BRANDEFENSE COUNTRY REPORT · UNITED KINGDOM 2026

Brandefense United Kingdom Cyber Threat Landscape Report 2026

Identity abuse, supplier exposure and service continuity

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

116 of 250
selected estates had a credential listed for sale when checked

12,071
distinct retained posts, a partial population rather than a national count

12
original-source incident families of UK relevance, with separate date and scope limits

80
group labels associated with UK extortion listings

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Digital services and the national threat context	10
03	National exposure: the selected organisation sample	14
04	What the retained dark-web material shows	22
05	Incident disclosures and targeting by sector	37
06	Hacktivism, DDoS and operational disruption	48
07	Threat actors and supported relationships	52
08	The fraud economy: identities, accounts and payment decisions	63
09	Banking and financial services	69
10	Regulatory response and reporting decisions	74
11	Outlook and conditions that would change it	79
12	A 30/60/90-day action plan	83
	Appendices	89
A	Appendix A. Sources, scope and confidence	90
B	Appendix B. Public evidence-card register	94
C	Appendix C. Sources	95
D	Appendix D. Glossary	98
	About this report	100

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.

AI-assisted research and drafting. Observed material, actor claims, original disclosures and analyst judgements are distinguished throughout. The snapshot reflects material available when checked on the cut-off day.

Identity abuse, customer-data disclosures and extortion claims make validation, supplier access and recoverable services the UK's practical priorities.

383

UK-labelled extortion listings, with incident outcomes unverified

116 / 250

selected estates with a current credential listing

12

original-source incident families of UK relevance, with date limits

18

extortion listings dated 9–22 November in the available snapshot

Contents and reading routes

The twelve chapters move from leadership decisions to evidence, then to a programme with accountable owners.

Chapter	Question	First reader
1. Executive summary	What should leaders decide first?	Board and CISO
2. Digital context	Which national features matter for security planning?	Security leadership
3. National exposure	What can the selected domain sample establish?	Infrastructure and identity
4. Dark-web evidence	What is advertised, and what remains unverified?	Threat intelligence
5. Incident disclosures	What did original notices establish by sector?	Service and sector owners
6. Hacktivism and disruption	What separates a claim from demonstrated impact?	Operations and communications
7. Threat actors	Which attributions and relationships have evidence?	SOC and threat intelligence
8. Fraud economy	How do identities, accounts and payments connect?	Fraud and customer teams
9. Banking	Which financial-service decisions need joint ownership?	Financial security leaders
10. Regulation	Which duties apply, and which developments are proposals?	Legal and compliance
11. Outlook	What would change the assessment?	Leadership and planning
12. Action plan	Who acts, and what demonstrates completion?	All owners

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, record or measurement is held. **Claimed** means a poster or listing asserts something. **Officially disclosed** means an organisation or authority published the stated account. An analyst judgement explains an implication without supplying missing proof.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which decisions follow from the UK 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

Extortion claims, customer-data disclosures and identity abuse require complementary responses. The available snapshot contains 383 UK-labelled extortion listings and original notices for 12 UK-relevant incident families. 116 of 250 selected estates have current credential listings, and the national Atlas headline is 61. Recent official material adds health-data access concerns and a financial cyber-resilience consultation. Validate credible account signals, constrain supplier permissions, prepare accurate notices and demonstrate recovery of important services.

This report combines retained Brandefense Blackhole posts, Ransompedia listing records, passive observations and source-checked public reporting. The populations remain separate. Country-tagged posts, retained case material and confirmed disclosures describe different populations. None supplies an attack census or an estimate of national financial loss [S1][S2][S3][S4].

1. Extortion claims justify continuity investment across the year. Ransompedia records 383 accepted listings with the UK country label in the window, compared with 288 in all of 2025. Each of the four peer countries also exceeds its full-year 2025 total within the partial 2026 period. This is not a matched-period growth rate or a national risk ranking. The UK records use 80 group labels; Qilin contributes 46 listings [S3].

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

2. Observable email policies do not establish complete protection. A DMARC reject or quarantine policy was observed for 205 of 250 assessed estates (82.0%). Monitoring policies were observed for 38, while no policy was observed for 7. The sample is purposive, and the results do not establish message-level enforcement or the security of every service. The national Atlas headline is 61; identity-exposure observations need their own validation [S2].

3. Original disclosures show why system and supplier boundaries matter. The 12 incident families include public-service portals, transport customer services, retail communications, education systems and suppliers. Their dates and confirmed scopes differ. They do not establish a single common entry route. The detailed cases preserve those boundaries rather than treating every disclosure as an institution-wide intrusion [S31][S32][S33][S34][S35][S38].

4. Underground material needs proposition-level validation. The retained offers include support-tenant access, financial leads, a multi-country connectivity claim and an older-labelled issue-tracker archive. A criminal offer can establish that advertising occurred. It does not independently establish current access, data authenticity, a completed sale or the number of newly affected people [S1].

5. Recent official material sharpens existing resilience decisions. The final fortnight contains eighteen extortion listings in this snapshot. ICO's 12 November health warning concerns more than 300 assessed access reports covering January to mid-October. The 19 November financial consultation clarifies existing requirements and proposes no new rules. These are different developments with different units and periods [S3][S19][S20][S30].

Four decisions for leaders

1. **Give identity validation an accountable owner.** Route credible account and access signals to identity operations and incident response. Record the match, current account status, relevant activity and escalation decision before choosing a disruptive response.
1. **Treat supplier permissions as a service dependency.** Identify which providers can access customer information, support privileged accounts or restore important services. Test the initial-notification route and emergency access restrictions with each critical provider.
1. **Prepare factual customer and regulator communications.** Have privacy, legal and communications teams work from one incident record. Distinguish known data fields, possible impact and unverified actor figures, while preserving the applicable reporting triggers.
1. **Prove recovery with business owners.** Restore an important service using protected data and separate recovery access. Measure integrity, customer readiness and business sign-off. Test availability mitigation where public access is essential.

The year in numbers

These figures describe different populations and must not be added together.

383

Accepted UK-labelled extortion listings in the 2026 window [S3]

WHAT IT IS NOT

Confirmed intrusions, distinct organisations or total UK ransomware activity

288

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

WHAT IT IS NOT

A matched-duration baseline for the partial 2026 window

80

Group labels associated with the UK window listings [S3]

WHAT IT IS NOT

Eighty independently verified operating teams

18

Listings dated 9–22 November in the available snapshot [S3]

WHAT IT IS NOT

Confirmed incidents occurring in that fortnight

250 / 250

Selected domain estates / estates with passive observations [S2]

WHAT IT IS NOT

A representative national sample or a complete corporate-group assessment

205 of 250

Estates with an observed reject or quarantine DMARC policy [S2]

WHAT IT IS NOT

Proof of complete enforcement across every message stream

12

Original-source incident families of UK relevance [S31][S32][S33][S34][S35][S36][S37][S38][S40][S42][S46][S47][S48]

WHAT IT IS NOT

A count of distinct UK victims or attacks starting in 2026

12,071

Distinct retained posts supporting this edition [S1]

WHAT IT IS NOT

The complete country-tagged population or unique criminal offers

116 of 250

Selected estates with a current credential listing [S2]

WHAT IT IS NOT

Confirmed incidents or completed sales

61 / 100

National Atlas headline for the selected portfolio [S2]

WHAT IT IS NOT

A national prevalence estimate or probability of intrusion

KEY TAKEAWAYS

01

Keep listings, posts, control observations and official disclosures separate.

02

Validate accounts and supplier permissions before inferring a wider incident.

03

Fund service recovery and accurate notification with named owners.

Report map

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

Board and executives	Which service risks justify action and investment?	01 05 11 12
CISO and security leads	Which controls and 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 are exposed?	04 05 08 09
Legal and communications	What can be said, and which duties have started?	05 06 10 12

01 Summary
Decisions and the evidence supporting them

02 Context
Digital-service dependencies and source boundaries

03 Exposure
National Atlas headline, identity exposure and public controls

04 Dark web
Advertisements, cases and their unresolved propositions

05 Incidents
Original disclosures and date-qualified sector examples

06 Disruption
Claims, availability and operational-system risk

07 Actors
Supported attribution, relationships and techniques

08 Fraud
Account, identity and payment opportunities

09 Banking
Financial-service scope and joint decisions

10 Regulation
Existing duties and proposed developments

11 Outlook
Conditional scenarios and assessment-change signals

12 Actions
Owners, timing and demonstrable completion

CHAPTER 02

Digital services and the national threat context

02

THIS CHAPTER ANSWERS

Which features of the United Kingdom change a defender's priorities?

97.8%

internet penetration in DataReportal's late-2025 baseline

2.1 A connected population, with a dated baseline 11

2.2 Shared services create dependencies across organisational boundaries 11

2.3 Public warnings describe several different threat populations 12

2.4 An older survey is context, not a 2026 incident total 12

2.5 The November warning concerns resilience as well as AI 12

CHAPTER 02

Digital services and the national threat context

IN SHORT

The UK combines extensive digital adoption with shared public services, international suppliers and a large financial sector. Those features make identity, supplier access and service continuity useful planning priorities. Official warnings address DDoS, exposed operational systems and activity attributed to state-linked groups. Their coverage differs from the country posts and extortion listings in this report. Map the services, identities and suppliers that your organisation actually depends on.

2.1 A connected population, with a dated baseline

DataReportal's Digital 2026 report describes late 2025, rather than measurements taken during this report's window. It gives 68.1 million internet users and 97.8% internet penetration. It also gives 99.3 million cellular connections, equivalent to 143% of the population. Connections are not unique subscribers, and some do not include internet access [S21].

The security implication is a planning judgement. Customer identities can appear across public services, banking, transport, shopping and communications. A disclosure in one service can make an impersonation attempt in another more convincing. It does not establish that the second service lost data or that a particular disclosed record was used in fraud.

An organisation should therefore map the customer journey beyond its own login page. Contact-centre verification, account recovery, new-device enrolment and payment changes all make decisions about identity. Improving one stage while leaving another dependent on easily obtained personal details can leave a usable route around the stronger control.

2.2 Shared services create dependencies across organisational boundaries

The selected domain estates cover central and devolved public services, councils, universities, health services and commercial organisations. Their inclusion is a research choice. It does not imply a weakness, an incident or a place in an official ranking [S2].

The government's November Bill factsheet identifies managed services, data centres and critical suppliers as areas for proposed regulatory expansion. It explains that suppliers can have substantial access to the systems of their customers [S16]. That rationale supports dependency mapping. It does not prove that suppliers caused the incidents examined in Chapter 5.

For each important service, identify the provider that controls authentication, the provider that stores the data and the provider that can restore operations. These can be different organisations. Record who can suspend access, export records, change recovery details or open a remote support session. A contract owner alone may not know those technical permissions.

Shared ownership also affects communications. A supplier may be investigating while its customers receive questions from employees, customers or regulators. A useful arrangement allows an early factual notice before every forensic question has been settled. Legal teams should agree its content and route before an incident.

2.3 Public warnings describe several different threat populations

NCSC's January alert describes frequent DDoS attempts against UK local government by NoName057(16). Its April router advisory describes activity continuing from 2024 into 2026 and attributes it to APT28. Another April publication addresses covert device networks attributed by the source to China-linked actors [S6][S7][S8].

These are official assessments with different scopes. They are not counts of newly affected UK organisations in 2026. A global advisory may be relevant to UK defenders without identifying a UK victim. Nor does a common technical control establish a relationship between the groups discussed.

This report takes no position on government decisions, territorial questions, monarchy, elections or foreign policy. State links and political motives are stated as the source's assessments or the actor's claims. They are not conclusions derived from language, a country tag or an actor's chosen name.

2.4 An older survey is context, not a 2026 incident total

The government's Cyber Security Breaches Survey 2025 found that 43% of businesses and 30% of charities identified a breach or attack in the preceding twelve months. Its fieldwork took place between August and December 2024. Among organisations identifying such activity, phishing was reported by 85% of businesses and 86% of charities [S22].

Those figures describe survey responses and an earlier period. They cannot be combined with the 383 extortion listings in this report. They also include activity broader than confirmed data theft. Use them to understand the importance of routine identity controls, rather than as an estimate of 2026 ransomware prevalence.

Reporting, collection and disclosure all affect visibility. A highly publicised incident may attract many posts, while a serious private incident may generate none. This report consequently avoids a single national attack total or a numerical probability of intrusion.

2.5 The November warning concerns resilience as well as AI

On 3 November, NCSC warned that AI-powered malware was highly likely to feature in a ransomware attack on UK critical infrastructure by 2028. This is NCSC's forward assessment, not an observed outcome in this report. The accompanying message called for foundational security investment and reduced unnecessary internet connectivity [S5].

The practical response does not depend on predicting a particular AI tool. Maintain an accurate inventory, shorten the time needed to assess a critical patch, remove obsolete access and prove recovery. AI may change speed or volume. Those controls address the underlying opportunity for harm.

KEY TAKEAWAYS

01

Digital-adoption figures carry their late-2025 measurement date.

02

Official advisories, survey responses and extortion listings describe different populations.

03

Map identity and supplier dependencies around the services that must keep operating.

CHAPTER 03

National exposure: the selected organisation sample

03

THIS CHAPTER ANSWERS

What do the selected UK estates reveal about identity exposure and defensive priorities?

116 of 250

selected estates had a credential listed for sale when checked

3.1 Universe card 15
3.2 National Atlas headline and sector signals 16
3.3 Device and credential associations 17
3.4 Documents, mentions and listing history 18
3.5 Email authentication 19
3.6 DNS delegation, certificates and web controls 20
3.7 Turn observations into an owner review 21

CHAPTER 03

National exposure: the selected organisation sample

IN SHORT

116 of 250 selected estates had a credential listed for sale when checked. The national Atlas headline is 61 out of 100. The portfolio records at least 751,712 device associations and 38,839,873 credential-record associations. These overlapping observations do not establish confirmed intrusions or national prevalence. Validate current listings, investigate relevant employee-device associations and assign recovery checks to service owners.

3.1 Universe card

Item	Definition
Population	250 selected UK-relevant public and private domain estates across twelve sectors
Selection	Purposive selection for public-service, financial, infrastructure or market relevance; not a random sample or official ranking
Unit	A selected primary domain estate; related businesses can belong to one corporate group
Exposure snapshot	21 November 2026 UTC; device, credential, document and market observations are cumulative records held on that date
Mention context	Previous 365 days through 22 November 2026; a mention does not establish targeting or an incident
Passive snapshot	22 November 2026; 250 assessed estates; web-control results available for 189 estates
Publication	National Atlas headline and anonymous sector signal counts; no sector or organisation ratings
Interpretation	Overlapping records and associations, rather than unique people, active accounts or confirmed intrusions

Shared government domains and multinational group domains require particular care. The observation belongs to the chosen estate. It cannot be assigned automatically to every public body, subsidiary or customer using related services [S2].

The portfolio includes prominent services in twelve sectors. Each published sector contains at least five selected estates. These denominators describe the sample; they do not establish representative coverage of the sector's employers, users or economic output.

3.2 National Atlas headline and sector signals

116 of 250 estates had a credential listed for sale when checked. The national Atlas headline for the selected portfolio is 61 on a scale from 0 to 100. Higher values mean greater observed exposure. It describes this portfolio, rather than every UK organisation [S2].

116 of 250

selected estates with a current credential listing

61 / 100

national Atlas headline for the selected portfolio

29,325

employee-device associations, requiring ownership validation

Current listings are advertisements associated with a selected domain. They do not establish a completed sale, a tested credential or active unauthorised access. Account validation is necessary before deciding whether a listing concerns a current incident.

The table reports signal counts by sector. Employee-device and document columns count associations; the credential-listing column counts estates. These are different units and are not added together.

Sector	Estates	Estates with current credential listings	Employee devices	Documents
Government	40	8	621	1,819
Education	30	24	9,316	1,372
Banking & finance	30	15	405	245
Energy & utilities	25	12	1,335	742
Transport & logistics	25	14	555	195
Retail & consumer	25	18	4,239	622
Manufacturing & industry	20	4	491	283
Technology & telecom	20	9	1,317	320
Healthcare	15	4	928	308
Insurance	10	1	84	65

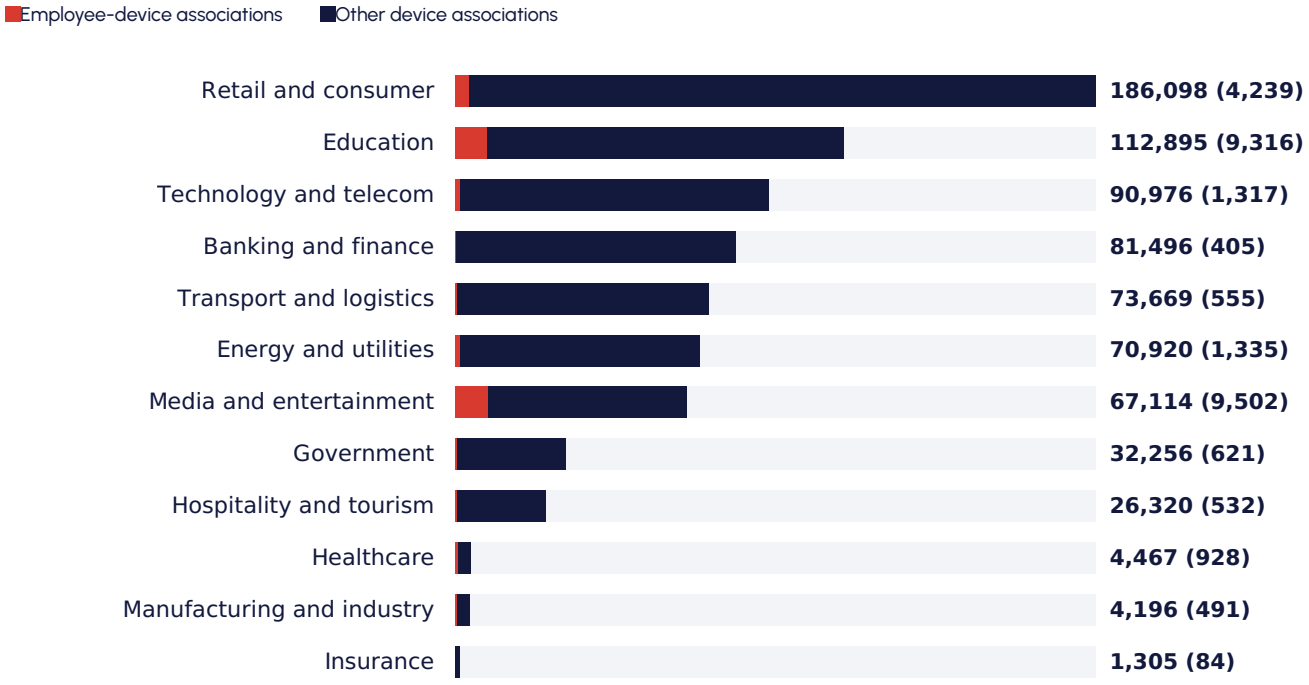
Sector	Estates	Estates with current credential listings	Employee devices	Documents
Media & entertainment	5	4	9,502	729
Hospitality & tourism	5	3	532	101
Total	250	116	29,325	6,801

The estate denominator and the observation date remain essential. A sector with more listings has more dated validation leads in this sample. Its listing share is not an incident rate or a numerical estimate of the likelihood of intrusion.

