reject or quarantine policy	25	25
SPF record	25	25
DKIM key	19	25
Certificate validated	25	25
HSTS header	18	19
Content Security Policy header	15	19

Financial-estate controls preserve their own available-service denominators



Source: dated public-control observations, 22 November 2026. Each control retains its own assessed-estate denominator; observations do not establish complete service assurance [S2].

These figures describe selected financial-estate control observations. They do not describe unique customers, payment cards or confirmed intrusions. The narrow payment-card scope remains in §8.5 and is not attached to the domain-control population.

The 25 financial estates have at least 296,404 device associations, including 76,452 employee-device associations. They also have 11,734,621 credential-record associations and 2,260 document associations. Credentials were listed for sale for 22 of the 25 estates when checked [S2].

The financial estates account for 10.0% of the portfolio's credential-record associations. That share describes historical records; it does not measure financial losses, active customers or confirmed bank intrusions. No financial-sector rating is published.

A subset of 13 banking estates within the 25 financial estates has the following observations. These estates have at least 174,026 device associations, including 55,319 employee-device associations. The remaining 118,707 associations are not identified as employee devices. Current credential listings concern 12 of these 13 estates.

This subset does not represent a national issuer census. The narrow card figures in §8.5 retain their own population. Neither a card observation nor a customer-device association establishes access to a bank's internal systems.

9.2 Several financial cases, several distinct questions

The selected original disclosures support three different financial-service reviews [S20][S21][S22].

Case	Established account	Decision implication
Internal information handling	Non-public customer information was handled in an unapproved AI application	Review authorised workflows and disclosure assessment without requiring an attacker label
Network access and data removal	A regional banking company confirmed unauthorised access and data removal	Scope accounts and data; do not treat an actor's deletion representation as verified erasure
Legal-service supplier	Borrower information was affected at a professional-services provider	Include advisers in data retention, investigation and notification arrangements

These cases are selected disclosures. They do not measure which route is most frequent across US financial institutions. Their common lesson is narrower: the relevant data and authority can sit outside the production transaction platform.

A bank can maintain account access while facing a significant confidentiality decision. Conversely, a technical service failure can require continuity and regulatory decisions without a confirmed malicious actor. Security, operational materiality and personal-information risk therefore need separate fields in the incident record.

9.3 Customer-account and employee-account evidence

An account associated with a financial brand is not automatically an employee identity. Consumer use, historical records and wider service contexts can explain an association. Establish the account type and service relevance before routing the response.

For an employee or contractor account, identity operations should check current status, privileges, recovery settings, application grants and relevant sessions. If internal evidence corroborates unauthorised activity, incident response should preserve and contain it. The response scope follows that evidence.

For a customer account, fraud and customer-protection teams may own validation. Review relevant sign-ins, account recovery, payee changes and transactions within the organisation's lawful process. A domain association alone does not justify describing an intrusion into the provider's corporate estate.

The two views can meet at a service desk or support platform. Staff with customer-account authority deserve particular scrutiny during recovery and privilege changes. Test the authority decision with realistic requests, including accurate personal details that should not by themselves authorise access.

9.4 Transactions and payment changes

The first useful question is what changed in the transaction. Was a payee amended, a new device enrolled, a recovery route replaced or a provider instruction received? Preserve the relevant evidence rather than describing every unusual event as the same type of fraud.

Use independent verification for a high-impact change. The approving staff member should have an established source for the counterparty's contact details. A message received within a known relationship can still originate from an unauthorised account or malicious application permission.

Customer protection also needs a practical service route. A customer who cannot use the ordinary application may seek help through another channel. The fallback should preserve verification and accessibility without silently lowering authority checks for a consequential transaction.

Track legitimate-customer friction as well as suspicious activity. A control that prevents access to an essential service can create harm even when it catches attempted fraud. The business owner should approve the exceptions and review the evidence of both outcomes.

The January DOJ notices also distinguish alleged ATM theft from adjudicated conduct in a separate case. Their charging and sentencing figures are not attack totals. The response should include approved physical servicing and cash-service continuity, rather than assuming every financial incident begins with a customer-account credential [S91][S94].

9.5 Supplier-held records and notification readiness

A provider can hold identification, legal, marketing or historical account information outside the bank's main transaction systems. Contract reviews should establish what information is held, why it remains necessary and who can provide an affected-data assessment during an incident.

The legal-service case demonstrates why supplier notification and the customer's incident decision are separate milestones [S22]. A provider's initial message may be incomplete. The financial institution still needs an accountable process for assessing its own information and reporting obligations.

Agree the minimum initial notice, the evidence needed later and an out-of-hours route. Test the arrangement with incomplete information. A contract requiring a final forensic answer before any notice may fail to support the customer's own prompt reporting decision.

9.6 Continuity and reporting clocks

The federal banking rule requires notification as soon as possible, and no later than 36 hours after a covered banking organisation determines that a defined notification incident occurred. It also creates a distinct provider-to-bank notice duty. The rule is not limited to malicious attacks [S36].

A material-incident filing by a public company has a different trigger under the SEC framework. New York DFS and FTC-jurisdiction financial institutions can face additional, separately scoped requirements. Chapter 10 preserves their recipients, triggers and maximum periods [S35][S38][S39].

A practical exercise should make the team decide which clock has begun and why. Record the evidence available at that moment, the decision maker and the next review time. Waiting for attribution is not a substitute for assessing a service or data trigger.

9.7 A financial-service closure record

Workstream	Accountable function	Completion evidence
Employee or contractor access	Identity and incident response	Validated account scope, relevant session action and recovery checks
Customer-account concern	Fraud and customer protection	Transaction assessment, customer route and documented disposition
Supplier-held information	Supplier owner and privacy	Verified data scope, changed access and notification decision
Payment or instruction change	Operations and finance	Independent verification and authorised transaction record
Service interruption	Business continuity	Tested fallback, reconciled work and business sign-off
Regulatory reporting	Legal and compliance	Applicability decision, timely notice where required and update record

These workstreams should share verified facts without treating every team as the owner of every task. A clear hand-off identifies the unresolved proposition and the evidence needed from the next owner.

The November company statements distinguish marketing or benefit-program information from payment-network availability. They do not identify a shared supplier or establish bank-network compromise. Privacy and fraud owners still need an affected-information decision when payment processing remains available [S107] [S108].

KEY TAKEAWAYS

01

Financial estates, customer identities, employee devices and payment cards have different units.

02

Supplier records and internal handling can matter while transaction systems remain available.

03

Test account, transaction and reporting decisions with security and business owners together.

CHAPTER 10

Regulatory response and notification decisions

10

THIS CHAPTER ANSWERS

Which reporting duty applies, which decision starts its clock, and who owns the evidence?

6

distinct reporting scopes to assess

10.1 One incident record, several legal decisions 100
10.2 Securities disclosure: discovery and materiality are different milestones 101
10.3 Banking notification includes consequential service failures 101
10.4 Health information: the population and recipient matter 102
10.5 Additional financial-service requirements 102
10.6 State notices and developments under review 102
10.7 A reporting exercise with incomplete information 103

CHAPTER 10

Regulatory response and notification decisions

IN SHORT

US incident reporting combines securities, banking, health-information, financial-services and state requirements. Their recipients and triggers differ. An internal disclosure, supplier incident or technical failure can require a decision without a confirmed attacker. A final-rule submission under review is not a commenced universal duty. Map the legal entity and service, record awareness and materiality decisions, and exercise prompt reporting with incomplete information.

10.1 One incident record, several legal decisions

Legal and compliance teams should determine applicability against the actual entity, activities, data and affected people. An incident label alone does not identify the correct regulator or notification route. The table is a decision aid rather than a complete statement of every applicable law.

Keep the shared facts in one record: when the organisation became aware, what service was affected, what information was involved and what remains unknown. Record each legal determination separately, with its owner, evidence and next review time.