3.3 Device and credential associations

The selected portfolio records at least 751,712 device associations, including 29,325 employee-device associations. Credential-record associations total 38,839,873 across 248 selected estates. Associations can overlap across domains, sources and people [S2].

Retail and consumer services carry the largest device-association total in this portfolio



Source: Brandefense exposure associations for 250 selected estates, 21 November 2026. Cumulative, overlapping associations; not confirmed intrusions or national prevalence [S2].

Sector	Devices, at least	Employee devices	Credential records
Government	32,256	621	780,581
Education	112,895	9,316	6,036,057

Sector	Devices, at least	Employee devices	Credential records
Banking & finance	81,496	405	376,806
Energy & utilities	70,920	1,335	1,650,002
Transport & logistics	73,669	555	552,911
Retail & consumer	186,098	4,239	1,494,676
Manufacturing & industry	4,196	491	848,106
Technology & telecom	90,976	1,317	5,110,143
Healthcare	4,467	928	1,051,059
Insurance	1,305	84	115,854
Media & entertainment	67,114	9,502	20,618,162
Hospitality & tourism	26,320	532	205,516
Total	751,712	29,325	38,839,873

Employee-device associations are included in the device view and must not be added to it. Device totals are lower bounds. A device associated with a consumer-facing service is not automatically an endpoint operated by that service.

Credential records comprise 14,930,407 breach-database records, 4,991,853 stealer-log lines and 18,917,613 combolist entries. Historical, repeated and multi-domain records can all contribute. These figures do not count unique people or currently usable accounts.

The media and entertainment row contains 20,618,162 credential-record associations. That is 53.1% of the portfolio total. Global consumer services and historical account use can influence such totals; this concentration does not establish sector-wide compromise.

Retail and consumer services account for at least 186,098 device associations. Customer use and domain context affect interpretation. Fraud and account-protection teams may own a customer-device signal, while endpoint and identity teams own a corroborated employee-device signal.

For a relevant record, establish whether the account remains active, whether its secret has changed and whether associated sessions or recovery routes remained usable. Preserve evidence before closing the case. A password reset alone does not demonstrate complete containment.

3.4 Documents, mentions and listing history

Document associations total 6,801 across 217 estates. A document association does not establish that its content is sensitive, was obtained without authorisation or remains accessible. The information owner should establish those facts before describing a disclosure [S2].

Listing history concerns 111 selected estates. It is a separate historical observation, rather than evidence of completed sales or continued access. The current-listing and historical populations can overlap and must not be summed as distinct organisations.

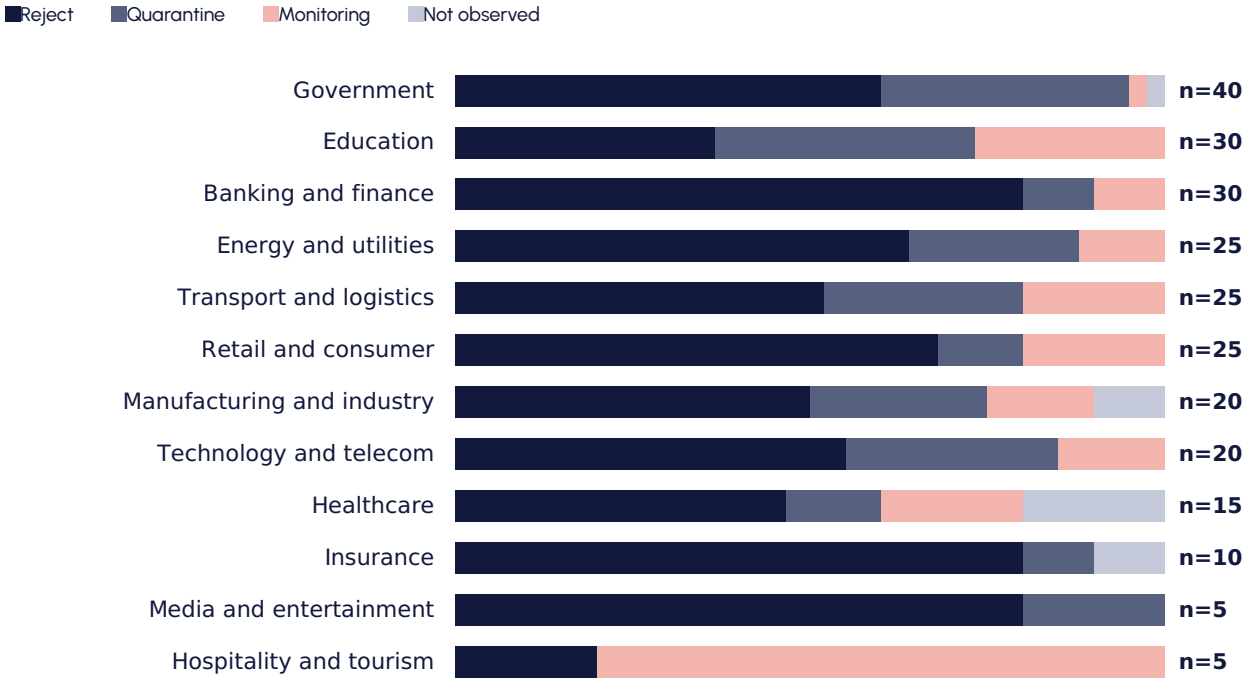
Dark-chat mentions appear for 112 estates, and dark-web mentions for 135. These counts use the previous 365 days through 22 November. They count estates with a mention, rather than confirmed targets or incidents.

Brand and lookalike references require separate ownership checks. Similar names can belong to unrelated lawful services. No candidate-domain observation is treated here as verified phishing, and no domain-level identifier is published.

3.5 Email authentication

A DMARC reject or quarantine policy was observed for 205 of 250 assessed estates (82.0%). Monitoring-only policies were observed for 38; no policy was observed for 7. These are policy observations, not a finding of complete message-level enforcement [S2].

Email-policy observations vary across the selected sectors



Source: public technical observations, 22 November 2026. Policies observed do not establish message-level enforcement; denominators are the assessed estates [S2].

Observation	Estates	Denominator	Interpretation
DMARC reject policy	146	250	Published policy label
DMARC quarantine policy	59	250	Published policy label

Observation	Estates	Denominator	Interpretation
DMARC monitoring policy	38	250	Monitoring rather than requested rejection or quarantine
DMARC not observed	7	250	Requires owner validation
SPF record observed	232	250	Record presence, not complete sender coverage
DKIM key observed	200	250	Key observed; signing coverage not established
Mail exchange observed	236	250	A mail-routing observation

An SPF record does not establish that every authorised service is listed correctly. A DKIM key observation does not establish that every outgoing message is signed. A key not observed in this assessment is not proof that DKIM is absent.

The messaging owner should validate actual mail flows and sender coverage before changing policy. Domains used for transactional mail, staff mail and little or no outgoing mail can require different decisions. Check delivery after an approved change.

3.6 DNS delegation, certificates and web controls

Certificates validated for 239 of 250 assessed estates. 4 did not validate, and 7 had an unavailable certificate result. Web-control results were available for 189 estates. The remaining 61 are not classified as missing web controls [S2].

Observation	Estates	Denominator	Interpretation
DS record observed	26	250	Delegation record, not complete DNSSEC validation
Certificate validated	239	250	Time-specific public certificate observation
Certificate did not validate	4	250	Owner should check the intended service
Certificate result unavailable	7	250	Not classified as a certificate defect
Web-control results available	189	250	Coverage of the available web-control results
HSTS header observed	151	189	Observed response, including intermediaries
Content Security Policy (CSP) header observed	93	189	Observed control, not complete application protection

A DS record is evidence of a DNSSEC delegation record, rather than a verified end-to-end validation chain. A certificate observation is time-specific and service-specific. Neither establishes application security.

Content Security Policy (CSP) restricts the content sources a browser may load [S51]. An observed header does not establish complete application protection.

Web headers can be set by an application, a hosting platform or an intermediary. Evaluate their presence against the service's requirements. An unavailable response is not silently classified as a missing control.

3.7 Turn observations into an owner review

Signal	First validation	Action trigger	Closure evidence
Current credential listing	Match an active account and relevant service	Corroborated exposure or unauthorised activity	Recorded disposition, session review and relevant remediation
Employee-device association	Confirm endpoint ownership and account relationship	Evidence of an affected managed endpoint	Endpoint investigation and identity recovery checks
Document association	Establish sensitivity and authorised availability	Owner confirms an unintended disclosure	Access correction and privacy assessment
Unexpected email or web observation	Check the actual service and intended configuration	Owner confirms an unintended gap	Approved change with successful validation

KEY TAKEAWAYS

01

The national Atlas headline describes a selected portfolio, not national prevalence.

02

Listings, devices, credentials and documents retain their distinct units and limits.

03

Validate account relevance, ownership and current activity before remediation.

CHAPTER 04

What the retained dark-web material shows

THIS CHAPTER ANSWERS

What do UK-labelled offers establish, and which claims deserve an organisation's time?

12,071

distinct retained posts, a partial population rather than a national count

4.1 Universe card 23
4.2 Composition of the retained material 23
4.3 Specific offers with a UK connection 25
4.4 Six detailed cases 27
4.5 Other offers and the freshness question 32
4.6 Replies can challenge a claim without settling it 35
4.7 Extortion listing dates are a separate population 35
4.8 What is not established 36

CHAPTER 04

What the retained dark-web material shows

IN SHORT

The retained material includes administrative-access offers, customer-data advertisements, financial leads, business accounts and older-labelled archives. The useful distinction is between an offer and the underlying proposition it asserts. A UK title can cover a multinational dataset, and a recent post can circulate older material. Six cases below preserve those limits. Validate service ownership, current account relevance and data provenance before escalating an advertisement into an incident account.

4.1 Universe card

Item	Definition
Population	12,071 distinct retained posts with dates in the requested window [S1]
Coverage	Forum-heavy material and partial chat coverage; not a complete national post population
Unit	A post, rather than a unique offer, seller, incident or affected person
Country relevance	A UK reference can describe a claimed target, a customer subset, a company document, a product or a wider discussion
Status	Contents are observed advertisements or statements; authenticity, access and completed transactions need separate evidence
Time	Post dates describe publication; advertised data may concern an earlier period

The retained population contains material that is not a UK-specific incident. The report selects cases for a clearly stated UK connection and records exclusions separately. It does not infer targeting merely from a country label.

4.2 Composition of the retained material

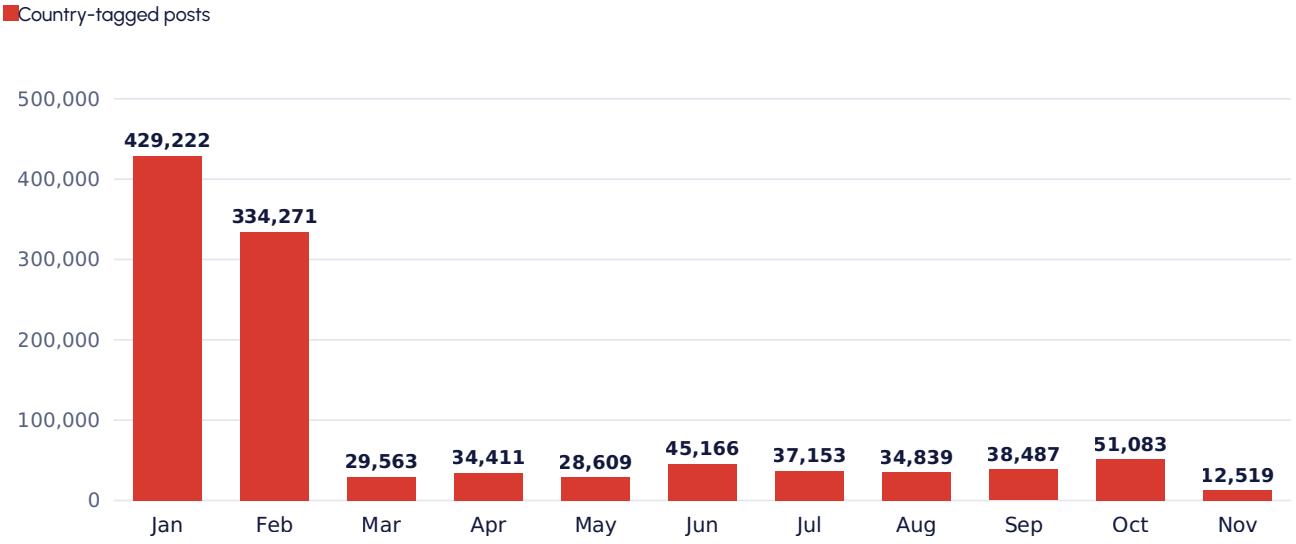
The table describes this retained population. It is not a platform or language distribution for all UK cybercrime.

Dimension	Category	Retained posts	Limit
Platform	Forum	10,649	Retained posts, not national platform prevalence
Platform	Telegram	1,422	Partial chat coverage
Language	English	10,675	Recorded language; labels may overlap
Language	Russian	1,209	Language does not establish nationality
Language	Turkish	50	Includes account and company-document offers

The composition reflects the available evidence. It cannot support a claim that one platform accounts for the same share of UK criminal activity. Language also does not establish an operator's nationality, location or affiliation.

The country-tagged source population contains 1,075,323 posts in the observation snapshot. It is separate from the 12,071 distinct retained posts used for case analysis. Neither population is a count of UK criminal incidents.

Country-tagged monthly post volumes describe source visibility, not confirmed incident frequency



Source: Brandefense Blackhole, country-tagged posts, 1 January–22 November 2026; November partial. Separate from the 12,071 retained posts; not confirmed incidents [S1].

Month	Posts tagged
2026-01	429,222
2026-02	334,271
2026-03	29,563

Month	Posts tagged
2026-04	34,411
2026-05	28,609
2026-06	45,166
2026-07	37,153
2026-08	34,839
2026-09	38,487
2026-10	51,083
2026-11	12,519

November is a partial month. Country tags can reflect advertising, commentary or a passing reference. Source coverage can change, so monthly differences do not establish changes in underlying criminal activity. No national crime-family share is inferred. Advertisements, commentary and relays can coexist in the same retained material. A defensible case therefore needs its own source and scope assessment.

4.3 Specific offers with a UK connection

The six offers below are case-level observations. None is promoted to an independently verified incident on the strength of a post alone.

Post date	Claimed source or product	Observed offer	Status
10 November	A support-platform tenant	Administrative access and member/contact records	Access and ownership unverified; Case A
5 October	A transport operator	Customer and booking-related information	Event chronology and dataset identity unestablished; Case B
16 November	Financial-application records	Identity and financial-circumstance fields	Provenance and currency unverified; Case C
3 October	Investment-user information	A UK-labelled contact dataset with several advertised totals	Population and source unverified; Case D
13 November	A travel-connectivity service	Customer and partner/provisioning records, including a claimed UK subset	Multi-country claim; Case E
23 August	A manufacturer issue tracker	An archive carrying a January 2025 label	A 2026 circulation post, not proof of a fresh incident; Case F

Evidence card B01 — 10 Nov 2026

Forum seller | Forum | Forum | English

ORIGINAL

[Paraphrase: an advertiser offers administrative access to a customer-support tenant and member records attributed to a UK service operator.]

TRANSLATION

[Paraphrase, not a verbatim quote.]

Held
An advert describing a support tenant and three record categories.

Not established
Administrative access, record totals, ownership, any intrusion or completed sale.

Evidence card B02 — 5 Oct 2026

Forum seller | Forum | Forum | English

ORIGINAL

[Paraphrase: an advertiser offers customer and booking information attributed to a UK transport operator; precise counts, locations, field detail and contacts withheld.]

TRANSLATION

[Paraphrase, not a verbatim quote.]

Held
A dated data offer with a seller-stated leak date.

Not established
Authenticity, intrusion date, extent, entry route or a confirmed affected population.

Evidence card B05 — 3 Oct 2026

Data seller | Forum | Forum | English

ORIGINAL

Data fields: Name, Number, City, Address, Email, Gender, Date of Birth

TRANSLATION

Source English; victim and contact material omitted.

Held
The advertised field list of a UK-labelled investment-data offer.

Not established
The origin, record counts, UK residence or any completed sale.

Evidence card B06 — 16 Nov 2026

Data seller | Forum | Forum | English

ORIGINAL

[Paraphrase: a seller advertises a UK financial-application dataset containing identity, income, household and debt-related fields. Record values and identifying details removed.]