Scope	Trigger and recipient	Timing	Important boundary
SEC domestic registrants	Material cybersecurity incident; Form 8-K Item 1.05	Generally within four business days of materiality determination	Determination must occur without unreasonable delay; qualifying national-security or public-safety delay has its own procedure [S35]
Covered banking organisations	Defined notification incident; primary federal regulator	As soon as possible, no later than 36 hours after determination	Includes qualifying major non-malicious failures; not every security alert [S36]
Bank service providers	Defined incident affecting covered bank services; affected bank contact	As soon as possible after determining the qualifying service effect	Material disruption or degradation for four or more hours is part of the defined scope [S36]
HIPAA and Part 2 reporting	Breach of unsecured covered health records; Secretary and other required recipients	Secretary notice without unreasonable delay, at most 60 calendar days for the 500-or-more population	Smaller breaches have a different Secretary reporting schedule; individual and business-associate duties remain separate [S37][S77]

Scope	Trigger and recipient	Timing	Important boundary
New York DFS covered entities	Defined cybersecurity incident; superintendent	As promptly as possible, no later than 72 hours after determination	Separate extortion-payment notices and continuing updates apply [S38]
FTC-jurisdiction financial institutions	Defined notification event; FTC	As soon as possible, no later than 30 days after discovery	At least 500 consumers' unencrypted information under the rule's acquisition definition; not every bank or incident [S39]

These maximum periods do not authorise waiting where the rule requires prompt action. Nor does notifying one recipient demonstrate compliance with every other duty. State resident notices, contractual obligations and sector requirements may also apply.

10.2 Securities disclosure: discovery and materiality are different milestones

The SEC guide ties the ordinary four-business-day Item 1.05 period to materiality determination, rather than discovery. Both quantitative and qualitative factors matter. A sensitive-data event can be material even when the company reports no material operational interruption [S35].

The bank's internal information-handling case and the clinical application notices illustrate that distinction. Their existence does not establish one general financial threshold. Legal and business leadership must assess the particular facts and preserve the decision record [S20][S16].

A voluntary Item 8.01 filing is not automatically an Item 1.05 filing. The laboratory-ordering case is expressly identified as Item 8.01. It should not enter a material-filing total merely because it describes a cybersecurity incident [S29].

An amendment also is not another independent intrusion. Track what the amended filing adds and retain the original event's identity. The public review does not publish a national count derived from third-party filing trackers whose populations or amendment treatment differ.

10.3 Banking notification includes consequential service failures

The federal rule distinguishes a computer-security incident from the narrower notification incident. The latter concerns specified material disruption or degradation to banking operations, significant business lines or financial stability. Covered technical failures can meet the definition without a malicious cause [S36].

The provider notice has a separate purpose: helping the banking customer assess its own service effect. A supplier should not wait for a customer's materiality decision before applying its own defined notice duty. The customer's regulator notification remains the customer's decision.

This creates a practical exercise requirement. Give the team a significant provider failure with incomplete cause information. Require a documented scope and timing decision, while technical teams investigate whether the cause was malicious, accidental or still unresolved.

The rule took effect on 1 April 2022, with compliance from 1 May 2022. It is an existing requirement in this report's window, rather than a proposed response to the November outage stories [S36].

10.4 Health information: the population and recipient matter

HHS distinguishes breaches affecting 500 or more people from smaller breaches for reporting to the Secretary. The larger population requires notice without unreasonable delay and no later than 60 calendar days after discovery. Smaller breaches are due within 60 days after the discovery year's end [S37].

That distinction does not replace individual notification or the business associate's duty to the covered entity. The HHS overview describes separate individual, media and supplier-notice requirements and relevant conditions. A provider's service restoration is not itself a completed breach-notification assessment [S77].

The portal's submission date is not an intrusion date. Its affected-person figure also is not a count of unique national victims when reporting populations overlap. This edition does not infer a January–November national patient total from the partial portal view [S33].

For a supplier event, the controller and provider need an agreed initial notice and later data package. The education and healthcare cases show why the affected-data review can continue after services return. Track that work with a privacy owner rather than silently closing the incident at restoration.

10.5 Additional financial-service requirements

New York DFS Part 500 applies to its defined covered entities. Its incident definition includes qualifying events at an entity, affiliate or third-party provider. The rule also requires continuing updates when material information changes [S38].

An extortion payment has separate notice requirements: notice within 24 hours, followed within 30 days by the required explanation and diligence account. These are payment-related notices, not alternative incident-reporting periods. Applicability and any exemption should be assessed against the actual entity.

The FTC Safeguards Rule applies to financial institutions within the FTC's stated jurisdiction, rather than every organisation commonly called a bank. Its notification-event definition includes the relevant acquisition, information and consumer-population conditions. The guide also treats access to an encryption key as relevant to whether information is unencrypted [S39].

A financial group can therefore need more than one applicability decision. Record the responsible legal entity and regulator rather than assuming the parent brand determines every duty. Use a shared fact record while preserving separate submissions and update obligations.

10.6 State notices and developments under review

State notification obligations depend on the applicable law, affected residents and information. A regulator-hosted company letter establishes the company's stated notice, not a national resident total or a universal state deadline. The selected California notices retain their own event and notification dates [S31][S32].

Legal teams should maintain a jurisdiction matrix that includes who must be notified, what triggers the duty and when a supplement is required. Confirm the current statute and regulator instructions for the actual incident. Do not import a neighbouring state's deadline into another jurisdiction.

On 22 November, OIRA's public record marks the CIRCIA final-rule submission as pending review, received on 1 October. This is a dated rulemaking status. It is not evidence that a universal new reporting duty had commenced [S40].

Prepare by mapping potentially relevant services and incident information, while monitoring official finalisation and commencement. Keep readiness work separate from the table of duties already in force. The report takes no position on the government's rulemaking choices.

10.7 A reporting exercise with incomplete information

Decision	Owner	Evidence to prepare
Which entities and services are in scope?	Legal and compliance	Approved applicability matrix and current source references
What is known about awareness and materiality?	Incident command and disclosure counsel	Time-stamped determination record and supporting facts
Which data fields and people may be involved?	Privacy and data owners	Scoped field inventory, population evidence and outstanding questions
Which service effects are material or qualifying?	Business continuity and service owner	User impact, disruption evidence and relevant definition assessment
What can the supplier state now?	Supplier owner and incident response	Initial notice, evidence requests and update timetable
Which notices and updates were sent?	Legal and communications	Approved text, recipient, submission time and version record

Test the process outside ordinary working hours. A supplier may not yet know the final affected population, and an actor may publish a conflicting number. The organisation still needs a defensible decision about prompt reporting and the facts it can accurately state.

KEY TAKEAWAYS

01

Reporting periods have different triggers, recipients and promptness requirements.

02

An internal disclosure or major technical failure can require a reporting decision.

03

Separate current duties from proposed developments and test the process with incomplete facts.

CHAPTER 11

Outlook and conditions that would change the assessment

11

THIS CHAPTER ANSWERS

What should leaders prepare for, and which new evidence would change that preparation?

4

conditional service-based scenarios

11.1 Key judgements 105

11.2 Four conditional planning scenarios 106

11.3 What the evidence does not support 106

11.4 Leadership review triggers 107

CHAPTER 11

Outlook and conditions that would change the assessment

IN SHORT

The evidence supports preparation for extortion, identity deception, supplier incidents and interrupted services. It does not support a numerical forecast of US attacks or losses. Recent browser-code and runtime notices strengthen the case for knowing what can change a customer-facing service. Choose service-based scenarios, identify their activation signals, and revisit the assessment when confirmations, supplier changes or control tests alter the facts.

11.1 Key judgements

Confidence attaches to the stated proposition, rather than an actor's general credibility or an organisation's security.

Judgement	Confidence	Basis and limit	Assessment-change signal
Extortion warrants a funded recovery exercise	High for the planning decision	4,605 publication-dated claims demonstrate sustained source visibility; outcomes remain unverified [S3]	A relevant incident or failed restore changes the organisation's own priority
Credible identity offers deserve an accountable validation decision	High for the response principle	Advertisements require account, service and freshness checks [S1]	Corroborated unauthorised activity justifies incident escalation
Supplier permissions belong in continuity planning	High	Original cases establish several specific provider dependencies [S8][S10][S19][S22]	A provider change, broader access or failed notification test changes the response need
Operational effects need process-owner evidence	High	Water-system reporting distinguishes technology impact from individual service outcomes [S6][S7]	Confirmed process changes or user harm justify a broader incident account
Bundled software requires explicit ownership	High for inventory need	Recent Java alerts include runtimes within other products [S45][S46]	An affected owned build, unsupported service or provider warning activates remediation
The recent claim population remains a monitoring priority	High for observation, not prediction	357 publication-dated records fall in 8–22 November [S3]	New confirmations, corrections or withdrawals change the closing-period picture

The identity judgement does not assume that every offer is genuine. It says a credible signal should receive a reproducible decision. The response can become more urgent when the organisation finds corroborating activity in its own records.