TRANSLATION

[Paraphrase, not a verbatim quote.]

Held
A financial-application-style offer with sample dates older than the post.

Not established
Data controller, freshness, a 2026 intrusion, valid records or unique people.

4.4 Six detailed cases

A

CASE A

Administrative access advertised at a support tenant

Evidence card B01 | 10 Nov 2026 | Forum | Support services

Unverified claim

CLAIM	A 10 November advertiser offered administrative access to a customer-support tenant and described member-contact, support-ticket and case information. The post presents a UK service connection [S1].
CHRONOLOGY	A 4 January user-dataset offer uses similar service branding. The 10 November post concerns support-tenant access. No common dataset, account or incident is established. Neither post is an organisation statement.
WHAT IS HELD	An advertisement describing a support tenant and several data categories. The advertiser's description of the operator and its service relationship is not independently verified.
ALTERNATIVES	Genuine access to a third-party tenant; a misdescribed customer environment; stale exports; a fabricated offer.
LIMITS	The post does not establish administrative access, the claimed record population, possession of the data or a sale. A community-facing brand is not automatically the tenant operator.
RESPONSE	Identify support and relationship-management tenants operated by partners. Review administrator sign-ins, exports, recovery permissions and notification contacts, escalating when internal evidence corroborates the signal.

Bottom line

Validate tenant ownership and administrative access before escalating the advert.

B

CASE B

A transport-data offer and separate relays

Evidence card B02 | 5 Oct 2026 | Forum | Transport

Unverified claim

CLAIM	An October post offered transport customer and booking-related information. Separate August news-style relays described an alleged incident and attributed it to an extortion group [S1].

CHRONOLOGY	The advert and relays carry different event-date references. A coherent incident chronology and a common underlying dataset are not established by these records.
WHAT IS HELD	A data offer and third-party repetitions of claims. A relay is not an original statement from the organisation or independent authentication of the seller's account.
ALTERNATIVES	An earlier dataset advertised again; separate datasets; inaccurate relay reporting; an inflated or fabricated offer.
LIMITS	No link is asserted to any named confirmed case in Chapter 5. The posts do not establish the access route, the time of intrusion or the number of affected people.
RESPONSE	Review customer-marketing, booking and registration providers. If records are internally corroborated, prepare warnings about messages that quote genuine journey or booking details.

Bottom line

An offer and its relays do not establish a common dataset or incident chronology.

Evidence card B03 — 30 Aug 2026

News relay | Forum | Forum | Russian

ORIGINAL

[Пересказ: канал пересказывает заявление группы вымогателей о данных британского транспортного оператора. Названия, объём и детали предполагаемого доступа удалены.]

TRANSLATION

[Paraphrase: a channel relays an extortion group's claim concerning a UK transport operator; names, volume and alleged access details withheld.]

Held

A third-party relay of a claim.

Not established

An original organisation statement or independent confirmation; a coherent incident chronology is not established.

Evidence card B04 — 23 Aug 2026

Forum poster | Forum | Forum | English

ORIGINAL

[Paraphrase: a poster offers an issue-tracker archive attributed to a vehicle manufacturer and labels it January 2025. Technical identifiers and attachment details withheld.]

TRANSLATION

[Paraphrase, not a verbatim quote.]

Held

A 2026 circulation post that uses an older date label.

Not established

A new 2026 intrusion, validated archive contents or connection to another incident.

CASE C

C

Financial-application leads with older-looking field values

Evidence card B06 | 16 Nov 2026 | Forum | Financial applications

Unverified claim

CLAIM	A 16 November seller advertised a UK financial-application dataset. The described fields concern identity, household circumstances, employment, income, debt and banking details [S1].
CHRONOLOGY	The displayed application-related date fields include 2024 values. These are values in the post, rather than independently verified extraction or intrusion dates.
WHAT IS HELD	An offer with financial-application-style fields and more than one advertised population measure. The records and unique-person population are not independently reconciled.
ALTERNATIVES	Older lead-generation exports; broker or affiliate records; aggregated or fabricated data; a more recent export containing historical applications.
LIMITS	Neither the data controller nor the advertised brand's regulated status is established. The post does not support a claim of a new 2026 intrusion at a bank.
RESPONSE	Compare a credible signal with authorised broker and affiliate export formats. Review bulk access and retention, and strengthen customer verification against knowledge of genuine financial circumstances.

Bottom line

Older-looking fields do not date extraction or establish a current bank incident.

CASE D

D

An investment-user offer with several advertised counts

Evidence card B05 | 3 Oct 2026 | Forum | Investment information

Unverified claim

CLAIM	An October seller advertised a UK-labelled investment-user dataset. The title and body give different totals, with the body describing a smaller population after a claimed processing step [S1].
WHAT IS HELD	The offer and its advertised contact and identity fields. Different counts can describe different stages or units; they are not automatically proof that the advert is false.
CHRONOLOGY	

A similar offer appears in September, before the selected October post. Matching advertising does not establish file identity, collection date or newly obtained material.

ALTERNATIVES	Marketing data; historical customer records; a fresh export; misattributed or padded material.
LIMITS	The claimed business operates across several countries. A UK heading does not establish that every row concerns a UK resident or that a particular source system was accessed.
RESPONSE	Validate source and population before briefing leadership. Prepare investment-impersonation controls, while avoiding account-wide resets based only on this advertisement.

Bottom line

Advertised populations require validation and cannot be treated as verified affected people.

CASE E

E A travel-connectivity claim with a UK-labelled subset

Evidence card B07 | 13 Nov 2026 | Forum | Travel connectivity

Unverified claim

CLAIM	A November advert described customer, order, subscription, partner and provisioning information for a travel-connectivity service. The poster placed a claimed UK subset within a multi-country population [S1].
WHAT IS HELD	A specific platform claim with both customer and partner-related categories. The country scope in the title is broader than the claimed UK subset.
CHRONOLOGY	The post is dated 13 November. No independently established access or extraction date follows from it.
ALTERNATIVES	A partner environment; test data; an older service export; a genuine platform incident; misattribution or fabrication.
LIMITS	UK-labelled users are not verified UK residents, unique people or confirmed affected customers. The post does not establish live credentials or a UK-only incident.
RESPONSE	Review partner access, provisioning permissions and bulk exports. Investigate internally corroborated accounts and keys before deciding containment or notification scope.

Bottom line

A claimed UK subset is not a UK-only incident or a verified resident population.

Evidence card B07 — 13 Nov 2026

Forum poster | Forum | Forum | English

ORIGINAL

[Paraphrase: an advert describes customer, partner, order and provisioning records for a travel-connectivity service, with a claimed UK subset among several countries.]

TRANSLATION

[Paraphrase, not a verbatim quote.]

Held
A multi-country platform claim mentioning UK-labelled users.

Not established
A UK-only breach, residence of users, live secrets or record authenticity.

Evidence card B08 — 2 Nov 2026

Forum poster | Forum | Forum | English

ORIGINAL

DATABASE SAMPLE - EMAİL - PASS - NUMBER - İD

TRANSLATION

Source English as posted; identifying title and links omitted.

Held
A post advertising a sample with credential and identity fields.

Not established
Sample validity, account control, source ownership or a completed sale.

CASE F

F

An issue-tracker archive carrying an older date label

Evidence card B04 | 23 Aug 2026 | Forum | Manufacturing

Unverified claim

CLAIM	An August poster offered an issue-tracker archive attributed to a manufacturer and labelled it January 2025. The post separately advertised related attachment material [S1].
WHAT IS HELD	A 2026 circulation message with a poster-supplied older date. The label is not independent verification of when the archive was created or obtained.
CHRONOLOGY	The established post date is 23 August. No connection to a later publicly reported disruption is inferred from a shared brand reference.
ALTERNATIVES	An older archive circulated again; a contractor export; a partial technical collection; fabricated or misattributed material.
LIMITS	The archive's contents, ownership, completeness and availability are not validated. No fresh 2026 intrusion is established by this post.
RESPONSE	Review issue-tracker exports, contractor access, attachment retention and secret exposure in authorised internal archives. Keep recirculation handling separate from an investigation of current access.

Bottom line

A poster-supplied older label does not establish a new intrusion or verified archive contents.

4.5 Other offers and the freshness question

Other posts advertise healthcare and energy archives without establishing a new intrusion date. A multi-country hotel-management offer includes the UK among several markets. That reference alone does not establish a particular UK victim or UK payment-data exposure [S1].

Other specific claims widen sector coverage, while remaining unverified [S1].

Sector	Observed offer or report	Not established	Review owner
Energy	Development, source and cloud-related archives	Ownership, current secrets or operational impact	Engineering and cloud security
Manufacturing	Corporate and customer files attributed to a boatbuilder	Authenticity, incident date or completed negotiation	Incident response and data owners
Financial services	An alleged employee identity and credential bundle	Current validity or access to the employer	Identity operations
Financial services	A news relay about customer information disclosed to an impersonator	Original confirmation, event date or a wider system intrusion	Customer verification and privacy owners
Travel services	Website source, mailbox access and ransom pressure	An airline incident or a wider transport campaign	Service and messaging owners
Aviation services	An alleged maintenance-services corporate archive and extortion claim	Archive possession, event date, operational or safety impact	Supplier and incident response owners
Pharmaceuticals	A claimed data collection	Possession, population or a new intrusion	Data owners and incident response
Professional services	A relay concerning tax and support records	Original possession, attribution or verified data access	Privacy and service owners
Education suppliers	Applicant-tracking information with mixed record dates	When extraction occurred or which records remain current	Supplier and recruitment owners
Communications suppliers	A claimed compliance archive containing business counterparties	Whether a named counterparty is an affected organisation	Supplier and privacy owners
Consumer-device suppliers	A relay about purchaser contact and delivery information at a logistics partner	Original confirmation or the size of any UK subset	Supplier and customer-communications owners
Business directories	Multinational employee contact-directory offers with UK company references	Recent access, advertised totals or an intrusion into the cloud platform	Identity and threat intelligence

Sector	Observed offer or report	Not established	Review owner
Mobile applications	A report includes UK-related apps among a malware campaign's intended targets	UK infections, successful access or affected-user totals	Mobile security and fraud owners
Public services	News-style credential-exposure relays	Original confirmation, event year or verified system access	Identity and incident response
Creative services	A multinational content-supplier archive and access offer	File possession, usable access or UK operational impact	Supplier and engineering owners
Education platforms	Cloud, identity and tenant-data claims concerning a wider service	Access validity or a UK-specific affected population	Platform and supplier owners
Manufacturing	Employee and device dossier advertisements with changing country menus	Authenticity, current availability or a common underlying collection	Identity and threat intelligence

The employee-level claim is not proof of employer access. Technical archives can justify an internal secret and permission review when relevance is corroborated, without establishing the claimant's broader account.

Evidence card B09 — 5 Nov 2026

Forum seller | Forum | Forum | English

ORIGINAL

[Paraphrase: a seller claims reservation and payment-related data from a common hotel-management dashboard; the UK is one of several markets listed.]

TRANSLATION

[Paraphrase, not a verbatim quote.]

Held
A hotel-data offer framed as a multi-country supply-chain source.

Not established
A particular UK victim, possession, live access, data volume or valid payment data.

Evidence card B10 — 22 Aug 2026

Forum poster | Forum | Forum | English

ORIGINAL

[Paraphrase: a poster advertises a file collection attributed to a healthcare service provider. Names, precise size, technical access references and links removed.]

TRANSLATION

[Paraphrase, not a verbatim quote.]

Held
An archive-circulation post.

Not established
The age, contents, a new intrusion in 2026 or any verified clinical impact.

Evidence card B11 — 21 Oct 2026

Forum poster | Forum | Forum | English

ORIGINAL

[Paraphrase: a short post advertises an alleged data archive attributed to an energy company; identifying size, name and links removed.]

TRANSLATION

[Paraphrase, not a verbatim quote.]

Held
A short archive claim with hidden content.

Not established
Contents, provenance, when any data was taken or an actual incident.

Evidence card B18 — 6 Jan 2026

Forum poster | Forum | Forum | English

ORIGINAL

Enjoy HQ UK Combo

TRANSLATION

Source English as posted; invitation, claimed count, links and other material omitted.

Held
A UK-labelled combolist distribution message.

Not established
Line count, freshness, usability or the source of the credentials.

A credential-format file also does not prove infostealer provenance. Reused lists, other exports and fabricated material can have similar fields. Defenders should verify relevance and recent account activity rather than infer the capture mechanism from the file's advertised format.

The financial and account-trading material includes UK company documents and business-account offers. Chapter 8 considers those advertisements alongside separately reported fraud patterns. The posts do not establish the validity or use of the advertised accounts.

4.6 Replies can challenge a claim without settling it

A forum commenter described part of a dataset as possibly years old. That is evidence of a freshness challenge, rather than independent validation of the underlying data [S1]. A rival, buyer or casual commenter may have information, but may also be mistaken.

Evidence card B16 9 Jan 2026

Fraud-service advertiser Forum Forum English

ORIGINAL

[Paraphrase: a multi-country carding advert lists UK card and account products, asking prices and old-looking sample material. All card, identity and contact values removed.]

TRANSLATION

[Paraphrase, not a verbatim quote.]

Held
A generic supply advert that includes the UK.

Not established
Current usable cards, ownership, a specific bank breach or fraud loss.

Evidence card B17 13 Jan 2026

Forum commenter Forum Forum English

ORIGINAL

So from that dataset im gathered it was possibly years n years old data which once upon a time was valid

TRANSLATION

Source English as posted; identifiers and surrounding access claims omitted.

Held
A commenter disputes the freshness of part of a dataset.

Not established
Independent validation that the dataset was old, valid, invalid or from a specific breach.

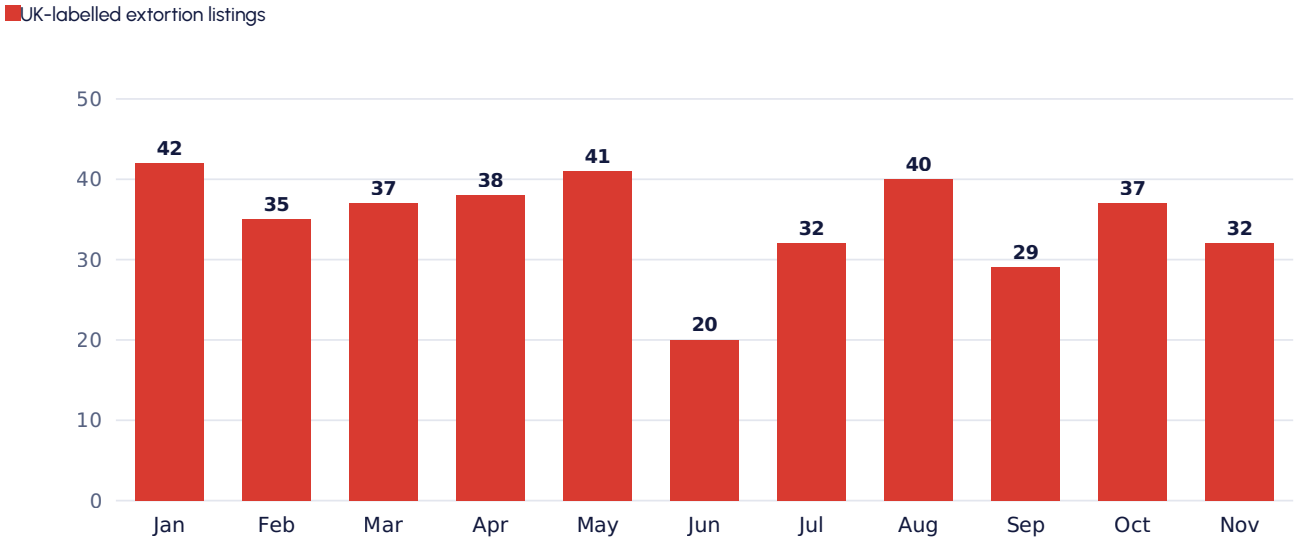
The product advertisement in B16 and the comment in B17 are separate examples. No common dataset is established.

Use replies as leads for validation. Compare the proposition being challenged with the proposition in the original offer. A claim that some rows are old does not establish that every row is old, that all records are invalid or that no current exposure exists.

4.7 Extortion listing dates are a separate population

Ransompedia's 383 UK-labelled listings span every month in the window. January has 42 records and June has 20 in this snapshot. November is a partial month. These are posting dates, not dates of intrusion or measures of attack severity [S3].

UK-labelled extortion records appear throughout the window, with a partial November bar



Source: Brandefense Ransompedia accepted country-labelled listings, 1 January–22 November 2026; November partial. Listing dates are not incident dates [S3].

The listing population is separate from the posts and offers above. Numerical overlap or a repeated organisation label would not establish that two records describe the same incident. Chapter 7 gives the regional and group-label comparisons.

4.8 What is not established

The retained material does not establish a national market size, a completed-sales total or a reliable count of active access offers. Exact advertised record counts are also not validated affected-person counts. These limits apply to the summaries and cards as well as the case text.

No UK-specific DDoS claim was established from the retained availability item discussed in the audit. That item concerns another country. Chapter 6 therefore relies on the relevant official UK warning rather than turning a co-mention into a UK campaign.

KEY TAKEAWAYS

01

Specific offers deserve service and account validation, not automatic breach conclusions.

02

Post dates, record dates and intrusion dates are different facts.

03

UK references in multinational offers do not establish a UK-only affected population.

CHAPTER 05

Incident disclosures and targeting by sector

THIS CHAPTER ANSWERS

What did original public disclosures establish, and what can each sector act on?

12

original-source incident families of UK relevance, with separate date and scope limits

5.1 What the confirmed subset means 38
5.2 Public-service portals 39
5.3 Transport customer data 40
5.4 Retail communications and accounts 41
5.5 Education and limited system access 42
5.6 Charity and customer-service suppliers 43
5.7 Other original-source incident families 44
5.8 Security issues, accidents and historical follow-ups 45
5.9 Recent activity: 9–22 November 46

CHAPTER 05

Incident disclosures and targeting by sector

IN SHORT

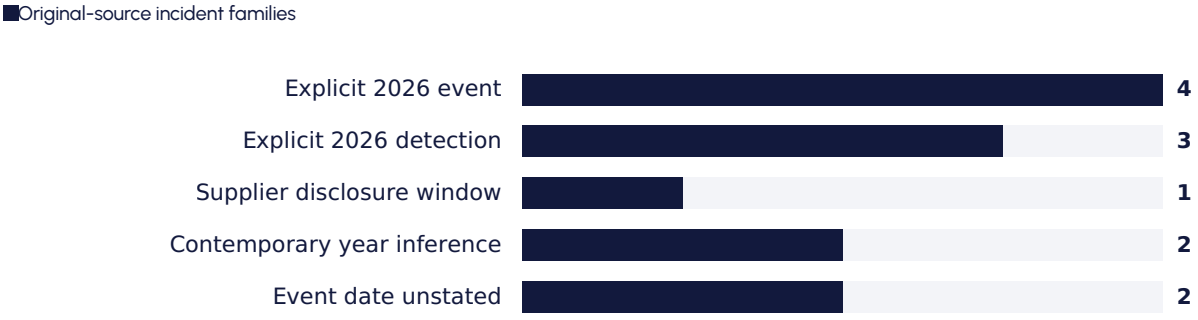
Original public notices describe customer-data access, supplier incidents, service disruption and limited system-specific exposure. They do not establish a single entry route or national incident total. This chapter separates confirmed incident families from security defects, accidental disclosures, historical follow-ups and unresolved claims. Six cases show the defensive decisions in detail. Use the disclosed facts to validate your own dependencies, prepare customer communications and test recovery.

5.1 What the confirmed subset means

This edition records 12 incident families of UK relevance supported by an opened original organisation or authority notice. They are a verified subset of public disclosures. They are not a census of UK attacks, distinct victim organisations or intrusions beginning in 2026.

The date evidence matters. Four families have explicit 2026 event dates, three have explicit 2026 detection dates and one has a 2026 supplier-disclosure window. Two rely on contemporary-year inferences, and two have no event date stated in the original notice. A notification date or detection date does not establish when access began. A supplier incident can affect several organisations without becoming several independently verified intrusions into their own systems.

The twelve confirmed incident families have different date-evidence boundaries



Source: original disclosures in the incident register; twelve UK-relevant families, with separate event, detection and disclosure-date limits [S31][S32][S33][S34][S35][S36][S37][S38][S40][S42][S46][S47][S48].

We name Manchester Airports Group and ASOS because official confirmation and wider reporting were checked. Other victims remain described by broad roles. Identifying article links for withheld organisations are omitted from public citations. The private evidence register retains their source mapping.

An official disclosure confirms only its stated scope. It does not authenticate an actor's record count, claimed access route, group attribution or proposed price. Chapter 4 treats underground claims as a separate evidence population.

5.2 Public-service portals

CASE G

A public-service body's two online portals

Public services

Original notice confirms a scoped incident

DISCLOSURE	A public-service body published a July notice about a security issue affecting two online portals. It became aware after claims appeared over a weekend. The portals were temporarily taken offline and subsequently restored [S31].
ESTABLISHED SCOPE	The notice limits affected information to people who directly used the portals. It lists contact and professional details, including names and, where supplied, email addresses, telephone numbers, job titles and business addresses.
CHRONOLOGY	The body dates awareness to July. The page later records a November update. The update is not a second incident, and the publication does not establish the start of unauthorised activity.
NOT ESTABLISHED	The notice does not substantiate the large record counts or actor identity appearing in some reporting. It also does not imply that other systems of the body were affected.
ALTERNATIVES AND LIMITS	A claim may describe a broader population than the affected portal records. The official notice is the basis for the scoped incident account; the two populations are not reconciled here.
RESPONSE	Public-service owners should map which contact records each portal holds and who can suspend access. Prepare a warning about messages that quote genuine service interactions.

Bottom line

Validate portal-specific data and permissions before describing a wider incident.

The useful lesson is the service boundary. A portal may hold valuable contact information while remaining separate from the organisation's other systems. Both containment and communications should explain that boundary accurately.

5.3 Transport customer data

CASE H

H

Manchester Airports Group customer services

Transport

Company-confirmed incident

DISCLOSURE	Manchester Airports Group said an unauthorised third party obtained customer data during an August incident. Its notice concerns parking, lounge and Fast Track bookings, plus airport Wi-Fi registrations [S32].
ESTABLISHED SCOPE	The company lists email addresses, telephone numbers, vehicle registrations and postcodes. It says the affected system did not hold bank or payment details.
OPERATIONAL BOUNDARY	The company says operational airport systems were not involved and airport operations were unaffected. This is its stated account, rather than an independent safety assessment by this report.
NOT ESTABLISHED	The original notice does not give the widely reported affected-customer total. This report does not substitute an actor's or press figure for an original-source count.
ALTERNATIVES AND LIMITS	An incident in a customer service is not evidence of access to aviation-control systems. Similar customer fields in another advertisement do not establish that it is the same dataset.
RESPONSE	Travel operators should separate customer-service permissions from operational systems. Brief customer teams about messages that quote a real booking or vehicle detail.

Bottom line

Customer-data exposure and operational-system impact are separate questions.

This case illustrates why confidentiality and operational safety are different questions. A useful customer notice can state what information was involved while explaining which services continue to operate.

5.4 Retail communications and accounts

CASE I

ASOS customer information and an unauthorised notification

Retail

Official notice and company account

DISCLOSURE	NCSC reports ASOS's confirmation that an unauthorised notification was sent to customers in October and that customer names and contact information were accessed [S33].
ESTABLISHED SCOPE	The company said it did not believe payment-card information or account passwords were affected. NCSC advised customers to assume they were affected, even if they did not receive the notification.
ADDITIONAL REPORTING	Reuters reported a later customer email in which ASOS said an unauthorised party accessed an employee account after impersonating a trusted contact to obtain credentials [S43]. That is the company's account as relayed by Reuters.
NOT ESTABLISHED	The unauthorised message does not authenticate every statement made by its sender. It also does not establish that a recipient's device was accessed.
ALTERNATIVES AND LIMITS	Customer-facing messaging and data systems can have distinct permissions. The visible message should not be treated as a complete map of the incident.
RESPONSE	Review employee identity verification, messaging permissions and customer-notice channels together. Give customers an established route for checking a suspicious notification.

Bottom line

Protect staff identities and customer messaging permissions together.

The control question is broader than the public website. A legitimate notification channel can carry an unauthorised message. Customers need clear guidance about which action to take, without being asked to trust the disputed message itself.

5.5 Education and limited system access

J

CASE J

A university admissions-system connection

Education

Original notice confirms limited data access

DISCLOSURE	A university said it was alerted in July to potential unauthorised data access. Its investigation identified a configuration issue affecting a connection to one admissions system [S34].
ESTABLISHED SCOPE	The university said limited contact information was involved. It explicitly excluded admissions and examination-result data from that scope and said the access had been removed.
WIDER-SYSTEM BOUNDARY	The statement said investigators had no evidence of broader system access, ransomware or malware deployment. A limited incident should not be rewritten as an institution-wide ransomware event.
CHRONOLOGY	The notice dates awareness and a later August update. It does not establish the initial access date or the complete period of exposure.
ALTERNATIVES AND LIMITS	An actor's reference to a university can obscure the particular system connection involved. The institution's stated boundary is more useful for a defender than a generic breach label.
RESPONSE	Inventory application connections as well as servers. Review what contact information each connection can access and how its permissions are removed.

Bottom line

Inventory application connections and preserve the stated system boundary.

The wider education set also includes a university notice about a teaching-platform supplier incident. That notice says the supplier contained the incident and that no ongoing threat to university systems was evident. It does not establish a separate intrusion into the university's core estate [S40].

5.6 Charity and customer-service suppliers

CASE K

K

A charity relationship-management supplier

Charity and suppliers

Supplier assessment: export scope uncertain

DISCLOSURE	A recipient organisation published the supplier's notices about unauthorised access to its relationship-management service. The supplier's account identifies malicious activity in late July [S35].
ESTABLISHED SCOPE	The supplier assessed that a database copy, including attachments, was likely downloaded. Its update says available records could not identify exactly which objects were accessed or their download destination.
PROBABLE CAUSE	The supplier described a cloud access key as the probable initial cause and a possible exposure in public build material. This remains the supplier's assessment, including its stated uncertainty.
NOT ESTABLISHED	The source did not identify the actor. A likely whole-database export assessment does not establish that every recipient's every record was read or subsequently used.
ALTERNATIVES AND LIMITS	Several customer notices can describe one supplier incident. Counting each recipient as an independent intrusion would overstate the incident population.
RESPONSE	Review secrets in build processes, supplier permissions and attachment sensitivity. Agree an early notification route that supports the controller's assessment while forensic work continues.

Bottom line

Test supplier notification and cloud-secret handling while preserving forensic limits.

A separate public-service complaints body described a third-party incident affecting case management in October. It said the system was taken offline while investigators assessed data impact [S36]. Availability action and uncertainty about personal information can coexist. The notice should retain both.

CASE L

L

A retailer's UK-store information at a supplier

Retail and suppliers

UK-store information included

DISCLOSURE	A household-goods retailer said a US-based provider informed it in November of unauthorised access involving information from its Australian, UK and US stores [S38].
CHRONOLOGY	The notice dates access to 30 October, provider identification to 31 October and containment to 1 November. The retailer says it was informed on 6 November.
ESTABLISHED SCOPE	UK-store information is included in the disclosed scope. The opened notice does not provide a UK-specific affected population.
NOT ESTABLISHED	A multi-country supplier event does not establish equal impact in every country. It also does not establish an intrusion into every customer's own infrastructure.
ALTERNATIVES AND LIMITS	A November publication or update can describe an October event. Those dates must remain separate when reviewing recent activity.
RESPONSE	Map the countries and data types held by each provider. Test who receives an initial supplier notice and how country-specific communications are prepared.

Bottom line

Separate October activity from November notification and country-specific scope.

5.7 Other original-source incident families

The remaining families add sector coverage without implying that every notice has a precise event date.

Sector or role	What the original notice supports	Date boundary	Decision
Education	A school newsletter describes four days of closure and staggered attendance after a serious cyberattack [S37]	January notice; exact attack start not stated	Test a usable education-continuity mode

Sector or role	What the original notice supports	Date boundary	Decision
Public services	A police force confirms non-emergency system disruption, with emergency and 101 services available; staff-data questions remained under investigation [S42]	September detection and notice	Separate public availability from staff-data investigation
Education suppliers	An official council decision documents ransomware response for a school-support platform [S46]	Decision published 11 November; incident date not established from it	Test supplier recovery and school communications
Public-service case management	A third-party incident affects a complaints-management service; data impact remains under investigation in the opened notice [S36]	October disclosure and update; exact event date unstated	Test case access and supplier notification
Retail	Two brand FAQs describe one group incident involving customer information, with stated limits on password and usable payment-data exposure [S47][S48]	Original FAQs undated; 2026 timing partly inferred from contemporary reporting	Treat the notices as one family and preserve date uncertainty
Education platforms	A university relays containment of a teaching-platform supplier incident; no ongoing threat to university systems was evident in its notice [S40]	May supplier-notification window	Review supplier-held data and follow-up phishing

A school notice can document a serious interruption without establishing an extortion group's claims. A business notice can confirm an incident while leaving the access route unknown. Preserve these limits when briefing staff or commissioning assurance work.

5.8 Security issues, accidents and historical follow-ups

A company-filing service disclosed an access-control issue discovered in March. The original update said it had received no reports of unauthorised use at that point. The defect is an established security issue; mass data theft is not established by that statement [S41].

A professional regulator's 18 November notice describes information disclosed in error. It is an accidental disclosure, not evidence of a malicious intrusion [S39]. It belongs in data-handling and notification planning, while remaining outside a count of attacker-led incident families.

Official 2026 notices also discuss older events. Enforcement, sentencing or a revised affected-data assessment may be important in 2026 without making the underlying intrusion a new 2026 event. These follow-ups remain separately classified in the coverage register.

The same care applies to reported global supplier incidents. UK use of a product does not establish that UK data or operations were affected. A cross-border case enters the UK-relevant confirmed subset only when the original evidence supports that relevance.

5.9 Recent activity: 9–22 November

The closing-period view is a snapshot through the material available when checked on 22 November. It is not a claim to cover the remainder of the cut-off day. Listing dates, disclosure dates, update dates and incident dates are distinguished below.

Date	New material or update	Evidence boundary	Immediate owner
9–22 November	Eighteen UK extortion listings in the snapshot [S3]	Eighteen claim records, not eighteen independently confirmed intrusions	Threat intelligence and incident response
10–16 November	Support-tenant, financial-lead and travel-connectivity offers appear [S1]	Claims with unverified access, provenance and UK population	Identity, supplier and fraud owners
10 November	A public-service portal incident page records an update [S31]	Original awareness was in July; this is not a new November incident	Public-service and privacy owners
12 November	ICO warning on unauthorised health-record access [S30]	More than 300 assessed reports cover January to mid-October; reports are not distinct organisations	Health data-access owners
18 November	A professional-regulator error disclosure [S39]	Accidental disclosure, with no malicious intrusion asserted	Data protection and communications
19 November	Joint financial cyber-resilience consultation [S19][S20]	Proposed guidance clarifying existing requirements, not a new incident or new rules	Financial compliance and resilience
November update	A retailer's supplier notice includes UK-store information [S38]	The disclosed access occurred in October	Supplier and customer-communications owners

The source review also records recent transport-account, financial-service, hospitality and supplier leads whose original confirmation or UK impact remains unresolved. They remain outside the confirmed subset. The coverage register preserves their dispositions rather than treating missing confirmation as evidence that nothing happened.

These developments support continued review of customer notices, supplier permissions and service resilience. They do not support a claim that every newly published story describes a fresh attack in the final fortnight.

KEY TAKEAWAYS

01

The confirmed subset describes incident families and preserves uncertainty about event dates.

02

Supplier, customer-service and core-system exposure require different responses.

03

Recent publication does not necessarily mean recent intrusion.

CHAPTER 06

Hacktivism, DDoS and operational disruption

06

THIS CHAPTER ANSWERS

How should defenders distinguish a claim, an observed outage and an official account of disruption?

19 January

NCSC's UK DDoS warning in this year's window

6.1 An official warning, with a defined scope 49
6.2 Timeline of claims and official reporting 49
6.3 Claims and impact require different evidence 50
6.4 Operational technology: the authority reports limited disruption 50
6.5 Availability decisions before an incident 51
6.6 Neutral handling of political rhetoric 51

CHAPTER 06

Hacktivism, DDoS and operational disruption

IN SHORT

NCSC warned in January about recurring DDoS attempts against UK local government. In August it described increased targeting of operational technology, including in the UK, with some limited real-world disruption. These are different observations. An actor's claim or control-panel image does not establish the affected service, duration or physical consequence. Prepare availability mitigation and operational-system access reviews, and communicate only the impact that your own evidence supports.

6.1 An official warning, with a defined scope

NCSC's January alert identifies NoName057(16) and describes frequent DDoS attempts against UK local government. It presents the group as Russian-aligned and discusses ideologically motivated activity. That description remains NCSC's assessment [S6].

The alert does not provide a UK total of successful outages. Nor does it establish that a particular actor post in this report caused a specific interruption. The relevant operational task is to verify user-facing availability and activate the service's agreed response.

6.2 Timeline of claims and official reporting

Both timeline entries are official notices. They describe different activity and retain the authority's stated scope.

19 Jan 2026	**NCSC** Warns about recurring DDoS attempts against UK local government [S6]
27 Aug 2026	**NCSC** Reports increased operational-system targeting, including the UK, with some limited real-world disruption [S25]

No UK-specific actor entry is drawn from the retained availability item. It concerns another country. This limits what this corpus can establish; it does not imply that UK organisations faced no DDoS activity. The official UK warning is a separate source [S1][S6].

6.3 Claims and impact require different evidence

Point	Retained actor material	Official account	Defender interpretation
UK DDoS relevance	No UK-specific target established from the retained availability item [S1]	NCSC describes frequent attempts against UK local government [S6]	Use the official warning for readiness; do not convert a foreign target reference into a UK case
Service impact	No independently established UK duration or impact from that item [S1]	The January warning is not a national outage count [S6]	Measure actual user-facing service impact separately
Operational systems	No retained claim is used to authenticate a particular UK industrial interface [S1]	NCSC describes some limited real-world disruption, including UK targeting [S25]	Review intended connectivity and access; do not assign an actor or facility without evidence

A website can be unavailable for several reasons. An actor's announcement may precede, follow or be unrelated to the user's experience. Establish the service impact from monitoring and operational records, and investigate attribution separately.

Do not calculate a success rate by dividing claimed targets by an authority's count of affected services. The units may be domains, URLs, organisations, attempted requests or service incidents. Unless those populations have been matched, the ratio would not answer a meaningful operational question.

6.4 Operational technology: the authority reports limited disruption

NCSC's August notice describes increased targeting of operational technology across multiple sectors globally, including in the UK. It says the activity resulted in some limited real-world disruption. The notice does not name a UK facility or assign that activity to a particular actor [S25].

That account supports an operational resilience review. It does not authenticate every screenshot or claim concerning an industrial interface. An image alone does not establish device location, reachability, authority to control a process or physical impact.

Operators should review the boundary between business networks, management access and operational systems. Confirm that external connectivity is intended, documented and controlled. Keep an operational owner involved: a security change must account for process safety and service requirements.

A reported incident at a small generator attracted wider political attribution in press coverage. This report does not adopt that attribution as its own. The original official material used here supports the broader warning and its limited-disruption statement, without a facility-specific attribution [S23][S25].