The supplier judgement likewise does not make a numerical prediction. It follows from the specific permissions and service dependencies in the original cases. A supplier with independently tested recovery and narrowly scoped access can present a different risk from another provider.

11.2 Four conditional planning scenarios

These scenarios are planning assumptions, rather than forecasts or assertions that a named organisation is vulnerable.

Scenario	Activation signal	Initial owner	First decision
An actor advertises recent access to a business application's data	Credible matching details or corroborated unauthorised activity	Identity, data owner and incident commander	Restrict relevant access, preserve records and define the data boundary
A provider changes code delivered to customer browsers	A provider notice or verified unexpected script behaviour	Web application and supplier owners	Identify affected pages, control the integration and assess visitor impact
An operational service loses remote monitoring or management	Independent process or service evidence confirms an effect	Operations, safety and network owners	Maintain safe function, validate intended access and activate a tested fallback
A critical update applies to software bundled in a managed service	Vendor or provider evidence identifies an affected owned runtime	Vulnerability management and platform owner	Verify scope, arrange remediation and obtain build or provider evidence

Each scenario also needs a communications decision. The organisation may have to explain service impact before attribution is known. It may need to warn people about misuse of personal information while the final data population remains under review.

A scenario should identify what would stop escalation as well as what would activate it. Prior remediation, an inactive account or an unrelated lawful service can narrow an external signal. Record that conclusion with its evidence rather than leaving an alert indefinitely unresolved.

11.3 What the evidence does not support

The comparator table is not a country ranking by the likelihood of attack. Its source labels, business populations and visibility differ. Comparing a partial year with a complete previous year also does not create a matched-duration growth measure [S3].

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

The selected estate portfolio does not establish the national proportion of organisations with an active unauthorised account. Public-control observations also cannot establish the strength of every internal system. An unavailable observation is not silently converted to a failure or a successful control [S2].

The public disclosure set does not establish the national share of incidents caused by suppliers, social engineering or a particular technology. Its healthcare concentration reflects selected original evidence. A meaningful national prevalence claim would require a different evidence population.

The report does not estimate national loss from asking prices, advertised record totals or global official campaign figures. Those are different quantities. A recently announced enforcement action may concern conduct over several earlier years and cannot be relabelled as current-window loss [S61][S63][S69].

A shared label does not establish one operator across every claim. A shared tactic does not establish a relationship between criminal, state-attributed and politically framed activity. Those relationships require concrete evidence beyond the resemblance.

11.4 Leadership review triggers

Revisit this assessment after a material supplier change, identity redesign, important service migration or new incident confirmation. A stronger original disclosure may replace a claim-only proposition. A correction or withdrawal may narrow an earlier account.

Use demonstrated control outcomes when deciding investment. An unowned privileged account, a provider unable to supply investigation records, or a failed recovery exercise is an actionable finding about the organisation. These findings can justify change without a national numerical forecast.

More alerts do not necessarily mean worse security, and fewer alerts do not necessarily mean less threat. Business activity, visibility and detection coverage can change. Leadership should ask which verified service or customer outcome changed, and what the responsible owner needs to do next.

KEY TAKEAWAYS

01

Scenarios are conditional plans with observable activation signals.

02

Confidence follows a proposition and its evidence, rather than an actor name.

03

Reassess when disclosures, supplier changes or control tests change the service facts.

CHAPTER 12

A 30/60/90-day action plan

12

THIS CHAPTER ANSWERS

Who acts, what should happen first, and what evidence demonstrates completion?

90 days

a proposed programme adjusted to essential service priorities

12.1 Delivery lanes 109
12.2 Identity operations: close the actual access question 111
12.3 Platform teams: connect inventory to a verified change 111
12.4 Business continuity: restore the process and reconcile the work 112
12.5 Supplier owners: obtain usable evidence and an actionable notice 112
12.6 Threat intelligence and the SOC: keep propositions separate 113
12.7 Fraud, privacy and communications: prevent the next avoidable harm 113
12.8 Leadership evidence at each checkpoint 113
12.9 How Brandefense can help 114

CHAPTER 12

A 30/60/90-day action plan

IN SHORT

Start with ownership and validation, then demonstrate that essential services can continue and recover. The plan joins identity, suppliers, customer fraud, public controls and notification. Its timing is a suggested programme, not a statutory deadline. Corroborated active incidents require immediate response. Have business leaders choose the important services, approve accountable owners and review demonstrated results at each phase.

12.1 Delivery lanes

Apply each action to an identified service or verified exposure. Urgent, applicable remediation and corroborated incident response should proceed immediately. The programme periods are assurance checkpoints, rather than waiting periods. An old or unverified advertisement needs validation before a disruptive estate-wide change.

1Days 1–30		
If a credible access or credential offer matches the estate, validate account status, relevant sessions and prior remediation	OWNER Identity operations and incident response	COMPLETION EVIDENCE Accountable disposition and escalation decision for each credible signal
Identify services whose interruption would cause unacceptable operational or customer harm	OWNER Business owners and CISO	COMPLETION EVIDENCE Approved service list, minimum usable function and responsible owner
Inventory supplier permissions supporting those services, including browser scripts and business-app integrations	OWNER Platform and supplier owners	COMPLETION EVIDENCE Permission owners, emergency restriction route and current support contacts
Reconcile reporting scopes, awareness decisions and out-of-hours contacts	OWNER Privacy, legal and compliance	COMPLETION EVIDENCE Applicability matrix and a completed incomplete-information exercise

For operational systems, validate intended external access and safe fallback

OWNER

Process, safety and network owners

COMPLETION EVIDENCE

Approved connectivity map and demonstrated fallback procedure

2Days 31–60

Where recovery depends on easily obtained personal details, strengthen independent verification

OWNER

Identity engineering and service desk

COMPLETION EVIDENCE

Tested recovery flow, protected audit records and approved exceptions

Reconcile bundled runtimes, managed-service dependencies and unsupported software

OWNER

Platform and supplier owners

COMPLETION EVIDENCE

Validated inventory and an owner for each unresolved support issue

Review email-policy observations against legitimate sending services

OWNER

Messaging and domain owners

COMPLETION EVIDENCE

Sender inventory, approved policy and successful delivery checks

If customer reports show impersonation using genuine details, adjust verification and warnings

OWNER

Fraud and customer operations

COMPLETION EVIDENCE

Updated contact process and review of observed outcomes

Rehearse an incident at an important supplier with incomplete initial facts

OWNER

Supplier owner and incident commander

COMPLETION EVIDENCE

Timed notice, dependent-service map and recorded decisions

3Immediate where urgent and applicable

Remediate the exact owned product and distribution under the applicable requirement or supported incident decision

OWNER

Vulnerability and platform owners

COMPLETION EVIDENCE

Version or provider evidence, approved change and service validation

4Days 61–90	
Restore an important service with protected backups and separate recovery access	
OWNER Continuity and platform teams	COMPLETION EVIDENCE Integrity checks, measured readiness and business sign-off
Test availability and reconciliation during a plausible provider failure	
OWNER Business and network operations	COMPLETION EVIDENCE Demonstrated fallback, reconciled queued work and tracked corrections
Review whether intelligence signals receive consistent dispositions	
OWNER CISO and assurance	COMPLETION EVIDENCE Sampled decisions, exceptions and assigned corrective work
Present unresolved service risks and funding decisions to leadership	
OWNER CISO and business owners	COMPLETION EVIDENCE Accepted risks, funded actions and review dates

12.2 Identity operations: close the actual access question

A useful intelligence disposition records the account or service match, current status, relevant activity and prior remediation. Another analyst should be able to understand why the signal was closed or escalated. Preserve necessary evidence without circulating personal information unnecessarily.

When unauthorised activity is corroborated, use incident response to contain relevant access and investigate persistence. The scope may include sessions, recovery routes and application permissions. A password change answers only one part of that investigation.

Test service-desk authority with realistic requests. A caller may possess genuine customer or employment details and use a familiar displayed number. Independent verification should remain usable when staff face urgency, seniority or a plausible technical problem.

Prefer phishing-resistant MFA for privileged and remote access where the service supports it. The election warning provides a relevant official recommendation without implying an election outcome or party-specific risk. Test recovery so it does not quietly bypass the stronger sign-in control [S56].

12.3 Platform teams: connect inventory to a verified change

The technical examples in Chapter 7 show why a product name is insufficient. Model, hardware revision, distribution, build and support status can change the affected scope. An application can bundle a runtime that is absent as a separate inventory entry [S42][S45][S75].

Assign responsibility for that hidden dependency. For a managed service, obtain the provider's applicability and remediation statement. For an owned platform, validate the installed build and restart requirements through the authorised change process. A purchased licence does not demonstrate that the required correction is present.

Treat passive control observations as owner-review leads. Confirm domain purpose and intended configuration before changing a mail policy or web control. The closure evidence should include a service test, not only the presence of a new record or header.

Browser-code providers need a specific emergency decision. Identify which pages load the integration and who can disable or re-enable it. Test the effect on important transactions, including payment or identity functions where relevant. Preserve evidence before routine deployment overwrites it.

12.4 Business continuity: restore the process and reconcile the work

A restore test should include identities, configurations, approvals, keys and supplier dependencies. Protected backup data is only one requirement. The team also needs a route to coordinate when ordinary collaboration tools are unavailable.

Measure completion at the business function. Demonstrate an order, clinical request, customer transaction or public notice using the restored service. Check integrity and permissions, and have the business owner approve readiness.

Reconcile work performed during the interruption. A service can be online while delayed or duplicate work still causes harm. Record what needs repetition, correction or customer explanation, with an owner for each unresolved item.

Operational systems require process and safety approval. Test a manual or degraded mode under realistic staffing and time constraints. A security team should not declare a physical process safe merely because a management connection works again.

12.5 Supplier owners: obtain usable evidence and an actionable notice

For each critical provider, record data held, permissions granted, emergency controls and investigation-record availability. Establish the first-notice recipient and an alternative route outside working hours. Verify that those contacts can act.

Exercise a notice that lacks a final affected-person count. The customer should still be able to identify dependent services, preserve its own records and begin the required legal assessment. A later provider package can update the scope without erasing the earlier decision history.

Apply the same process to professional advisers, cloud business applications and website providers. Their data and permissions can matter even when the primary production platform is unaffected. The case evidence supports service-specific reviews, rather than an assumption that every provider has the same risk.

12.6 Threat intelligence and the SOC: keep propositions separate

Store an actor post, a third-party relay, a listing and an official disclosure as separate evidence records. Link them only when a concrete common element supports the relationship. A shared brand or broad sector is insufficient.

When a recent advert resembles an old one, identify what is actually repeated. Matching wording can support a repost assessment. It does not establish file identity, a new theft date, a completed sale or current access.

An alert should tell the receiving owner which question to answer. Current account relevance, sensitive document availability and service impact require different evidence. Avoid distributing actor contacts, downloadable samples or unnecessary victim identifiers in ordinary tickets.

No untested production detection rule is presented here. Implement monitoring appropriate to the actual platform and validate expected alerts alongside legitimate activity. Keep the distinction between a review recommendation and a tested detector.

12.7 Fraud, privacy and communications: prevent the next avoidable harm

Share a corroborated disclosure with fraud and customer operations when the information can affect verification or transactions. Define the customer action clearly, using an established route. An actor's name or claimed population is rarely the most useful instruction.

Privacy should maintain the affected-data assessment after restoration. Communications should preserve known fields, date boundaries and unresolved scope. A supplier's reassurance, actor deletion promise or removed listing is not independent evidence that every copy has disappeared.

Legal should record each applicable reporting trigger and update obligation. A public-company filing, regulator notice and individual warning can require different information at different times. Keep their facts consistent while respecting the separate duties.

12.8 Leadership evidence at each checkpoint

Checkpoint	Leadership question	Evidence that answers it
Day 30	Do we know which services, identities and suppliers matter most?	Approved service map, validated signal dispositions and reporting matrix
Day 60	Have we removed consequential avoidable access paths?	Tested recovery verification, supplier review and applicable remediation evidence
Day 90	Can the business continue, restore and reconcile its work?	Witnessed restore, usable fallback, integrity checks and business sign-off

A completed document is not the same as a demonstrated control. Ask to see one realistic account-recovery test, one supplier-notification exercise and one service restore. Keep unresolved findings visible until the owner supplies closure evidence.

12.9 How Brandefense can help

Odin by Brandefense connects external observations to security decisions grounded in evidence. Brandefense's threat intelligence, digital risk protection and external attack surface management capabilities can support assessment of relevant external signals. Agree the scope, validation needs and response ownership for the actual environment.

Request a Brandefense demo to discuss the services, domains and intelligence decisions that matter to your team.

KEY TAKEAWAYS

01

Every action needs an accountable owner and demonstrable completion.

02

Escalate corroborated unauthorised activity while preserving claim-only evidence limits.

03

Prove continuity and recovery with the business before closing the programme.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Appendix A. Scope, populations and evidence limits · Appendix B. Evidence and decision register · Appendix C. Sources · Appendix D. Terms used in the report

108

sources

Appendix A. Scope, populations and evidence limits 116
Appendix B. Evidence and decision register 120
Appendix C. Sources 126
Appendix D. Terms used in the report 131

Appendix A. Scope, populations and evidence limits

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

A.1 Publication window and edition

This is the English master of the Brandefense United States Cyber Threat Landscape Report 2026. No translated edition accompanies it. The research window is 1 January–22 November 2026, with a closing-activity section covering 8–22 November. The cut-off applies to post or publication dates through 22 November. Source checks can occur at different times; each source entry retains its actual verification date.

Dates describe post or publication timing, with timezone uncertainty where applicable. They do not establish when access or acquisition occurred. Public-source cases distinguish access, discovery, awareness, materiality, publication, notification and recovery. An in-window filing can describe activity beginning before 2026. A recent announcement can describe enforcement against a campaign active for several years.

A.2 The populations used in this report

Evidence population	Result or coverage	Interpretation limit
Retained post evidence	37,866 distinct retained post records available for case analysis [S1]	Examples and retained observations, not a national census of offers or attacks
Extortion listings	4,605 US-labelled publication-dated claims [S3]	Claims, not confirmed access, encryption or independently verified victims
Closing-period extortion	357 publications dated 8–22 November [S3]	Publication dates do not establish access dates
Selected portfolio	250 operating estates across ten sectors; national Atlas headline 80/100 [S2]	Purposive selection; shared ownership and infrastructure can exist
Current credential listings	172 of 250 estates [S2]	On offer when checked; not sold accounts or confirmed intrusions
Device associations	At least 2,251,336, including 633,281 employee-device associations [S2]	Cumulative overlapping associations, not distinct national endpoints
Credential-record associations	117,106,392 across 250 estates [S2]	Historical records, not active accounts or unique people
Passive observations	248 assessed estates; available controls retain their own denominators [S2]	Dated public observations, not complete service assurance
Source-supported cases	29 incident and disclosure families	Includes an earlier incident update and events with different date boundaries

Evidence population	Result or coverage	Interpretation limit
Public campaign notices	Selected official notices across the window	Publication and attribution belong to each source; historical and global totals stay separate
Card material	Limited post-based payment-card observations [S4]	Not all cards seen by Brandefense, national card theft or financial loss
IC3 context	2025 complaints and reported losses, published in 2026 [S5]	Earlier-year complaint population; no extrapolation to 2026
HHS OCR context	Available displayed notices [S33]	Partial view, not a national January–November breach total

Posts can refer to the same offer, data or event. A listing can concern a multinational organisation, a subsidiary or a repeated organisation label. Provider incidents can also produce several customer notices. These populations cannot be added together as unique affected organisations.

A.3 What the public-source coverage achieves

The selected original notices cover healthcare, manufacturing, education, financial services, communications, public services and customer-facing web software. They identify concrete differences between information access, service interruption, supplier exposure and an internal disclosure to an unapproved application.

The official campaign coverage includes identity deception, router activity, supporting device networks, operational-system warnings, extortion and enforcement actions. CISA, FBI and IC3, DOJ, NSA, healthcare notices, SEC filings and selected state breach notices provide complementary evidence. They do not share one incident definition.

The retained corpus supports selected cases and thematic review. Material outside the priority organisation and campaign scope receives no incident determination in this edition.

Monthly official-source coverage is bounded to priority organisations, important campaigns and material service effects. It is not a reading of every US breach notice, every state submission or every securities filing. Missing source coverage is not evidence that no incident occurred.