6.5 Availability decisions before an incident

Decision	Owner	Evidence to prepare
What user function must remain available?	Business service owner	Essential transaction and tolerable disruption
Who can activate provider mitigation?	Network operations	Current contact, authority and activation test
How will administrators retain access?	Infrastructure and identity	Protected management route and recovery credentials
What can be safely reduced or suspended?	Service and application owners	Approved degraded mode and capacity assumptions
What will customers be told?	Communications and incident command	Independent status route and factual approval process
Which operational connections are permitted?	Operational-system owner	Approved connectivity and support-access map

A public service may remain reachable while a critical transaction fails. Measure the function that matters, rather than relying only on a homepage response. Include accessibility and the needs of users who depend on the service.

6.6 Neutral handling of political rhetoric

The report records politically framed claims for their security relevance. It does not repeat slurs, recruitment appeals or intimidation. A quoted motive does not establish that a government decision caused an attack or that a state controlled the claimant.

Use observed activity and verified impact as planning signals. If actor channels publish new UK references, the service owner can review readiness. That is an operational trigger, not a position on the issue the actor invokes.

KEY TAKEAWAYS

01

NCSC's DDoS warning describes attempts, rather than a national outage count.

02

Operational-system claims need evidence beyond screenshots and actor language.

03

Prepare service, provider and communications decisions before disruption occurs.

CHAPTER 07

Threat actors and supported relationships

07

THIS CHAPTER ANSWERS

Which actor judgements have evidence, and which relationships remain unknown?

80

group labels associated with UK extortion listings

7.1 A relationship map with evidence on every connection 53
7.2 Ransomware and extortion: distributed claim activity 54
7.3 APT28: the source attributes a router-interception campaign 58
7.4 Techniques named in the advisory 59
7.5 A verified vulnerability example 60
7.6 Covert networks: keep the assessment attributed 61
7.7 Hacktivist claims and criminal personas 61

CHAPTER 07

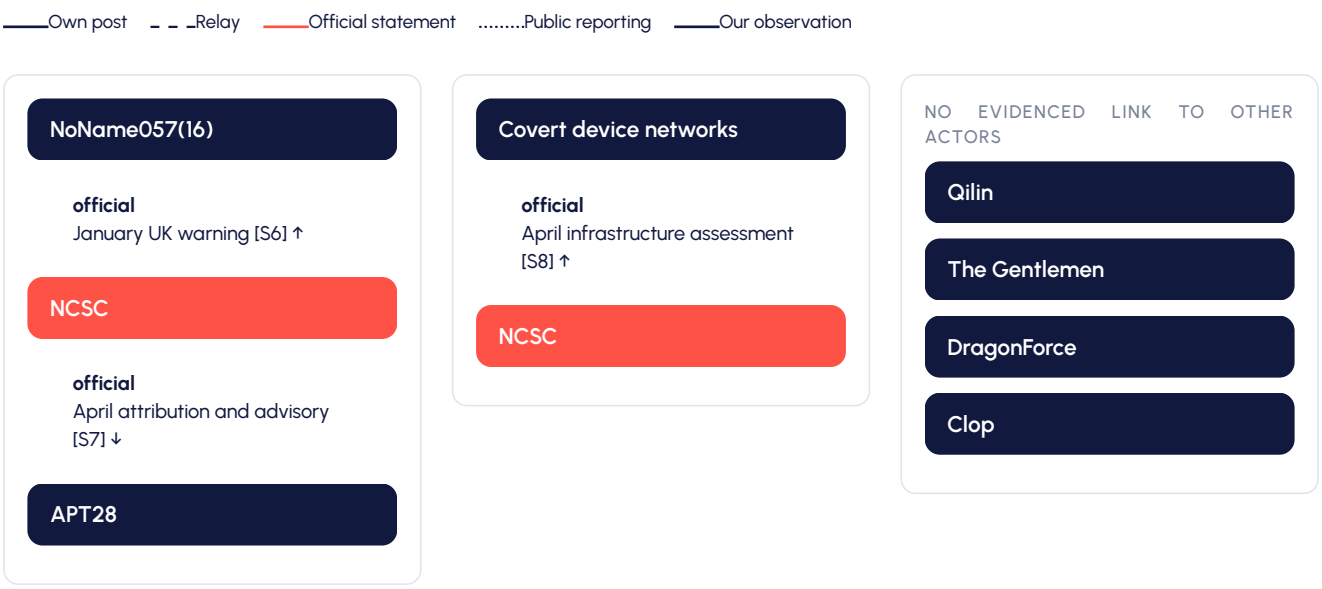
Threat actors and supported relationships

IN SHORT

The evidence supports several distinct actor views. Extortion listings describe public criminal claims under group labels. Official advisories describe DDoS, router interception and covert infrastructure, with attribution stated by the issuing authority. Neither shared timing nor a common country label links these populations. Use actor knowledge to select relevant validation and continuity tasks, while keeping the response useful when attribution remains unresolved.

7.1 A relationship map with evidence on every connection

The map shows source-supported reporting relationships. It does not show a coalition, a shared operator or a common incident across all the profiled groups.



Connection	Evidence	What it establishes	What it does not establish
NCSC to NoName057(16)	January official warning [S6]	The authority identifies recurring UK local-government DDoS attempts	That every associated claim caused an outage or that a state directed each attempt
NCSC to APT28	April official advisory [S7]	The authority attributes the described router-interception activity	A newly confirmed incident at a particular UK organisation
NCSC and partners to China-linked covert networks	April official publication [S8]	The issuing agencies assess infrastructure use and defensive relevance	A single operator for all networks or a UK victim count
Extortion group labels to UK listings	Ransompedia records [S3]	Claims recorded under the specified labels and dates	Shared operators, identical affiliates or successful encryption

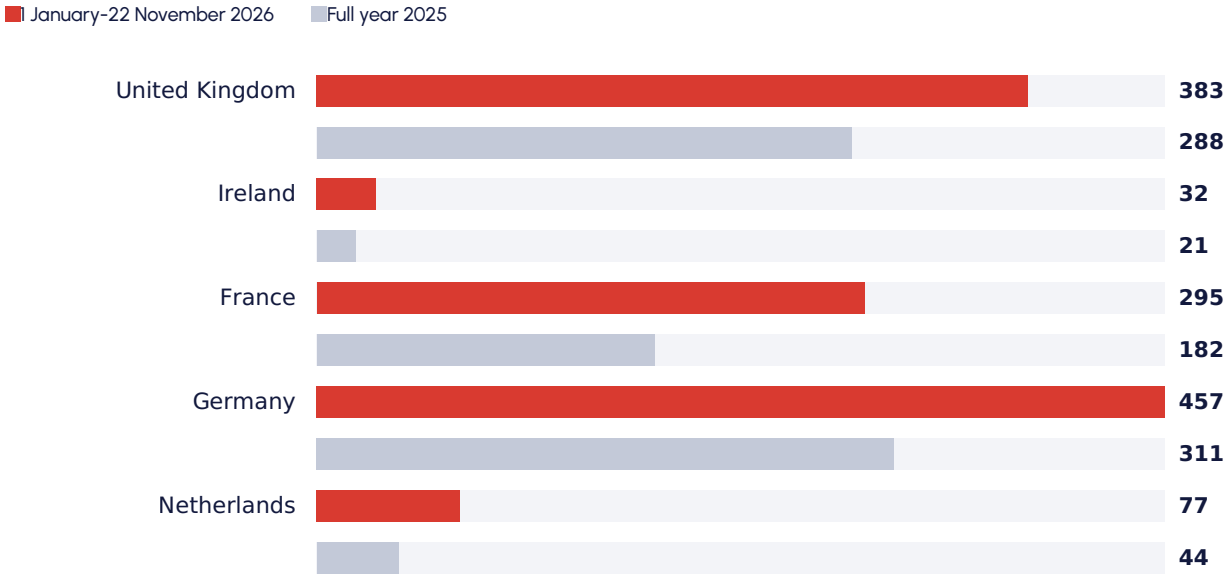
No evidence in this edition links the extortion populations to the state-attributed campaigns. Matching a broad tactic would be insufficient to make that connection.

7.2 Ransomware and extortion: distributed claim activity

The regional table uses four peers selected for geographic and economic relevance. These are counts from one listing source, not country risk rankings.

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

All five countries exceed their full-year 2025 listing totals within the partial 2026 window



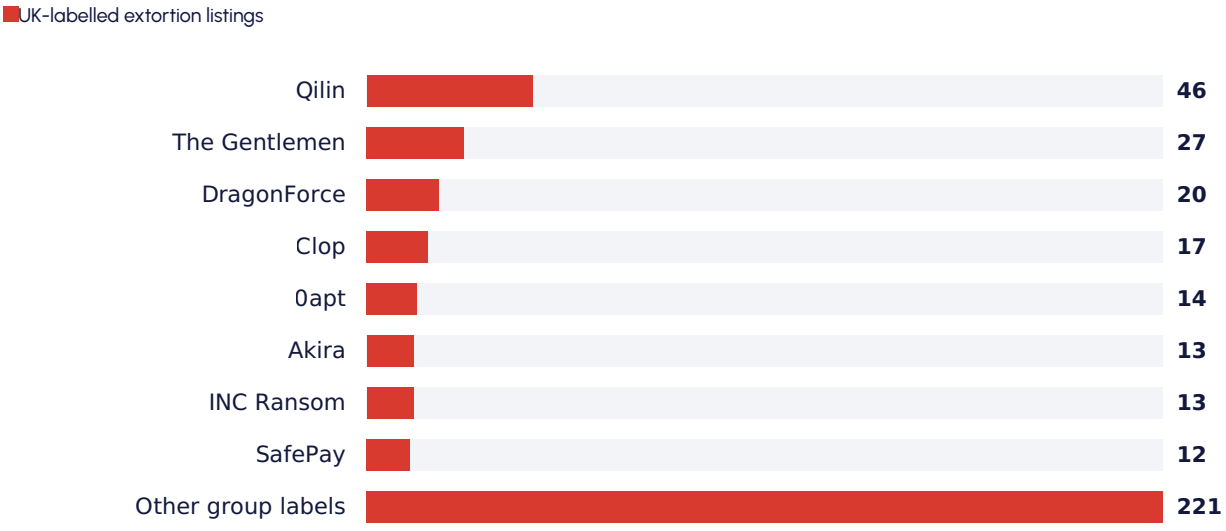
Unmatched periods; not a national risk ranking. Source: Brandefense Ransompedia accepted country-labelled listings, 1 January-22 November 2026; November partial. Listing dates are not incident dates [S3].

Country	2026 window	Full-year 2025	Scope
United Kingdom	383	288	UK country label
Ireland	32	21	Irish country label
France	295	182	French country label
Germany	457	311	German country label
Netherlands	77	44	Dutch country label

The 2026 period ends at the available 22 November snapshot. It is being compared with the whole of 2025, so the difference is not a matched-period growth rate. Country size, business composition and source visibility differ [S3].

The UK snapshot contains 383 listings across 80 group labels. The five most frequent labels account for 124 listings, or 32.4%. The remaining 259 listings account for 67.6%. This is a distribution of recorded claims, not a distribution of confirmed intrusions [S3].

The five leading labels account for 32.4% of UK extortion listings



Source: Brandefense Ransompedia accepted country-labelled listings, 1 January–22 November 2026; November partial. Listing dates are not incident dates [S3].

Group label	UK listings	Share	Decision implication
Qilin	46	12.0%	Include extortion and recovery in exercises without assuming a particular entry route
The Gentlemen	27	7.0%	Validate any matching claim against the organisation's own evidence

Group label	UK listings	Share	Decision implication
DragonForce	20	5.2%	Preserve the distinction between a group label and a verified operator
Clop	17	4.4%	Investigate the claimed service or data source before attributing a broader estate incident
0apt	14	3.7%	Treat the label and its claims as source observations
Other labels	259	67.6%	Maintain a recovery plan that does not depend on recognising a name

Rounded shares may not sum to exactly 100%. The chart retains additional group rows for descriptive detail, while this table groups every label outside the leading five.

Qilin

Extortion listing label | No state attribution made in this report

IN THE UNITED KINGDOM, 2026

1 January–22 November

46 UK extortion listings in the snapshot

CLAIMED TARGETS

Organisations recorded as UK-relevant in the listing source; identities withheld

SEEN IN PUBLIC REPORTING

[S3] 46 accepted UK listings; the label is not independent confirmation of an incident

OUR ASSESSMENT

Use a matching listing as an investigation lead and continuity trigger. Do not infer successful encryption, a common affiliate or an initial access route from the name.

CONFIDENCE

High for retained listing counts; incident outcomes unverified

The Gentlemen

Extortion listing label | No state attribution made in this report

IN THE UNITED KINGDOM, 2026

1 January–22 November

27 UK extortion listings in the snapshot

CLAIMED TARGETS

Organisations recorded as UK-relevant in the listing source; identities withheld

SEEN IN PUBLIC REPORTING

[S3] 27 accepted UK listings; the label is not independent confirmation of an incident

OUR ASSESSMENT

Use a matching listing as an investigation lead and continuity trigger. Do not infer successful encryption, a common affiliate or an initial access route from the name.

CONFIDENCE

High for retained listing counts; incident outcomes unverified

DragonForce

Extortion listing label | No state attribution made in this report

IN THE UNITED KINGDOM, 2026

1 January–22 November

20 UK extortion listings in the snapshot

CLAIMED TARGETS

Organisations recorded as UK-relevant in the listing source; identities withheld

SEEN IN PUBLIC REPORTING

[S3] 20 accepted UK listings; the label is not independent confirmation of an incident

OUR ASSESSMENT

Use a matching listing as an investigation lead and continuity trigger. Do not infer successful encryption, a common affiliate or an initial access route from the name.

CONFIDENCE

High for retained listing counts; incident outcomes unverified

Clop

Extortion listing label | No state attribution made in this report

IN THE UNITED KINGDOM, 2026

1 January–22 November
17 UK extortion listings in the snapshot

CLAIMED TARGETS

Organisations recorded as UK-relevant in the listing source; identities withheld

SEEN IN PUBLIC REPORTING

[S3] 17 accepted UK listings; the label is not independent confirmation of an incident

OUR ASSESSMENT

Use a matching listing as an investigation lead and continuity trigger. Do not infer successful encryption, a common affiliate or an initial access route from the name.

CONFIDENCE
High for retained listing counts; incident outcomes unverified

The criminal label is useful for tracking a claim. It is less useful than a service map for deciding which supplier access to restrict or which service to restore. Do not assume that historical descriptions of a group's techniques establish the entry route in a new case.

7.3 APT28: the source attributes a router-interception campaign

NCSC's 7 April advisory describes router activity continuing from 2024 into 2026. It attributes APT28 to Russia's military intelligence service, using the authority's stated confidence. The described activity changes DNS settings and can support interception of account credentials and tokens [S7].

This is the authority's attribution. The report's own country posts do not independently reproduce it. The advisory does not provide a national count of UK organisations affected by the campaign.

APT28

Aliases discussed in the official source

Espionage activity attributed by NCSC | Attributed by NCSC to Russian military intelligence

CLAIMED TARGETS

Web and email credentials in the reported campaign; no UK victim count supplied

IN THE UNITED KINGDOM, 2026

7 April

NCSC publishes router DNS interception advisory describing activity from 2024 into 2026

SEEN IN PUBLIC REPORTING

[S7] NCSC technical advisory and its stated attribution

OUR ASSESSMENT

Review device support, DNS configuration and relevant authentication evidence. The advisory is not a newly confirmed case at a particular UK organisation.

CONFIDENCE

Attribution as stated by NCSC; no independent attribution by this report

For defenders, the response has two parts. Infrastructure owners should verify router support status and configuration. Identity owners should consider session and token evidence when investigating suspected interception. Changing a password alone may not answer every question about a potentially exposed session.

7.4 Techniques named in the advisory

The matrix reproduces technique identifiers and tactics named in the NCSC advisory. It describes the reported campaign, rather than detections measured in this country dataset [S7].

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Initial Access	Credential Access	Resource Development
T1190 Exploit Public-Facing Application	T1557 Adversary-in-the-Middle	T1583.002 Acquire Infrastructure: DNS Server
		T1583.003 Acquire Infrastructure: Virtual Private Server
		T1584.008 Compromise Infrastructure: Network Devices
		T1586 Compromise Accounts
		T1588.006 Obtain Capabilities: Vulnerabilities

Technique identifiers and tactics as named in the NCSC 7 April 2026 router advisory [S7]. No detections or UK victim counts are implied. [S7]

Tactic	Technique	Defensive review
Initial Access	T1190, Exploit Public-Facing Application	Identify exposed management services and applicable remediation
Credential Access	T1557, Adversary-in-the-Middle	Review unexpected authentication flows and relevant session evidence
Resource Development	T1583.002, Acquire Infrastructure: DNS Server	Investigate unapproved DNS configuration changes
Resource Development	T1583.003, Acquire Infrastructure: Virtual Private Server	Assess suspicious communications in their full context
Resource Development	T1584.008, Compromise Infrastructure: Network Devices	Maintain support and configuration evidence for boundary devices
Resource Development	T1586, Compromise Accounts	Validate the authority and provenance of account activity
Resource Development	T1588.006, Obtain Capabilities: Vulnerabilities	Link vulnerability intake to the owned asset inventory

The source's technique names are descriptive labels. No exploit instructions, victim addresses or deployable offensive code accompany the matrix.

7.5 A verified vulnerability example

CVE-2023-50224 is a credential-disclosure vulnerability affecting legacy networking products. NVD describes a network-adjacent attack condition. NCSC's April advisory says the issue was likely used in the described router activity. A passive DNS or TLS result does not establish this vulnerability in any assessed organisation [S7][S9].

The vendor's May advisory distinguishes hardware variants and regional firmware. Its remediation table identifies TL-WR841N V8–V12 as affected and only partly patched. These details matter when a device name appears in an inventory [S10].