The public account of the learning-platform incident evolved during the year. Earlier English and Russian reporting does not replace a later supplier update. The current original account governs the reported scope where it differs from earlier coverage [S9][S73].

The source-supported case set contains 29 disclosure families. Selected official and vendor material spans January–November [S89][S42][S62]. Securities and state-notice coverage remains selective. Healthcare portal records were available in partial views, while full monthly populations were not established. No national healthcare or state-notice total is inferred.

The report does not infer confirmed incidents from announcements alone. An alert can describe an ongoing risk without identifying a new US victim. An enforcement release can describe earlier global conduct. An operational notice can attribute a service problem to maintenance rather than unauthorised activity [S47][S61][S65].

A.4 Confidence attaches to the proposition

Evidence type	Proposition with support	Proposition not established by that support
Retained post	The advertised text and date were observed	Authenticity, payment, delivery or current access
Extortion listing	The source records a claim with a publication date	Successful encryption or an independent victim count
Original company notice	The company disclosed the stated scope at that time	Every earlier or later consequence, or an actor's full account
Agency attribution	The agency published the stated assessment	Independent attribution by Odin by Brandefense
Passive control	The stated public observation was available	Complete configuration correctness or absence of intrusion
Analytical judgement	A defined decision follows conditionally from the evidence	A measured forecast or proof of an actor relationship

High confidence in a retained count does not imply high confidence in every advertiser's assertions. A company's later amendment can also change the scope of an earlier notice. The relevant date and proposition therefore accompany the assessment.

A.5 Privacy and naming

Unverified targets receive broad role labels. An organisation is named for an incident only where an official confirmation and substantial independent reporting support that use. Named examples retain the source's scope and date limits.

Source references for withheld organisations use a neutral publisher's root and mark the article URL as withheld. No contact route, personal record or card number is necessary for the report's defensive decisions. A generic case label is not a claim about every organisation in that sector.

A.6 Exposure coverage and interpretation

Atlas supplies a national headline of 80/100 for the selected 250-estate portfolio. Only that national rating is published. Anonymous sector rows show signal counts and denominators, without organisation or sector ratings [S2].

The exposure snapshot is dated 22 November 2026. Device, credential and document associations reflect cumulative records available on that date. Current listings describe credentials on offer when checked. Mention context covers 23 November 2025–22 November 2026; lookalike context covers the preceding 30 days.

Associations can overlap across domains and sources. They do not supply unique people, unique national endpoints, confirmed intrusions or verified current account validity. Device totals are lower bounds, and employee associations are included within the device view.

Passive controls describe a separate assessed population of 248 estates. Two selected estates lack validated assessed results, and unavailable web or certificate observations remain separate from observed control absence. Exposure totals do not repair those passive-coverage limits.

A.7 Revision rules

A later source may establish a different incident scope or outcome. A revision should preserve the prior account's date and explain what changed. Counts with different periods or definitions should be restated explicitly, rather than silently replacing one denominator with another.

Readers should use the current original notice for an operational or legal decision. This report supplies a dated research assessment and accountable defensive tasks. It does not replace an organisation's own incident evidence or a determination of its applicable legal duties.

Appendix B. Evidence and decision register

The register below links the supported disclosure families to their source and first defensive decision. It is not a national incident list. Several notices can belong to one family, and the water-system family describes several affected systems without a common actor finding.

B.1 Source-supported disclosure families

Report reference	Family or role	Evidence boundary	Source	Decision
G	Stryker's operations and restoration milestone	Company filing; dated recovery milestone	[S12]	Recovery must demonstrate the business process, not only the return of individual systems.
H	Amgen's information in third-party cloud environments	Company-confirmed data incident	[S14]	A data incident can require a substantial response while specified operations remain unaffected.
I	A limited electronic-health-record environment	Original filing confirms a scoped incident	[S16]	Service restoration and the patient-data assessment are separate closure decisions.
J	A medical manufacturer's network outage	Original filing confirms operational disruption	[S17]	An outage exercise should follow an order through production and delivery.
K	Impersonation against healthcare personnel	Company account; investigation continuing at filing	[S18]	Verify authority through a trusted process, not through the incoming caller's presentation.
L	A customer-management integration at a communications provider	Original filing identifies an integration boundary	[S19]	The integration's actual permissions define the first investigation boundary.
M	Internal disclosure through an unapproved AI application	Confirmed internal information-handling incident	[S20]	A material information incident can occur without an attacker or an outage.
N	A banking investigation and a deletion representation	Original amendment; erasure not independently verified	[S21]	A deletion assertion cannot substitute for an affected-data and customer-risk decision.

Report reference	Family or role	Evidence boundary	Source	Decision
O	Financial information at a legal-service provider	Original filing; supplier environment distinguished	[S22]	A professional-services supplier belongs in the data and notification dependency map.
P	A contractor session and healthcare business applications	Company-confirmed session and data incident	[S23]	A session investigation must include connected services and exposed stored credentials.
Q	Hosted applications and a separate extortion demand	Company-confirmed data removal; demand separately dated	[S24]	The extortion narrative and the organisation's confirmed scope need separate evidence.
R	A clinical supplier's older incident and later confirmation	2026 follow-up to an incident disclosed in 2025	[S25]	An older incident can create new response work without becoming a new attack.
S	Encryption, data removal and manufacturing restoration	Company filing confirms encryption and data removal	[S26]	Confirmed encryption and confirmed data removal require complementary recovery and privacy decisions.
T	Patient records in a laboratory ordering application	Item 8.01 notice; scope under investigation	[S29]	Operational materiality and patient-data exposure answer different questions.
U	Instructure's education-platform incident and later review	Provider and federal agency confirmation	[S8]	Institution-specific evidence matters more than an actor's advertised school count.
V	Optimizely's website-script incident and downstream response	Provider-confirmed incident; downstream boundaries stated	[S10]	Trusted third-party browser code needs an inventory, an emergency control and an impact review.
W	A court-service provider's interruption and restoration	Official service notice and dated restoration update	[S30]	A restored supplier service still needs business reconciliation and accountable sign-off.
X	An insurance quotation tool's pre-fill information	Submitted organisation notice; access period crosses years	[S31]	Public workflow responses deserve a privacy review alongside account and network controls.

Report reference	Family or role	Evidence boundary	Source	Decision
Y	A school-system notice with a limited network boundary	Submitted original notice; student-store boundary retained	[S32]	Preserve the affected segment and data-owner boundary in every communication.
Z	Water-system technology and actual service effects	Official incident reporting; attribution unresolved	[S6]	Technology impact, service disruption, public-health consequence and attribution require separate evidence.
Note 1	An investment-management company	The recent date is directory reporting, not new access in November. Do not convert cloud-file access into trading-account or payment-system intrusion.	[S84]	Validate affected cloud permissions, sessions and institution-specific data fields; route credible customer questions through established contacts.
Note 2	A mobility-services company	Notice date is within the recent window. Access determination and provider alert are October events.	[S85]	Test revocation of provider connections and determine what data remained accessible under the affected provider account.
Note 3	A medical-device company	Recent directory reporting is established. Do not imply every listed data category affected every person or that device products/patient care were disrupted.	[S86]	Review employee-account sessions and file access, validate individual notice fields, and coordinate privacy and identity response.
Note 4	A medical-components manufacturer	One incident family with a later notice, not February plus November attacks. 5 November is before the recent window.	[S87]	Preserve service-level continuity evidence and follow data review through to individual notifications.
Note 5	A dental-services company	Use the later acquisition finding. The 7 October cover date is the reported earliest-event date; the filing was signed on 13 October. One incident family across both disclosures.	[S88]	Reconcile privacy notification scope with forensic findings and keep litigation allegations separate from established facts.

Report reference	Family or role	Evidence boundary	Source	Decision
Note 6	A legal-information provider	Direct company responses confirm limited server access; most information was older. Access timing, actor volumes and US-only affected population remain unconfirmed.	[S101][S102][S103]	Validate legacy-server retention and access, preserve evidence and assess the information actually involved.
Note 7	November bank marketing-data notice	The company believed marketing information was accessed at suppliers; access date and vendor identities unknown. Services were not disrupted.	[S107][S108]	Validate supplier information scope and customer-protection decisions.
Note 8	November benefit-program email exposure	Limited email information at a supplier; payment network and payment information excluded by the company. Relation to the bank disclosure unresolved.	[S107][S108]	Reconcile provider relationships and data fields without adding overlapping populations.
Note 9	Federal application security incident	On-record cyberthreat acknowledgement on 20 November; reported application effects and an expected recovery milestone. No actor or completed-restoration finding.	[S109][S110][S111]	Demonstrate service readiness and reconcile interrupted work.

B.2 Main numerical findings

Finding	Numerator and denominator	Period	Supported interpretation
Strict US extortion population	4,605 publication-dated claims	1 January–22 November 2026	Source listing assertions, not unique confirmed victims [S3]
Closing-period extortion	357 of 4,605 window claims	8–22 November 2026	A publication-date subset, not access dates [S3]
Leading five listing labels	1,602 of 4,605 claims; 34.8%	Window	Concentration of labels, not verified operator shares [S3]
Selected estate portfolio	250 estates; 25 in each of ten sectors	Selection for this edition	Purposive operating-estate population, not a national sample [S2]

Finding	Numerator and denominator	Period	Supported interpretation
Passive assessed population	248 of 250 selected estates	22 November 2026	Available observations; two estates lack an assessed result [S2]
DMARC policy	169 reject, 41 quarantine, 32 monitoring, 6 not observed; 248 assessed	22 November 2026	Published-policy observations, not universal message enforcement [S2]
Web-control population	155 available results and 93 unavailable; 248 assessed	22 November 2026	Header results use 155; unavailability is not control absence [S2]
Disclosed families	29 supported families	Various disclosed dates	Distinct sources and updates, not 29 new attacks beginning in 2026
Earlier IC3 context	1,008,597 complaints; approximately $20.877 billion reported losses	Whole 2025	Complaint and reporting context, not a 2026 estimate [S5]

B.3 Supported campaign propositions

Publication	Proposition retained	Limit	Owner decision
January QR warning [S47]	The FBI describes QR-based phishing and its attribution	Concrete examples predate 2026	Verify sign-in destinations and preserve suspicious-message evidence
March and June messaging notices [S48][S49]	Official guidance distinguishes linked devices and recovery material	Account compromise does not establish broken application encryption	Review account recovery, linked devices and relevant sessions
April router warning [S50]	FBI describes router-mediated credential exposure and its attribution	Activity begins before 2026; no US-window victim total	Validate router configuration, support and affected account activity
April supporting-network guidance [S51]	NSA and partners describe multiple actor sets' use of device infrastructure	Shared infrastructure categories do not establish one operator	Review external administration and unexpected device changes
May and September identity warnings [S67][S66]	Device-code and application-consent lures involve different grants	No universal failure of multi-factor authentication is established	Revoke the relevant permission or session and assess activity
July water warnings [S6][S7]	Sources report technology effects and some operational consequences	No universal water interruption or contamination finding	Work with operational owners and communicate utility-specific facts
August PLC warning [S59]	Agencies describe reconnaissance and capability development	Potential physical harm is not an observed national outcome	Validate operational connections and approved monitoring software

Publication	Proposition retained	Limit	Owner decision
October election warning [S56]	Agencies warn of phishing against election-related accounts	No vote or result manipulation finding	Protect administration accounts and use trusted reporting routes
October SafePay advisory [S57]	Agencies describe extortion behaviour and named techniques	Historical international figures are not US 2026 prevalence	Test relevant detection, containment and independent recovery
November malware action [S61]	DOJ announces infrastructure disruption	Historical victims do not become recent infections	Investigate relevant internal evidence and confirm actual recovery
November fake-meeting warning [S62]	FBI describes deceptive meetings and its attribution	Global historical losses are not US-window losses	Verify meetings and sensitive actions through another trusted channel
November Java notices [S43] [S44][S45][S46]	NVD, vendor and agencies support a scoped remediation review	A notice is not exploitation at a selected estate	Match distribution, affected component and supported update

B.4 How to close an unresolved proposition

A credible external signal should lead to an explicit owner decision. Record what matched, the current service boundary, the evidence consulted and the remaining uncertainty. A claim can close as uncorroborated, or it can lead to an incident when the organisation's evidence supports that conclusion.

For original notices, preserve the version and date of the source. A later acquisition finding supersedes an earlier possible-access description for that proposition. A recovery statement remains limited to the services and date it actually covers.

For source-attributed campaigns, retain the agency's attribution language. The report does not extend it to every similarly named persona, related tool or contemporaneous disruption. A relationship needs its own concrete evidence.

Appendix C. Sources

Original bodies and source records were checked for the propositions used in this edition. A publisher-root link marked article URL withheld preserves an unnamed organisation's identity. Brandefense links identify the publisher of retained evidence; they do not provide a public download of the private observation set.

S1: Odin by Brandefense. Country-associated source counts and retained post observations. https://brandefense.io/. Verified on 2026-11-22.

S2: Odin by Brandefense. Brandefense Atlas exposure snapshot for 250 selected estates, 22 November 2026, and separate passive control observations for 248 estates. Mention context: 23 November 2025–22 November 2026; lookalike context: preceding 30 days. https://brandefense.io/. Verified on 2026-11-22.

S3: Odin by Brandefense. Ransompedia extortion-listing snapshot. https://brandefense.io/. Verified on 2026-11-22.

S4: Odin by Brandefense. Narrow post-based payment-card aggregates. https://brandefense.io/. Verified on 2026-11-22.

S5: FBI IC3. 2025 Internet Crime Report. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf. Verified on 2026-11-22.

S6: Minnesota IT Services. Water-system incident response and attribution limits. https://content.govdelivery.com/accounts/MNIT/bulletins/422e230. Verified on 2026-11-22.

S7: FBI and EPA. Water and wastewater operational-system warning. https://www.ic3.gov/PSA/2026/PSA260730.pdf. Verified on 2026-11-22.

S8: Federal Student Aid. Learning-management incident security alert. https://fsapartners.ed.gov/fsa-print/publication/1007163. Verified on 2026-11-22.

S9: Instructure. Security incident updates and FAQs. https://www.instructure.com/incident_update. Verified on 2026-11-22.

S10: Optimizely. Web Experimentation incident summary. https://pages.optimizely.com/rs/947-RKE-048/images/Security%20Incident%20Report%20-%20Optimizely%20Web%20Experimentation%20-%20Nov%2017%202026.pdf. Verified on 2026-11-22.

S11: Salesforce Security. Response to third-party website-script incident. https://www.salesforce.com/blog/our-response-to-the-optimizely-optimjack-supply-chain-compromise/. Verified on 2026-11-22.

S12: Stryker, SEC filing. Operational-impact and restoration amendment. https://www.sec.gov/Archives/edgar/data/310764/000119312526149607/d112875d8ka.htm. Verified on 2026-11-22.

S13: Stryker. Customer network-disruption updates. https://www.stryker.com/tr/en/about/news/a-message-to-our-customers-03-2026.html. Verified on 2026-11-22.

S14: Amgen, SEC filing. Third-party cloud data incident. https://www.sec.gov/Archives/edgar/data/318154/000031815426000119/amgn-20260729.htm. Verified on 2026-11-22.

S15: Reuters via Investing.com. Reporting on cloud-held patient information. https://www.investing.com/news/stock-market-news/amgen-discloses-data-breach-says-patient-information-was-stolen-4829238. Verified on 2026-11-22.

S16: An electronic-health-record provider. March limited-environment disruption filing. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S17: A medical-device manufacturer. August disruption and September operational update. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S18: A healthcare-management company. September social-engineering incident filing. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S19: A communications-services company. June customer-management integration incident. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S20: A regional financial-services company. Internal disclosure to unapproved AI application. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S21: A regional banking company. Network-access investigation amendment. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S22: A financial-services company. Legal-service provider ransomware disclosure. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S23: A home-healthcare company. Cloud and contractor-session incident. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S24: A medical-monitoring company. Hosted business-application data incident. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S25: A clinical-care company. Earlier supplier incident with May scope update. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S26: A pharmaceutical-supply manufacturer. May restoration and data-theft amendment. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S29: A diagnostic-services company. Laboratory ordering-system incident notice. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S30: US Courts. Court-service provider interruption and restoration. https://www.uscourts.gov/ (article URL withheld). Verified on 2026-11-22.

S31: California Attorney General, submitted organisation notice. Insurance-quotation pre-fill information incident. https://oag.ca.gov/ (article URL withheld). Verified on 2026-11-22.

S32: California Attorney General, submitted organisation notice. School-system limited-segment access notice. https://oag.ca.gov/ (article URL withheld). Verified on 2026-11-22.