Product scope	Affected detail	Remediation reference
TL-WR841N hardware V8, V9 and V10	NVD lists affected hardware without a fixed firmware version in those entries	Vendor lists the family as partly patched; replace unsupported variants without an applicable update [S9][S10]
TL-WR841N V11	NVD's range includes `11_150616` and excludes `11_211209`	Vendor lists `EU_V11_211209` and the US `V11_us_3_16_9_up_boot(260415)` build [S9][S10]
TL-WR841N V12	NVD's range includes `12_160624` and excludes `12_230317`	Vendor lists `EU_V12_230317` [S9] [S10]

The excluded upper versions describe the NVD affected ranges. They are not permission to install a firmware image for another hardware revision or region. The owner should check the vendor's current device-specific instructions and prefer supported equipment.

7.6 Covert networks: keep the assessment attributed

On 23 April, NCSC and international partners described covert networks used by actors they link to China. The publication discusses vulnerable edge and connected devices used to disguise malicious activity. It also warns that infrastructure indicators can change quickly [S8].

The assessment is relevant to network monitoring and device lifecycle management. It does not mean that every connection from a residential network is malicious. Investigate context and behaviour before blocking a shared or reassigned address.

The report does not infer a common operator between these networks and the router-interception campaign above. Both justify attention to edge devices, but a shared defensive priority is not an attribution link.

7.7 Hacktivist claims and criminal personas

NoName057(16)

DDoSia discussed by NCSC

DDoS activity identified in official reporting | Russian-aligned per NCSC

IN THE UNITED KINGDOM, 2026

19 January

NCSC warns of frequent DDoS attempts against UK local government

CLAIMED TARGETS

Local-government services in the official warning; no national outage total

SEEN IN PUBLIC REPORTING

[S6] NCSC alert concerning UK organisations and denial-of-service resilience

OUR ASSESSMENT

Verify user-facing service impact and prepare provider mitigation. An actor announcement is not independent evidence of duration, cause or success.

CONFIDENCE

High for publication of the official warning; individual claim outcomes remain separate

NCSC's January notice identifies NoName057(16) as a recurrent DDoS concern for UK local government [S6]. Any posts discussed in Chapter 6 retain their own claim and impact limits. An actor's political explanation is reported as that actor's framing, rather than an established cause of the activity.

Public persona labels in the evidence cards describe roles rather than contact values. Repeated labels do not establish shared authorship. An actual alias may also be shared, copied or changed. A similar advertisement can support a repost assessment when the text matches, but it does not establish file identity, a completed sale or a single human operator [S1].

KEY TAKEAWAYS

01

Eighty group labels describe claim activity, not eighty verified operating teams.

02

State attribution remains the issuing authority's assessment.

03

Shared technical controls do not establish relationships between separate actor populations.

CHAPTER 08

The fraud economy: identities, accounts and payment decisions

THIS CHAPTER ANSWERS

How can advertised data and account access become a fraud risk for UK organisations and customers?

£24.3m

reported losses in one official January–August investment-fraud assessment, not this report's loss estimate

8.1 Advertising is an input, not a measure of the economy 64
8.2 Payment-card material has a narrow scope 66
8.3 Credential reuse has an official retail example 66
8.4 Payment diversion concerns the payee decision 66
8.5 AI-assisted investment impersonation is a separately reported population 67
8.6 Asking prices and service claims 67

CHAPTER 08

The fraud economy: identities, accounts and payment decisions

IN SHORT

Fraud evidence includes underground advertising and official reports about actual losses. Those sources answer different questions. An offer can show what a persona markets; it does not establish a transaction. Official warnings describe credential reuse, payment diversion and AI-assisted investment impersonation. Card material is a narrow additional view. Connect credible external signals to account recovery, customer contact and payment controls, while preserving the evidence and reporting periods.

8.1 Advertising is an input, not a measure of the economy

The retained posts include claims concerning identities, credentials and financial services [S1]. A product name in an advertisement does not establish that the provider lost data. An account offered as verified may have been created, borrowed, stolen, fabricated or already closed. The post alone cannot distinguish those possibilities.

Turkish-language offers advertise business accounts alongside UK company documents. A Russian-language account-service message also appears in a UK-fintech discussion. These establish advertising, rather than valid ownership, actual supply or use in fraud. Separate account pre-orders state asking prices [S1].

Evidence card B12 3 Jan 2026

Account seller Forum Forum Turkish

ORIGINAL

Selamlar, elimde ingiltere şirketi belgeleri (şirket şifresi dahil) + Tr iban [payment providers removed] şirket hesapları hesapları mevcuttur bunları kiralamayı ya da satmayı düşünüyorum.

TRANSLATION

Hello, I have UK company documents (including the company password) and company accounts with a Turkish IBAN at [payment providers removed]. I am considering renting or selling them.

Held
An offer to rent or sell business accounts with UK-company documents.

Not established
Account validity, lawful ownership, actual use or an intrusion at a payment provider.

Evidence card B13 4 Jan 2026

Account seller Forum Forum Turkish

ORIGINAL

UK şirket üzerine kurulu [payment provider removed] Business hesabı satılıktır. Şirket evrakları ile teslim edilecek.

TRANSLATION

A [payment provider removed] Business account set up under a UK company is for sale. It will be delivered with company documents.

Held
A business-account offer linked to UK-company documents.

Not established
Account validity or a breach at the advertised payment provider.

Evidence card B14 7 Jan 2026

Account-service advertiser Forum Forum Russian

ORIGINAL

Я могу предоставить личные (с индивидуальными именами) и бизнес-учетные записи (с/без продавца).

TRANSLATION

I can provide personal accounts (with individual names) and business accounts (with or without a seller).

Held
An advertiser's claim about account supply in a UK-fintech discussion.

Not established
Actual supply, customer identity, use or compromise of a financial institution.

Evidence card B15 14 Jan 2026

Account-service advertiser Forum Forum English

ORIGINAL

Pre order [...] [payment provider removed] UK Personal [...] 650$ [...] [payment provider removed] UK CUSTOM [...] 1000$

TRANSLATION

Source English fragments; punctuation, symbols, brand and contact material omitted.

Held
UK account pre-order asking prices.

Not established
Completed transactions, genuine accounts or their use.

A useful analytical model connects four decisions: obtaining identifying information, making a convincing approach, changing account access or payment instructions, and moving money. This is a model of possible fraud progression. It is not an observed common operator or a measured conversion rate between the retained posts.

Defenders should identify which decision they control. A retailer controls account recovery and order collection. A bank controls some payment and beneficiary decisions. A supplier may control an administrator's access. Sharing a credible signal across those owners can be useful without asserting that one incident caused another.

8.2 Payment-card material has a narrow scope

SCOPE OF THE CARD FIGURES

These figures concern only payment cards that appeared in clear text in the dark-web posts collected for this report. Brandefense detects stolen cards through other methods outside this scope. The figures do not measure national card theft, active cards or fraud losses.

The narrow country-labelled subset contains 28 distinct card values in 33 retained posts. Country labels come from the posts and are not independently authenticated issuer-country assignments. The observations do not establish current validity, ownership or when any underlying data was obtained [S4].

The recent forum refresh also contains multi-country payment-data advertisements with claimed UK offerings. They do not establish affected issuers, current validity or a fresh intrusion. Their advertised prices are not evidence of completed sales [S1].

An issuer name or card-related advertisement is not evidence that the issuer's systems were accessed. Responses should follow validated relevance and payment-provider evidence. Broad card replacement or customer notification should not be inferred from an unauthenticated post alone [S4].

8.3 Credential reuse has an official retail example

Report Fraud's June warning describes criminals reusing login details obtained from earlier data breaches to access retail accounts. It describes expensive orders and collection of goods in person. A report mentioning a retailer is not evidence of a new breach of the retailer's systems [S26].

The control implication concerns the account and fulfilment journey. Review unusual sign-ins, recovery changes, payment changes and high-value collection together. Stronger login controls can lose value if an impersonator can reset the account through a weaker recovery process.

If suspicious activity is found, the customer response should explain which account needs attention and which trusted route to use. Avoid sending customers to a new link that resembles the messages the warning is trying to prevent.

8.4 Payment diversion concerns the payee decision

Report Fraud reported 3,657 payment-diversion reports and more than £101 million in reported losses for the 2025/26 financial year. Its September warning describes altered invoices, impersonation and misuse of email. The period spans two calendar years and is not a calendar-2026 total [S28].

The decision point is a request to change where money goes. A familiar name, accurate invoice or plausible email history may make the request convincing. Verify a material change through a previously established contact route and preserve the approval record.

The organisation should also protect the legitimate process. Staff need a clear exception route when a supplier genuinely changes bank details. An undocumented workaround can recreate the same weakness that the control was intended to remove.

8.5 AI-assisted investment impersonation is a separately reported population

An October Report Fraud warning gives £24.3 million in reported losses and more than 1,300 reports of AI-assisted investment fraud between January and August 2026. It describes fabricated endorsements and requests for further payments when victims try to withdraw funds [S27].

Those figures are not derived from the underground posts in this report. They should not be added to the payment-diversion figures, whose period and categories differ. The source's reported-loss population is also different from an estimate of all UK fraud.

For financial institutions, the relevant task is to recognise the customer journey and interruption points. For other employers, it is a communications and staff-welfare issue as well as a security issue. A convincing image or voice is not independent verification of investment authority.

Report Fraud also warned in October about callers impersonating police forces through spoofed telephone numbers. The displayed number is not independent proof of identity, and the warning does not establish an intrusion into police telephone systems [S29].

8.6 Asking prices and service claims

Advertised product	Asking price	Currency	Evidence
UK-labelled personal-account pre-order	650	Dollar symbol as posted; specific dollar currency unverified	B15 [S1]
UK-labelled custom-account pre-order	1,000	Dollar symbol as posted; specific dollar currency unverified	B15 [S1]

These are advertised pre-order prices from one post. No completed transaction or valid account was established.

A price list can help explain the kind of access or information a persona advertises. It cannot establish demand, completed sales, profit, the value of the underlying data or the size of a national market. Similar wording across several posts may simply reflect copied advertising.

Where a claim concerns the organisation, give the relevant owner enough context to validate it. Preserve the difference between an account, a set of records and a service advertised by subscription. Do not turn mixed units into a single exposure total.

KEY TAKEAWAYS

01

Underground offers describe advertising, while official loss figures describe separately reported populations.

02

Reused credentials and changed payee details create different control decisions.

03

Card observations remain a narrow signal with no national fraud-loss inference.

CHAPTER 09

Banking and financial services

09

THIS CHAPTER ANSWERS

Which financial exposure signals need security, fraud and service owners to act together?

30

selected banking and finance domain estates, including institutions beyond retail banks

9.1 Define the financial population before interpreting it 70
9.2 What the available controls can show 71
9.3 Keep four financial questions separate 72
9.4 The closing-period regulatory signal 72
9.5 A joined exercise for security and fraud teams 72
9.6 Reimbursement context does not replace prevention 73

CHAPTER 09

Banking and financial services

IN SHORT

Financial institutions face both service-continuity and customer-fraud decisions. The selected financial portfolio records device and credential associations, current listings and public-control observations. Official November material reinforces the need to evidence resilience under existing requirements. Use credible intelligence to validate accounts, review payment and recovery decisions, and test important business services with their suppliers.

9.1 Define the financial population before interpreting it

The sample contains 30 banking and finance domain estates. It includes banking, building societies, payments, investment services and financial infrastructure. It is neither a list of every licensed UK bank nor a representative sample of every financial institution [S2].

A group and a customer-facing business can have separate operational domains. Domain observations describe the selected estate. They should not be read as a complete assessment of the corporate group, every subsidiary or every customer service.

The 30-estate portfolio records at least 81,496 device associations and 376,806 credential-record associations. Current listings concern 15 estates. These observations do not establish bank-system intrusions [S2].

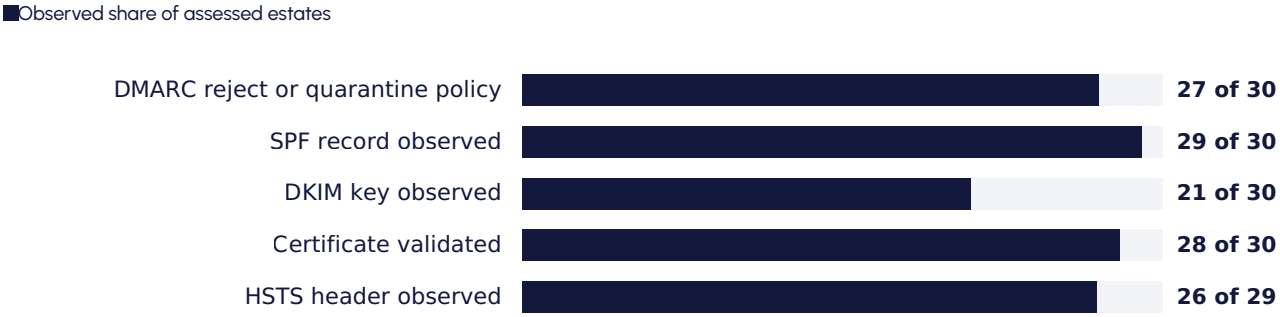
Observation	Quantity	Population	Limit
Device associations, at least	81,496	30 selected financial estates	Not bank-operated end-points or confirmed intrusions
Employee-device associations	405	Within the device view	Endpoint ownership needs validation
Credential-record associations	376,806	30 selected financial estates	Historical and repeated records; current validity unknown
Current listing estates	15	30 selected financial estates	Advertised associations, not completed sales
Document associations	245	30 selected financial estates	Sensitivity and authorisation unresolved
Issuer-domain matches	10	Within the 30-estate portfolio	Research mapping, not a verified licensing census

The financial comparison covers ten selected issuer domains within the portfolio. Their records contain 38,565 non-employee-device associations and 153 employee-device associations. These are overlapping service associations, rather than uniquely owned bank endpoints.

The card population in Chapter 8 remains separate: 28 distinct values in 33 posts explicitly presented as UK-related. Issuer assignments and country labels are unverified. No per-issuer card-loss total or bank-intrusion inference follows [S2][S4].

9.2 What the available controls can show

The financial sample has visible email controls, with service-level validation still required



Banking and finance: 30 selected estates; HSTS assessed for 29. Source: public technical observations, 22 November 2026. Policies observed do not establish message-level enforcement; denominators are the assessed estates [S2].

Observation	Estates	Denominator	Limit
Assessed financial estates	30	30	Selected domains; not all UK licensed banks
DMARC reject or quarantine policy	27	30	Policy observation; full enforcement not inferred
SPF record observed	29	30	Owner validation required
DKIM key observed	21	30	Signing coverage not established
Certificate validated	28	30	Does not establish application security
HSTS header observed	26	29	Web-control results available for 29 financial estates

These are the available passive observations [S2]. An email policy observation does not establish the strength of payment authorisation, customer identity checks or transaction monitoring. A valid certificate does not establish application security.

The owner should interpret each result against actual services. Confirm which services each observation concerns before assigning a remediation priority.

9.3 Keep four financial questions separate

Question	Evidence needed	Responsible owner	Avoid this inference
Is an employee or administrator account being misused?	Active account match, relevant sessions and authentication evidence	Identity and incident response	Historical credentials automatically mean current access
Is customer fraud changing?	Customer reports, account events and payment evidence	Fraud operations	A bank-themed advertisement demonstrates a bank intrusion
Can an important service remain within tolerable disruption?	Dependency map and severe but plausible testing	Business service owner	A successful backup job demonstrates end-to-end recovery
Does a notification or reimbursement duty apply?	Legal scope, awareness, risk and transaction facts	Compliance, privacy and payment operations	One reporting route or cap applies to every event

A single case can involve more than one question. It should still retain the evidence for each. For example, a customer may suffer payment fraud without an intrusion into the bank's own systems.

9.4 The closing-period regulatory signal

On 19 November, the Bank of England said that October had the second-highest monthly number of cyber incidents reported to the FCA in five years. It described that figure as 52% above the previous eighteen-month peak in May 2025. The release does not provide a national incident count for this report [S20].

The same announcement accompanied consultation on cyber risk and resilience management. The consultation states that it proposes no new rules, instead clarifying existing requirements [S19]. Firms should preserve that distinction when briefing the board.

The useful response is to review evidence already required for important business services. Map material suppliers, explain the basis of impact tolerances and test recovery under severe but plausible disruption. A consultation can sharpen the questions without establishing a new legal deadline for every control.

9.5 A joined exercise for security and fraud teams

Choose a scenario in which a credible account or supplier alert arrives while customers report unusual payment requests. Ask security to establish the access facts, fraud operations to evaluate customer harm and the service owner to assess continuity. Legal and communications should work from the same factual record.

The exercise should test how disagreements are handled. The teams may use different case definitions and reporting periods. A fraud report, a suspicious session and an extortion claim can concern the same business context without representing three confirmed intrusions.

Record the points where information is missing. Assign an owner and a decision time for obtaining it. An unresolved uncertainty is easier to manage when it is explicit than when a combined dashboard silently treats it as zero.

9.6 Reimbursement context does not replace prevention

The PSR's APP framework covers qualifying transfers and claimants within its stated conditions. Its £85,000 standard maximum is a reimbursement limit, not a general cyber-loss cap [S18]. Payment teams should maintain the correct process for the transaction and customer concerned.

Security investment should still address the observed route to harm. Examples include stronger account recovery, independent verification of changed payment details and protected supplier access. Evaluate the customer experience and false positives alongside the intended fraud reduction.

KEY TAKEAWAYS

01

The financial sample covers more than retail banks and does not support a national bank ranking.

02

Passive controls cannot substitute for missing identity or transaction evidence.

03

Test security, fraud and service-continuity decisions together while preserving their separate case definitions.

CHAPTER 10

Regulatory response and reporting decisions

10

THIS CHAPTER ANSWERS

Which obligations apply at the cut-off, and which developments still require implementation?