S33: HHS OCR. HIPAA breach reports under investigation. https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf. Verified on 2026-11-22.

S35: SEC. Cybersecurity incident-disclosure compliance guide. https://www.sec.gov/resources-small-businesses/small-business-compliance-guides/cybersecurity-risk-management-strategy-governance-incident-disclosure. Verified on 2026-11-22.

S36: OCC, Federal Reserve and FDIC. Banking computer-security incident notification final rule. https://www.govinfo.gov/content/pkg/FR-2021-11-23/pdf/2021-25510.pdf. Verified on 2026-11-22.

S37: HHS. Breach Notification Rule and Secretary reporting. https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html. Verified on 2026-11-22.

S38: New York DFS. 23 NYCRR Part 500. https://www.dfs.ny.gov/system/files/documents/2026/10/NYCRR-part-500-Cybersecurity-Regulation_1.pdf. Verified on 2026-11-22.

S39: FTC. Safeguards Rule compliance guide. https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know. Verified on 2026-11-22.

S40: OIRA. Submissions under review on the cut-off date. https://www.reginfo.gov/public/do/eoReviewSearch?agencyCode=1600&searchType=0. Verified on 2026-11-22.

S41: NVD. CVE-2026-1731 record. https://nvd.nist.gov/vuln/detail/CVE-2026-1731. Verified on 2026-11-22.

S42: BeyondTrust. BT26-02 advisory. https://www.beyondtrust.com/trust-center/security-advisories/bt26-02. Verified on 2026-11-23.

S43: NVD. CVE-2026-114938 record. https://nvd.nist.gov/vuln/detail/CVE-2026-114938. Verified on 2026-11-23.

S44: Oracle. November 2026 Critical Security Patch Update. https://www.oracle.com/security-alerts/cspunov2026.html. Verified on 2026-11-22.

S45: New York DFS. Java inventory and patching alert. https://www.dfs.ny.gov/industry-guidance/industry-letters/il20261118-Java-Vulnerability. Verified on 2026-11-22.

S46: CISA. Java runtime patching alert. https://content.govdelivery.com/accounts/USDHSCISA/bulletins/4332a87. Verified on 2026-11-22.

S47: FBI. Foreign-policy and academic QR phishing. https://www.ic3.gov/CSA/2026/260108.pdf. Verified on 2026-11-22.

S48: FBI/CISA. Commercial messaging-account phishing warning. https://www.ic3.gov/PSA/2026/PSA260320. Verified on 2026-11-22.

S49: FBI/CISA. Messaging backup-recovery-key update. https://www.ic3.gov/PSA/2026/PSA260626. Verified on 2026-11-22.

S50: FBI/NSA. Router DNS hijacking and disruption. https://www.ic3.gov/PSA/2026/PSA260407. Verified on 2026-11-22.

S51: NSA. Covert device networks advisory. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4467839/nsa-and-others-release-joint-guidance-addressing-multiple-china-nexus-threat-ac/. Verified on 2026-11-22.

S52: NSA. Distributed exploitation and obfuscation platforms. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4583539/nsa-joins-fbi-in-issuing-warning-about-chinese-hacking-group-qtfy-cyber-activity/. Verified on 2026-11-23.

S53: NSA/FBI. Automated and hands-on intrusion advisory. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4622576/nsa-joins-fbi-and-others-to-provide-guidance-to-mitigate-chinese-government-lin/. Verified on 2026-11-23.

S54: DOJ/FBI. Remote-work fraud operation and employer warning. https://www.justice.gov/opa/pr/justice-department-announces-coordinated-actions-combat-north-korean-remote-it-worker. Verified on 2026-11-22.

S55: DOJ. Domain seizure linked to medical-technology claim. https://www.justice.gov/opa/pr/justice-department-disrupts-iranian-cyber-enabled-psychological-operations. Verified on 2026-11-22.

S56: FBI/CISA. Election and campaign phishing warning. https://www.ic3.gov/PSA/2026/PSA261016. Verified on 2026-11-22.

S57: FBI/CISA/USSS. Extortion and ransomware advisory. https://www.ic3.gov/CSA/2026/261020.pdf. Verified on 2026-11-22.

S58: NSA/CISA. Automatic tank-gauge targeting. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/article/4507204/nsa-joins-cisa-and-partners-to-release-guidance-on-hardening-automatic-tank-gau/. Verified on 2026-11-22.

S59: NSA. PLC reconnaissance and capability development. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4578318/nsa-and-others-release-report-on-active-threats-of-programmable-logic-controlle/. Verified on 2026-11-22.

S60: CISA/FBI/HHS/USDA/DOT. Refrigeration and cold-chain warning. https://www.ic3.gov/CSA/2026/261105.pdf. Verified on 2026-11-22.

S61: DOJ. Malware access-broker infrastructure disruption. https://www.justice.gov/usao-co/pr/gootloader-malware-disrupted-international-cyber-operation. Verified on 2026-11-22.

S62: FBI. Fake-video-meeting theft and software-maintainer targeting. https://www.ic3.gov/CSA/2026/261112.pdf. Verified on 2026-11-23.

S63: DOJ. Virtual-asset restraint and FaceStealer infrastructure action. https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-north-koreas-massive-theft-cryptocurrency. Verified on 2026-11-22.

S64: FBI. Cryptocurrency-exchange theft attribution. https://www.fbi.gov/ (article URL withheld). Verified on 2026-11-22.

S65: NSA. Statement on internal network issues. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4650245/nsa-statement-on-network-issues/. Verified on 2026-11-23.

S66: FBI. OAuth consent phishing warning. https://www.ic3.gov/PSA/2026/PSA260901. Verified on 2026-11-22.

S67: FBI. Device-code phishing-service warning. https://www.ic3.gov/PSA/2026/PSA260521. Verified on 2026-11-22.

S68: FBI. Cyber-enabled cargo diversion warning. https://www.ic3.gov/PSA/2026/PSA260430. Verified on 2026-11-22.

S69: DOJ/FBI. Residential-proxy infrastructure disruption. https://www.justice.gov/usao-edca/pr/authorities-dismantle-global-malicious-proxy-service-deployed-malware-and-defrauded. Verified on 2026-11-22.

S70: DOJ. Malware infrastructure disruption. https://www.justice.gov/usao-cdca/pr/sality-malware-disrupted-international-cyber-takedown. Verified on 2026-11-22.

S71: CISA/FBI. Ransomware affiliate expansion warning. https://content.govdelivery.com/accounts/USDHSCISA/bulletins/4244745. Verified on 2026-11-22.

S72: CISA/FBI/EPA. PLC campaign update. https://content.govdelivery.com/accounts/USDHSCISA/bulletins/4219689. Verified on 2026-11-22.

S73: SecurityLab. Russian-language reporting on the education-platform incident. https://www.securitylab.ru/news/572526.php. Verified on 2026-11-22.

S74: NVD. CVE-2023-50224 record. https://nvd.nist.gov/vuln/detail/CVE-2023-50224. Verified on 2026-11-22.

S75: TP-Link. Legacy-product CVE-2023-50224 remediation. https://www.tp-link.com/us/support/faq/5058/. Verified on 2026-11-22.

S76: DataReportal. Digital 2026: United States of America. https://datareportal.com/reports/digital-2026-united-states-of-america. Verified on 2026-11-22.

S77: HHS. HIPAA Breach Notification Rule overview. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. Verified on 2026-11-22.

S78: Red Hat. Java CVE applicability and processor conditions. https://access.redhat.com/security/cve/cve-2026-114938. Verified on 2026-11-22.

S79: Ubuntu. Java CVE package status and fixed versions. https://ubuntu.com/security/CVE-2026-114938. Verified on 2026-11-23.

S80: RFC Editor. RFC 7489: DMARC. https://www.rfc-editor.org/rfc/rfc7489.html. Verified on 2026-11-22.

S81: RFC Editor. RFC 4034: DNSSEC resource records. https://www.rfc-editor.org/rfc/rfc4034.html. Verified on 2026-11-22.

S82: RFC Editor. RFC 6797: HSTS. https://www.rfc-editor.org/rfc/rfc6797.html. Verified on 2026-11-22.

S83: W3C. Content Security Policy Level 3, October 2026 Working Draft. https://www.w3.org/TR/CSP3/. Verified on 2026-11-22.