72 hours

several reporting regimes use this period, with different triggers and scope

10.1 Duties in force and developments under consideration 75
10.2 UK GDPR: awareness, risk and an initial notice 76
10.3 NIS: continuity impact and parallel obligations 76
10.4 Proposed reforms need a commencement check 77
10.5 Financial supervision and payment fraud 77
10.6 What CISOs should prepare now 78

CHAPTER 10

Regulatory response and reporting decisions

IN SHORT

A single incident can create several reporting decisions. UK GDPR, essential-service rules, communications duties and financial supervision have different scopes and triggers. The Cyber Security and Resilience Bill remained in parliamentary passage at the cut-off. The financial regulators' 19 November consultation clarifies existing requirements and proposes no new rules. Build a reporting matrix around your legal entities, services and data, then rehearse the awareness and escalation decisions with counsel.

10.1 Duties in force and developments under consideration

The table separates existing obligations from proposed changes. It is an operational reference, not legal advice.

Framework	Who and trigger	Timing or status	Consequence and limit
UK GDPR	Controllers handling a personal data breach; notification depends on risk to individuals	Notify without undue delay and, where feasible, within 72 hours of awareness, unless risk is unlikely [S11]	ICO guidance gives a maximum of £8.7 million or 2% of global turnover for failure to notify when required; other infringements have separate consequences
Processors under UK GDPR	A processor becomes aware of a personal data breach affecting a controller's data	Inform the controller without undue delay [S11]	Do not treat the controller's reporting period as permission to delay the processor's notice
Communications privacy	Communications service providers with a personal data breach	ICO guidance states 72 hours under PECR; the guide records the August 2025 change [S11]	Use the appropriate reporting route; this is not the same applicability test as UK GDPR
UK trust services	A security breach within the UK eIDAS reporting scope	ICO guidance states 24 hours [S11]	A GDPR report does not extend this separate deadline
NIS essential services	An operator of essential services with a significant continuity impact	Notify its competent authority without undue delay and within 72 hours of awareness [S12]	Applicability is service-specific; not every business is an essential-service operator
NIS digital services	A relevant digital service provider with a substantial service impact	Notify without undue delay and within 72 hours of first awareness, subject to the information condition in regulation 12 [S13]	The provider needs information enabling it to assess substantial impact
Telecommunications security	Public communications providers within the statutory regime	Ofcom's enforcement duties began on 1 October 2022 [S24]	Security-duty failures can attract up to 10% of relevant turnover or £100,000 per day for continuing failure

Framework	Who and trigger	Timing or status	Consequence and limit
Financial operational resilience	Firms in scope of the regulators' existing requirements	Mapping and testing were required by 31 March 2025; continuing resilience remains expected [S17]	Scope and supervisory consequences depend on the firm and applicable rules
Cyber Security and Resilience Bill	Proposed expansion and amendment of NIS	Lords third reading occurred on 2 November; Commons consideration of amendments was scheduled for 24 November [S15]	The scheduled event is after the cut-off; proposed duties are not treated here as operative obligations
Financial cyber guidance consultation	Firms in scope of existing operational-resilience requirements	Opened 19 November; closes 26 February 2027 [S19][S20]	The consultation proposes guidance and no new rules; final guidance was still to follow

Legal teams should verify the current text for the organisation's exact circumstances. The dates above do not establish that every provision in a framework applies to every organisation in a sector.

10.2 UK GDPR: awareness, risk and an initial notice

The ICO guide distinguishes regulator notification from communication to individuals. High risk to individuals calls for communication without undue delay. A decision not to notify must be justified and documented. An investigation can continue after an initial notification, with further information supplied in phases [S11].

The first operational question is who can make the awareness and risk assessment. A technical team may know that a system was accessed before anyone knows whether personal data was involved. A supplier may have useful evidence that the controller has not yet received. Escalation should preserve those distinctions without postponing a decision indefinitely.

A practical incident record should contain the first alert, the information available at each decision point, the legal assessment and the reason for reporting or not reporting. Record uncertainty explicitly. Do not wait for a criminal advertisement to be authenticated if other evidence already establishes a reportable personal data breach.

A post alone also does not settle the question. A claim may concern old data, another controller or an unauthenticated sample. Investigate it promptly and retain the assessment. Avoid turning either a seller's assertion or a seller's denial into the organisation's legal conclusion.

10.3 NIS: continuity impact and parallel obligations

Regulation 11 addresses significant impact on an essential service. Regulation 12 addresses substantial impact on a relevant digital service and includes an information condition. They therefore require a service-impact assessment, rather than a simple check for the word ransomware [S12][S13].

The current penalty provisions distinguish material and other contraventions. Regulation 18 provides maxima of £1 million, £8.5 million and £17 million for the relevant categories. The highest band concerns significant risk to, or significant impact on, service provision. These are statutory maxima, not automatic fines for an incident [S14].

A service outage can also involve personal data, communications or financial obligations. Reporting under one framework does not automatically satisfy another. Assign a legal owner to reconcile the reporting routes, while a business owner measures service disruption and customer harm.

Competent authorities differ by sector and, for some services, by jurisdiction within the UK. The government's factsheet sets out that structure [S16]. Do not assume that an England-specific health route covers every health-service operator across the UK.

10.4 Proposed reforms need a commencement check

The government's Bill summary describes proposed coverage of data centres, managed service providers, large load controllers and designated critical suppliers. It also describes proposed initial notification within 24 hours and a fuller report within 72 hours. Implementation is intended to be phased, with several duties dependent on secondary legislation [S16].

The parliamentary stages page places consideration of Lords amendments on 24 November, after this report's cut-off [S15]. A future timetable entry is not evidence that a stage occurred. Likewise, a proposed reporting period is not a current universal deadline.

Organisations can prepare without asserting that the reforms already apply. Identify potentially affected services, compare incident records with proposed information needs and assign someone to monitor commencement instruments. Keep that preparation separate from the matrix of duties already in force.

10.5 Financial supervision and payment fraud

The FCA's 2026 observations emphasise mapping dependencies, testing severe but plausible disruptions and remediating vulnerabilities that could defeat impact tolerances. An important business service is defined by the harm its disruption could cause, rather than by the name of a technology platform [S17].

The joint November consultation brings existing requirements together in a cyber context. It does not propose new rules [S19]. A firm should use the consultation to test the clarity of its current evidence, while legal and compliance teams track the eventual final guidance.

Payment-fraud reimbursement is a separate topic. The PSR describes protections for qualifying UK Faster Payments and CHAPS transfers made from 7 October 2024. Individuals, microenterprises and charities are included, subject to exclusions and conditions. The standard maximum is £85,000 per claim [S18].

That limit is neither a fine nor a measure of fraud in this report. Card payments, cash, cheques, unauthorised fraud and civil disputes have different arrangements. A security team should route a potentially affected customer to the payment provider's process, rather than promising that every loss will be reimbursed.

10.6 What CISOs should prepare now

Decision	Responsible function	Evidence to prepare
Which entities and services fall within each regime?	Legal and compliance	Approved applicability matrix with review date
Who assesses awareness and individual risk?	Privacy and incident response	Decision log and out-of-hours escalation route
How does a processor notify a controller?	Procurement and privacy	Contract terms, named recipients and exercise result
Which service impacts are significant or substantial?	Business continuity and service owners	Service map, impact measures and authority contacts
How will interim and final notices agree?	Communications and legal	Fact record, version history and approval owner
Who checks new commencement instruments?	Regulatory affairs	Monitoring owner and documented change assessment

Use an exercise with incomplete information. A useful plan still works when the supplier cannot yet give a final affected population or when an actor publishes a conflicting figure.

KEY TAKEAWAYS

01

Reporting periods have different triggers, exceptions and recipients.

02

The November Bill and guidance consultation must retain their proposed status.

03

Test the legal decision process alongside technical response and service recovery.

CHAPTER 11

Outlook and conditions that would change it

11

THIS CHAPTER ANSWERS

What should leaders plan for, and which new evidence would change the plan?

4

conditional planning scenarios

11.1 Key judgements 80

11.2 Four conditional scenarios 81

11.3 What the evidence does not support 81

11.4 Review triggers for the leadership team 82

CHAPTER 11

Outlook and conditions that would change it

IN SHORT

Extortion claims, identity abuse, supplier dependencies and service disruption support a practical resilience agenda. They do not support a numerical forecast of attacks or losses. Recent official guidance also puts patch capacity and AI-related change on the planning agenda. The judgements below identify their evidence and limits. Choose service-based scenarios, define the signals that would activate them, and revisit the assessment when stronger evidence arrives.

11.1 Key judgements

Confidence here applies to the stated proposition. It is not a rating of an actor, a country or an organisation's security.

Judgement	Confidence	Basis and limit	What would change it
Extortion deserves a funded recovery exercise	High	383 UK listings across 80 group labels demonstrate sustained public claim activity; they do not establish 383 successful intrusions [S3]	A material correction to dates, country attribution or listing acceptance would change the descriptive totals
Identity validation is a useful first response to a credible offer	High for the response principle	Account and access claims require account-level corroboration before disruptive action [S1]	Evidence of active unauthorised sessions would justify escalation beyond advertisement triage
Supplier permissions belong in continuity planning	High	Official policy and financial guidance emphasise dependencies; individual incident entry routes vary [S16] [S17]	Verified independent recovery and narrowly scoped supplier access would reduce the relevant exposure
Availability and data exposure need separate investigations	High	Official DDoS warnings concern availability; data claims concern confidentiality and sometimes integrity [S6]	Corroborated evidence linking a specific outage and unauthorised data activity would justify a combined incident account
AI-related change increases the value of patch readiness	Medium as a planning judgement	NCSC's November assessment is forward-looking; the report does not measure AI use in the retained posts [S5]	Evidence of materially faster exploitation in the organisation's technology estate would change response capacity needs
The closing period requires continued attention	High for monitoring, not prediction	Eighteen UK extortion listings fall in 9–22 November in this snapshot [S3]	Later disclosures, withdrawals or corrections could change the closing-period picture

The identity judgement does not assume that all criminal offers are genuine. It states that a credible signal deserves a reproducible validation decision. The response can be stronger when the organisation finds corroborating evidence in its own records.

11.2 Four conditional scenarios

These are planning assumptions. They are not forecasts or assertions that a named organisation is vulnerable.

Scenario	Activation signal	Initial owner	First decision
An actor advertises recent access to a supplier serving several business units	Credible matching service details or corroborated unauthorised activity	Incident commander and supplier owner	Restrict the relevant access, preserve records and identify dependent services
A politically framed DDoS claim accompanies a public-service outage	Independent service monitoring confirms customer impact	Service owner and network operations	Activate agreed mitigation while measuring availability from user-facing evidence
A customer-data disclosure is followed by convincing impersonation reports	Fraud operations sees matching contact patterns or changed customer behaviour	Fraud lead and customer operations	Update warnings and verification controls around the observed fraud route
A widely deployed edge product requires urgent remediation	Vendor or national advisory applies to an owned device version	Infrastructure and vulnerability management	Identify affected assets, contain exposure and verify the remediation or replacement

Each scenario should include a communications decision. The organisation may need to explain a service problem before attribution is known. It may also need to warn customers about fraud without endorsing an actor's claimed population.

11.3 What the evidence does not support

The data do not support a ranking of the UK against peers by the probability of an attack. Country size, economic composition, disclosure practices and source visibility differ. The comparator table is a description of listings observed in one database, with the stated periods [S3].

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

The figures do not establish the share of UK organisations with an active unauthorised account. The national Atlas headline of 61 describes a purposive 250-estate portfolio [S2]. Neither a missing observation nor an unpublished figure means that the risk is absent.

A shared group label also does not establish a common operator across every listing. A name can represent a service, affiliates or changing participants. The supported conclusion is narrower: the database records claims under those labels. The recovery plan should remain useful if attribution changes.

The report does not calculate national losses from advertisements, asking prices or disclosed record counts. Those are different quantities. A quoted price is not a completed transaction, and a count of records is not a count of unique people or successful frauds.

11.4 Review triggers for the leadership team

Review this assessment when a material supplier changes, when an important service is redesigned or when new evidence changes an incident's status. A fresh confirmation may replace a claim-only assessment. A correction or withdrawal may narrow an earlier account.

Use operational evidence to decide whether additional investment is required. Examples include an unowned privileged account, a recovery dependency that fails during an exercise, or a notification route that cannot be used outside working hours. These are actionable facts about the organisation itself.

A quarterly review should ask whether the controls remain aligned with the service. More alerts do not necessarily mean worse security. Fewer alerts do not necessarily mean less threat. Changes in collection, business activity and detection coverage can explain either direction.

KEY TAKEAWAYS

01

Scenarios are conditional plans with activation signals.

02

Confidence attaches to a proposition and its evidence, not to an actor label.

03

Reassess when incident confirmations, supplier changes or control tests change the facts.

CHAPTER 12

A 30/60/90-day action plan

12

THIS CHAPTER ANSWERS

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

90 days

a proposed programme, adjusted to each organisation's service priorities

12.1 The delivery lanes 84
12.2 Identity operations: establish a defensible disposition 86
12.3 Infrastructure teams: test controls in their actual service context 86
12.4 Threat intelligence and the SOC: preserve evidence boundaries 87
12.5 Fraud teams: connect the customer and payment decisions 87
12.6 Leadership evidence at each checkpoint 88
12.7 How Brandefense can help 88

CHAPTER 12

A 30/60/90-day action plan

IN SHORT

Start with ownership and validation, then prove that essential services can recover. The plan below connects identity, suppliers, availability, customer fraud and notification. Its timing is a proposed default, not a statutory deadline. Each action has a trigger, an owner and completion evidence. Have the board choose the important services, approve the accountable owners and review demonstrated results at the end of each phase.

12.1 The delivery lanes

The lanes are a working plan. Apply each action to an identified service or confirmed exposure, rather than treating every recommendation as a reason for an immediate estate-wide change.

1Days 1–30	
If an access or credential offer credibly matches your estate, validate account status, recent sessions and prior remediation	
OWNER Identity operations with incident response	COMPLETION EVIDENCE Every credible signal has an accountable disposition and escalation decision
Identify the services whose interruption would cause unacceptable customer or operational harm	
OWNER Business owners and CISO	COMPLETION EVIDENCE Approved service list with tolerable disruption and accountable owner
Inventory supplier permissions supporting those services, including help desks and remote support	
OWNER Procurement and platform owners	COMPLETION EVIDENCE Named permission owners, support routes and emergency restriction procedure
Reconcile reporting duties, awareness decisions and out-of-hours contacts	
OWNER Privacy, legal and compliance	COMPLETION EVIDENCE Applicability matrix and a completed notification exercise

Review public-service availability plans where DDoS would prevent essential access

OWNER

Network and service owners

COMPLETION EVIDENCE

Provider contacts, mitigation authority and alternative user information route

2Days 31–60

If privileged recovery relies on reusable personal information, strengthen identity proofing and independent verification

OWNER

Identity engineering and service desk

COMPLETION EVIDENCE

Tested recovery flow, exception approvals and protected audit records

Where an edge device is unsupported or an applicable advisory remains unresolved, patch or replace it

OWNER

Infrastructure owners

COMPLETION EVIDENCE

Version evidence, approved configuration and removal of obsolete access

Review email-authentication observations against legitimate sending services

OWNER

Messaging and domain owners

COMPLETION EVIDENCE

Approved sender inventory, staged policy change and delivery checks

If fraud reports show impersonation using real customer details, adjust contact-centre checks and warnings

OWNER

Fraud and customer operations

COMPLETION EVIDENCE

Updated scripts, known-number verification and review of observed outcomes

Rehearse an incident at a critical supplier using incomplete initial information

OWNER

Supplier owner and incident commander

COMPLETION EVIDENCE

Timed notice receipt, dependency map and decisions recorded in the exercise

3Days 61–90

Restore an important service with protected backups and separate recovery credentials

OWNER

Continuity and platform teams

COMPLETION EVIDENCE

Successful restore, integrity checks, measured service readiness and business sign-off

Test customer-facing availability during a plausible provider or network failure	
OWNER Service and network owners	COMPLETION EVIDENCE Demonstrated fallback, measured user impact and tracked remediation
Review whether credible alerts were closed consistently and whether escalations found active issues	
OWNER CISO and assurance	COMPLETION EVIDENCE Sampled decisions, documented exceptions and assigned corrective work
Present the unresolved service risks and funding decisions to the board	
OWNER CISO with business owners	COMPLETION EVIDENCE Accepted risks, funded remediation and review dates

12.2 Identity operations: establish a defensible disposition

An intelligence signal should lead to a decision that another analyst can reproduce. Record which account or service matched, whether the account remains active, whether recent activity is suspicious and whether earlier remediation already addressed it. Preserve the signal without circulating personal data unnecessarily.

If unauthorised activity is corroborated, use the incident process to contain access, revoke relevant sessions and investigate persistence. The scope should follow the evidence. A broad password reset may be appropriate in some incidents, but an old advertisement alone does not establish the need.

Service-desk recovery deserves its own test. A caller may possess accurate personal or contractual details. Those details can make a request persuasive without establishing authority. Use approved independent verification and require additional approval for high-impact recovery or privilege changes.

Prefer phishing-resistant MFA for privileged and remote staff access where the service supports it. NCSC identifies FIDO2 credentials with local user verification as a phishing-resistant option. Test account recovery so it does not bypass the stronger sign-in control [S50].

12.3 Infrastructure teams: test controls in their actual service context

Passive email and web observations are leads for the relevant owner. A missing observed record is not automatically a missing control, and a visible record is not evidence that every service is protected. Validate the result against the organisation's actual domains, mail flows and platform configuration [S2].

For email authentication, identify legitimate senders before changing enforcement. Include transactional mail, delegated services and rarely used business systems. Record how exceptions are approved and removed. Test delivery while the policy changes, rather than measuring success only by the presence of a DNS record.

For edge devices, maintain model, hardware revision, firmware and support status. The CVE example in Chapter 7 shows why a product-family name is insufficient. Several hardware variants have different remediation options [S9][S10]. Require evidence that the intended version is installed, or that the unsupported device was replaced.