S84: An investment-management company, original notice. Cloud-file access with client-account exclusions. https://oag.ca.gov/ (article URL withheld). Verified on 2026-11-22.

S85: A mobility-services company, original notice. Provider credential and connection notice. https://oag.ca.gov/ (article URL withheld). Verified on 2026-11-22.

S86: A medical-device company, original notice. Employee-account file-access notice. https://oag.ca.gov/ (article URL withheld). Verified on 2026-11-22.

S87: A medical-components manufacturer, original notice. February service and data incident with later notification. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-22.

S88: A dental-services company, original notice. Patient-data acquisition update. https://www.sec.gov/ (article URL withheld). Verified on 2026-11-23.

S89: Microsoft Digital Crimes Unit. January infrastructure-service disruption announcement. https://blogs.microsoft.com/on-the-issues/2026/01/14/microsoft-disrupts-cybercrime/. Verified on 2026-11-23.

S90: Netherlands Public Prosecution Service. January arrest notice following an earlier international action. https://www.om.nl/actueel/nieuws/2026/01/12/verdachte-aangehouden-in-onderzoek-naar-cybercriminaliteit. Verified on 2026-11-22.

S91: DOJ. January additional ATM-theft charging notice. https://www.justice.gov/opa/pr/investigation-international-atm-jackpotting-scheme-and-tren-de-aragua-results-additional. Verified on 2026-11-22.

S92: Cyber Centaurs. January ransomware-data recovery technical account. https://cybercentaurs.com/when-ransomware-makes-a-mistake-inside-inc-ransomwares-backup-infrastructure/. Verified on 2026-11-22.

S93: Cyber Centaurs. Earlier November 2025 data-recovery disclosure. https://cybercentaurs.com/infiltration-into-the-inc-ransomware-groups-infrastructure/. Verified on 2026-11-22.

S94: DOJ. Separate January ATM-theft sentencing notice. https://www.justice.gov/usao-sc/pr/venezuelan-nationals-convicted-atm-jackpotting-scheme-be-deported. Verified on 2026-11-22.

S95: BleepingComputer. Limited company response to a communications-data claim. https://www.bleepingcomputer.com/ (article URL withheld). Verified on 2026-11-23.

S96: SecurityWeek. Follow-up company statement on business-customer sales tools. https://www.securityweek.com/ (article URL withheld). Verified on 2026-11-22.

S97: DOJ, US Attorney District of Alaska. March four-botnet infrastructure disruption. https://www.justice.gov/usao-ak/pr/authorities-disrupt-worlds-largest-iot-ddos-botnets-responsible-record-breaking-attacks. Verified on 2026-11-22.

S98: DOJ, US Attorney District of Alaska. May botnet complaint and related service-seizure follow-up. https://www.justice.gov/usao-ak/pr/canadian-man-arrested-international-authorities-charged-administrating-kimwolf-ddos. Verified on 2026-11-22.

S99: BleepingComputer. January cybercrime-forum seizure-banner reporting. https://www.bleepingcomputer.com/news/security/fbi-seizes-ramp-cybercrime-forum-used-by-ransomware-gangs/. Verified on 2026-11-22.

S100: Ars Technica. Independent January seizure-banner reporting. https://arstechnica.com/security/2026/01/site-catering-to-online-criminals-has-been-seized-by-the-fbi/. Verified on 2026-11-22.

S101: BleepingComputer. March company confirmation of limited legacy-server access. https://www.bleepingcomputer.com/ (article URL withheld). Verified on 2026-11-22.

S102: CRN. Independent company response on legacy information and service scope. https://www.crn.com/ (article URL withheld). Verified on 2026-11-22.

S103: SecurityWeek. Updated company response on a legal-information provider incident. https://www.securityweek.com/ (article URL withheld). Verified on 2026-11-22.

S104: CISA. April agency bulletin on firewall persistence and federal guidance. https://content.govdelivery.com/accounts/USDHSCISA/bulletins/414353b. Verified on 2026-11-22.

S105: Cisco PSIRT. Current vendor advisory on perimeter-device persistence and recovery. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03. Verified on 2026-11-22.

S106: Cisco Talos. April vendor analysis of a firewall backdoor. https://blog.talosintelligence.com/uat-4356-firestarter/. Verified on 2026-11-22.

S107: The Register. November financial-provider responses on supplier incidents. https://www.theregister.com/ (article URL withheld). Verified on 2026-11-22.

S108: ABC News. November company statements on marketing and benefit-program information. https://abcnews.com/ (article URL withheld). Verified on 2026-11-22.

S109: DTN. Dated federal cyberthreat acknowledgement and recovery expectation. https://www.dtnpf.com/agriculture/web/ag/columns/washington-insider/article/2026/11/19/usda-loan-software-systems-face-amid. Verified on 2026-11-23.

S110: Nextgov/FCW. Federal application outages and reporter-reviewed incident documents. https://www.nextgov.com/cybersecurity/2026/11/usda-grapples-security-breach-it-staff-take-multiple-systems-offline/417350/. Verified on 2026-11-22.

S111: ABC News / Good Morning America. Reporting on federal application disruption and official remarks. https://www.goodmorningamerica.com/food/story/new-government-report-sparks-concern-potential-cyberattack-us-138316014. Verified on 2026-11-22.

Appendix D. Terms used in the report

Term	Plain meaning in this report
Actor claim	A statement by a persona or group whose asserted outcome is not independently established
Advertisement	An observed offer; not proof that the offered item is authentic or was delivered
Application consent	A permission granted to an application to access specified account resources
Atlas	Brandefense's exposure assessment product; this edition publishes the selected portfolio's national headline
Business impact	The effect on a defined service, its users or the organisation's ability to operate
Country label	A source association with a country; not proof of targeting, residence or incident location
Credential	Information used to authenticate an account; a historical record does not establish current usability
CSP	Content Security Policy, a browser policy controlling permitted content and execution sources
Data acquisition	Obtaining information, as stated by the source; distinct from its later use or public release
Device-code authentication	A sign-in flow that lets a user authorise an application through a separate interaction
Disclosure family	Related original notices and updates about one source-supported event or provider incident
DKIM	An email-signing mechanism; observing a key does not prove every message is signed
DMARC	A domain policy using email authentication and alignment to guide handling of messages
DNSSEC delegation	A DNS trust relationship indicated by a DS record; one record does not validate the entire chain
Extortion listing	A publication asserting victim or data exposure; not independent incident confirmation
HSTS	A browser instruction to use HTTPS for the covered host
Item 1.05	The SEC form item for a material cybersecurity incident, subject to its defined requirements
Materiality	A legal assessment in its relevant disclosure context; distinct from initial detection or an outage

Term	Plain meaning in this report
OAuth	A framework through which an application can receive limited access to account resources
Operating estate	The selected primary-domain service boundary used in the portfolio; not necessarily one legal entity
Original notice	The affected organisation's or authority's own published account
Passive observation	A dated observation of public service information and controls, rather than proof of intrusion
Protected health information	Health information within the relevant US privacy rule's defined scope
Recovery	Restoring a usable service and reconciling its work, with validation by the responsible business owner
Session	An authenticated interaction whose validity may need separate review from the account password
SPF	A domain record describing authorised mail senders; coverage still needs validation
Supplier dependency	A service or permission on which an organisation relies for data access or operations
Technique reference	A source-backed description supporting a defensive review; not a detection at a selected estate

Technical-control definitions follow the cited standards. Legal terms retain the scope of their primary rules and are not universal reporting triggers [S35][S37][S80][S81][S82][S83].

About this report

Odin by Brandefense presents dated threat observations, original disclosures and explicit analytical judgements for defenders. This edition uses US-relevant evidence to support identity validation, supplier governance, accurate notification and tested continuity.

The authors take no political position on administrations, parties, elections, government staffing, budgets, trade, immigration or foreign relations. State-related attributions belong to the cited sources. The report does not derive political conclusions from threat claims, source language or the timing of a publication.

Brandefense Blackhole, Ransompedia and Atlas are distinct public products or evidence contexts. Their observations answer different questions. A post or listing does not independently confirm the condition of a selected estate, and a passive control observation does not establish its exposure totals.

The practical outcome is a documented decision: validate a relevant account, constrain a supplier permission, correct a confirmed service issue, meet an applicable notification duty or demonstrate recovery. Each decision needs an owner and evidence supporting completion.

For a discussion of the relevant Brandefense services, use the Brandefense demo request page.

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