A recovery test should include the identities and dependencies required to restore the service. Protected data is only one requirement. The organisation also needs configuration, keys, approvals, communications and people who can work when normal collaboration services are unavailable.

12.4 Threat intelligence and the SOC: preserve evidence boundaries

Keep an actor's post, a third-party relay and an official disclosure as separate records. A relay may be useful for discovery, but it does not independently authenticate the original claim. A source that quotes a criminal figure does not turn it into an official figure.

When a new post resembles an older one, compare the propositions carefully. Matching wording supports a repost relationship. It does not establish that the same file changed hands or that the poster obtained fresh access. An alert should say which of these conclusions is supported.

Avoid distributing criminal contact information or victim samples in routine tickets. Provide the responsible team with the minimum evidence needed to assess relevance. Use a controlled evidence process for anything more sensitive, with access limited to the incident's needs.

Detection recommendations in this report are review and validation tasks. No untested detection rule is presented as production-ready. Teams should implement monitoring appropriate to their own platforms and check both expected detections and legitimate activity before relying on it.

12.5 Fraud teams: connect the customer and payment decisions

Customer-data disclosures and account-trading claims should be shared with fraud operations when they credibly concern the organisation. The useful question is whether an observed fraud route has changed, rather than whether a dramatic advertisement attracts attention.

Monitor account recovery, new-device activity, payee changes and transfer patterns together where lawful and proportionate. A warning should describe the action the customer should take. Advising customers to use an established contact route is more useful than asking them to identify an actor group.

Track false positives and customer harm alongside fraud outcomes. Added friction can delay legitimate payments or prevent access to an essential service. The business owner should understand both effects and approve the balance, with particular attention to vulnerable customers.

12.6 Leadership evidence at each checkpoint

Checkpoint	Leadership question	Evidence that answers it
Day 30	Do we know which services and identities matter most?	Service ownership, validated intelligence decisions and reporting matrix
Day 60	Have we removed the most consequential avoidable access paths?	Tested recovery verification, supplier permission review and applicable remediation evidence
Day 90	Can the business continue and recover under pressure?	End-to-end restore, availability exercise and business sign-off

A completed spreadsheet 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 the unresolved findings visible until their owners provide closure evidence.

12.7 How Brandefense can help

Odin by Brandefense connects external observations with evidence-led security decisions. Brandefense's threat intelligence, digital risk protection and external attack surface management capabilities can support assessment of relevant external signals. Scope, validation needs and response ownership should be agreed for the organisation's 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 completion evidence.

02

Escalate corroborated unauthorised activity while keeping unverified offers in a validation process.

03

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

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

What are the evidence boundaries, and where can a reader trace a finding?

4

appendices covering scope, evidence cards, sources and terminology

Appendix A. Sources, scope and confidence 90
Appendix B. Public evidence-card register 94
Appendix C. Sources 95
Appendix D. Glossary 98

Appendix A. Sources, scope and confidence

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

A.1 Window and snapshot

The post window is 1 January–22 November 2026. Post dates describe when material was published, rather than when an alleged intrusion occurred. The observation snapshot was taken when checked on 22 November. It cannot establish what was published during the remainder of that day.

The recent-activity section uses 9–22 November. A disclosure, an update, a listing and an incident can have different dates. The report states those distinctions where they affect interpretation. Older public material is used for context and clearly dated follow-ups, rather than silently added to a count of new 2026 incidents.

A.2 Dark-web evidence

Odin by Brandefense collected posts from monitored chat and forum sources. The country-tagged source population contains 1,075,323 posts. The retained case-analysis corpus contains 12,071 distinct posts and has different coverage. Neither measures the share of UK organisations targeted [S1].

A post is not a unique offer, an incident, a seller or a successful transaction. Country references can reflect global advertising, commentary or an organisation mentioned in passing. The report therefore uses the material as evidence of particular advertisements and claims, with their limitations preserved.

The public post cards contain redacted authentic excerpts or clearly labelled paraphrases. Translations are kept separate from original text. A translated claim is not an independently confirmed account. The public edition omits criminal contact routes, victim identifiers, personal data and downloadable samples.

A.3 Selected organisation universe and exposure

The portfolio comprises 250 selected UK-relevant domain estates across twelve sectors. It is purposive, rather than a national ranking or random sample. Related estates can share ownership, and multinational domains can include activity outside the UK [S2].

116 selected estates had a credential listed for sale when checked. The national Atlas headline is 61 out of 100. No sector or organisation rating is published. This headline is not an estimate of national prevalence or a probability of intrusion.

Exposure counts were read on 21 November 2026 UTC. Device, credential, listing-history and document observations are cumulative records held at that date, rather than exclusively 2026 events. Mention context covers the previous 365 days through 22 November.

Device totals are lower bounds. Employee-device associations sit within the device view. Credential sources, organisations and people can overlap. Associations do not establish ownership, active account validity or confirmed intrusions.

Passive observations cover 250 estates. Web-control results were available for 189 estates. Each observation keeps its own denominator, date and interpretation limits.

In the sector CSV, `estates_with_current_credential_listings` counts selected domain estates with current credential listings. It does not count distinct organisations or completed sales.

A.4 Passive observations

The available view covers public DNS, email policies, certificates and web controls. Counts retain the denominator relevant to each observation. Web-control results were available for 189 of the 250 selected estates [S2].

A published policy is not proof of complete enforcement. A key not observed is not proof of absent signing. A DS record is not complete DNSSEC validation. A public certificate result does not establish application security. Response intermediaries and service boundaries can affect what is observed [S44][S45].

The observations are time-specific validation leads. They do not establish unauthorised access or assess every service operated by a selected organisation. Owner records are needed to interpret an observation and choose a proportionate change.

A.5 Payment-card scope

Card material concerns only payment cards that appeared in clear text in the posts collected for this report. Brandefense detects stolen cards through other methods outside this scope. This material does not measure national card theft, active cards or fraud losses [S4].

The published subset contains 28 distinct card values in 33 posts. It is limited to material explicitly presented as UK-related. Country labels and current usability are not independently authenticated.

A card-related observation does not establish an intrusion into the issuer. Any response requires validation of relevance, currency and the applicable payment-provider evidence.

A.6 Extortion listings and comparators

Ransompedia supplied accepted listing records for the UK and four peers. The UK window contains 383 records. Dates are listing dates, not intrusion dates. Acceptance in the listing source is not independent confirmation that encryption, theft or payment occurred [S3].

Country classifications describe the source records. A multinational name does not establish which operating entity or population was affected. Repeated organisation labels also mean that listings cannot be interpreted as a count of distinct victim organisations.

The peers are Ireland, France, Germany and the Netherlands. They provide nearby economic and service contexts, rather than matched populations. The 2026 window is partial; the 2025 comparator is a complete year. No matched-period growth rate or probability ranking is inferred.

A.7 Original disclosures and incident families

The public-source evidence supports 12 incident families of UK relevance under the stated scope. Families group notices describing the same supplier or multi-brand event where the original evidence supports that relationship. They do not count every downstream customer as a separate intrusion.

Four families have explicit 2026 event dates, three have explicit 2026 detection dates and one has a 2026 supplier-disclosure window. Two rely on contemporary-year inferences, and two have no event date stated in the original notice.

The report also separates security defects without established misuse, accidental disclosures, older incidents with 2026 follow-ups, campaign warnings and unresolved claims. A global supplier incident does not enter the confirmed UK-relevant subset solely because UK organisations use its product.

Public-source coverage remains partial. The confirmed subset is bounded by the original passages that were read. Unresolved leads are not used to supply missing incident counts, affected populations or attributions.

A.8 Confidence and alternatives

High confidence is used for a narrowly stated observation directly supported by retained material or an original disclosure. It does not imply that every proposition in that material is true. For example, confidence can be high that an offer appeared while the authenticity of its contents remains unknown.

Moderate confidence identifies an interpretation with supporting evidence and a material remaining alternative. **Low confidence** identifies a plausible proposition with insufficient support for a stronger judgement. When an external source states its own confidence, the report attributes that assessment to the source.

Matching advertisements can support a repost relationship. Shared timing, language or country references do not establish common control. Forecasts remain conditional planning scenarios with evidence that would change the assessment.

A.9 Public naming and citations

An organisation is named as an incident victim only when original confirmation and widespread reporting were checked. This edition clears Manchester Airports Group and ASOS for that use. Other affected organisations remain described by roles. Source publishers and public authorities may be named in their publishing capacity.

An identifying article URL for a withheld organisation is replaced by the publisher's root with an article-withheld notice. The underlying article was read; the public citation intentionally does not identify it. Source titles and card text follow the same protection rule.

Each external source entry carries a verification date. CVE-2023-50224 was checked against NVD and the vendor's remediation advisory. Product variants and firmware scope are stated in Chapter 7; no general patch version is inferred for every affected device [S9][S10].

Appendix B. Public evidence-card register

Cards appear beside the analysis they support. Their identifiers do not disclose private source-record identifiers. Dates are post dates, and translations preserve the claim status.

Card	Date	Venue	Alias	Language	Chapter
B01	2026-11-10	Forum	Forum seller	English	4
B02	2026-10-05	Forum	Forum seller	English	4
B03	2026-08-30	Forum	News relay	Russian	4
B04	2026-08-23	Forum	Forum poster	English	4
B05	2026-10-03	Forum	Data seller	English	4
B06	2026-11-16	Forum	Data seller	English	4
B07	2026-11-13	Forum	Forum poster	English	4
B08	2026-11-02	Forum	Forum poster	English	4
B09	2026-11-05	Forum	Forum seller	English	4
B10	2026-08-22	Forum	Forum poster	English	4
B11	2026-10-21	Forum	Forum poster	English	4
B12	2026-01-03	Forum	Account seller	Turkish	8
B13	2026-01-04	Forum	Account seller	Turkish	8
B14	2026-01-07	Forum	Account-service advertiser	Russian	8
B15	2026-01-14	Forum	Account-service advertiser	English	8
B16	2026-01-09	Forum	Fraud-service advertiser	English	4
B17	2026-01-13	Forum	Forum commenter	English	4
B18	2026-01-06	Forum	Forum poster	English	4

The six detailed underground cases interpret the cited cards with chronology and alternative explanations. The six original-disclosure cases G–L use public source references rather than underground post cards.

Appendix C. Sources

The entries distinguish retained Brandefense observations from external publications. A verified-on date records the source check; it does not certify every assertion made by a criminal poster or every linked page.

Original notice URLs are withheld where their domains identify role-described organisations. Neutral publisher roots identify related coverage or context, as labelled below. Detailed incident accounts remain grounded in the original notices; precise source mappings remain private.

S1: Odin by Brandefense. Retained dark-web post observations. https://brandefense.io/ Underlying retained research data are private; the link identifies the publisher. 12,071 distinct retained posts; partial source coverage and source-level claim limits. Separate country-tagged source population: 1,075,323 posts. Verified on 22 November 2026.

S2: Odin by Brandefense. Atlas exposure and selected-domain passive observations. https://brandefense.io/ Underlying retained research data are private; the link identifies the publisher. 250 selected estates; 250 passive assessments; national Atlas headline 61; dated device, credential, listing and document associations. Verified on 22 November 2026.

S3: Odin by Brandefense. Ransompedia extortion listing snapshot. https://brandefense.io/ Underlying retained research data are private; the link identifies the publisher. 383 UK-labelled listings plus four regional peers; source acceptance is not independent incident confirmation. Verified on 22 November 2026.

S4: Odin by Brandefense. Payment-card post aggregates. https://brandefense.io/ Underlying retained research data are private; the link identifies the publisher. 28 distinct UK-labelled card values in 33 posts; narrow coverage and unverified country labels. Verified on 22 November 2026.

S5: NCSC. AI and critical-infrastructure resilience warning. https://www.ncsc.gov.uk/news/cyber-chief-uk-facing-ai-powered-attacks-on-critical-infrastructure-in-two-years Verified on 22 November 2026.

S6: NCSC. DDoS warning for UK organisations. https://www.ncsc.gov.uk/news/pro-russia-hacktivist-activity-continues-to-target-uk-organisations Verified on 22 November 2026.

S7: NCSC. APT28 router DNS interception advisory. https://www.ncsc.gov.uk/news/apt28-exploit-routers-to-enable-dns-hijacking-operations Verified on 22 November 2026.

S8: NCSC and partners. Covert device-network defensive advice. https://www.ncsc.gov.uk/news/international-cyber-agencies-fresh-advice-defend-against-china-linked-covert-networks Verified on 22 November 2026.

S9: NVD. CVE-2023-50224 vulnerability record. https://nvd.nist.gov/vuln/detail/CVE-2023-50224 Verified on 22 November 2026.

S10: TP-Link. CVE-2023-50224 legacy-product remediation advisory. https://www.tp-link.com/us/support/faq/5058/ Verified on 22 November 2026.

S11: ICO. Personal data breaches: a guide. https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/ Verified on 22 November 2026.

S12: UK legislation. NIS Regulations 2018, regulation 11. https://www.legislation.gov.uk/uksi/2018/506/regulation/11 Verified on 22 November 2026.

S13: UK legislation. NIS Regulations 2018, regulation 12. https://www.legislation.gov.uk/uksi/2018/506/regulation/12 Verified on 22 November 2026.

S14: UK legislation. NIS Regulations 2018, regulation 18. https://www.legislation.gov.uk/uksi/2018/506/regulation/18 Verified on 22 November 2026.

S15: UK Parliament. Cyber Security and Resilience Bill: stages. https://bills.parliament.uk/bills/4035/stages Verified on 22 November 2026.

S16: DSIT. Cyber Security and Resilience Bill summary. https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill Verified on 22 November 2026.

S17: FCA. Operational resilience: observations one year on. https://www.fca.org.uk/publications/good-and-poor-practice/operational-resilience-insights-observations-one-year Verified on 22 November 2026.

S18: PSR. APP fraud reimbursement protections. https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/ Verified on 22 November 2026.

S19: PRA, Bank of England and FCA. Cyber risk and resilience management consultation. https://www.bankofengland.co.uk/prudential-regulation/publication/2026/november/cyber-risk-and-resilience-management-consultation-paper Verified on 22 November 2026.

S20: Bank of England. Financial cyber-resilience consultation announcement. https://www.bankofengland.co.uk/news/2026/november/cyber-resilience-guidance-consultation-and-ai-and-quantum-effective-practices Verified on 22 November 2026.

S21: DataReportal. Digital 2026: United Kingdom. https://datareportal.com/reports/digital-2026-united-kingdom Verified on 22 November 2026.

S22: DSIT. Cyber Security Breaches Survey 2025. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025 Verified on 22 November 2026.

S23: House of Commons Library. Economic context and attribution evidence limits. https://commonslibrary.parliament.uk/research-briefings/impact-of-hostile-state-activity-on-the-uk-economy/ Verified on 22 November 2026.

S24: Ofcom. Telecommunications security enforcement responsibilities. https://www.ofcom.org.uk/internet-based-services/network-security/ofcom-begins-new-role-overseeing-security-of-telecoms-networks Verified on 22 November 2026.

S25: NCSC. Internet-exposed operational systems and edge devices. https://www.ncsc.gov.uk/news/disruptive-cyber-activity-highlights-risk-from-internet-exposed-systems-and-edge-devices Verified on 22 November 2026.

S26: Report Fraud. Online shopping account-abuse warning. https://www.reportfraud.police.uk/news/warning-for-online-shoppers/ Verified on 22 November 2026.

S27: Report Fraud. AI-assisted investment-impersonation warning. https://www.reportfraud.police.uk/news/alert-ai-enabled-investment-endorsement-schemes/ Verified on 22 November 2026.

S28: Report Fraud. Payment-diversion fraud warning. https://www.reportfraud.police.uk/news/criminals-steal-101-million-through-payment-diversion-fraud/ Verified on 22 November 2026.

S29: Report Fraud. Police-number impersonation warning. https://www.reportfraud.police.uk/null/news/alert-police-forces-being-impersonated-in-scam-calls/ Verified on 22 November 2026.

S30: ICO. Health-record access warning. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/11/uk-health-sector-warned-to-tackle-medical-record-snooping Verified on 22 November 2026.

S31: Public-service body. Scoped online-portal incident notice. Original notice URL withheld to protect a role-described organisation. Related reporting: https://www.itpro.com/ (article URL withheld). Original notice and related source verified on 22 November 2026.

S32: Manchester Airports Group. Customer-services data-security notice. https://www.manchesterairport.co.uk/help/data-security-incident/ Verified on 22 November 2026.

S33: NCSC. Incident affecting ASOS customers. https://www.ncsc.gov.uk/news/incident-affecting-asos-customers Verified on 22 November 2026.

S34: A university. Admissions-connection incident notice. Original notice URL withheld to protect a role-described organisation. Related reporting: https://security.geant.org/ (article URL withheld). Original notice and related source verified on 22 November 2026.

S35: A charity. Recipient-hosted supplier incident updates. Original notice URL withheld to protect a role-described organisation. Related regulatory context: https://www.fundraisingregulator.org.uk/ (article URL withheld). Original notice and related source verified on 22 November 2026.

S36: A public-service body. Case-management incident notice. Original notice URL withheld to protect a role-described organisation. Related official correspondence: https://www.parliament.uk/ (article URL withheld). Original notice and related source verified on 22 November 2026.

S37: A school. Original school-service disruption notice. Original notice URL withheld to protect a role-described organisation. Related reporting: https://www.computing.co.uk/ (article URL withheld). Original notice and related source verified on 22 November 2026.

S38: A household-goods retailer. Supplier incident affecting UK-store information. Original notice URL withheld to protect a role-described organisation. Related reporting: https://www.techradar.com/ (article URL withheld). Original notice and related source verified on 22 November 2026.

S39: A professional regulator. Information disclosed in error. Original notice URL withheld to protect a role-described organisation. Related official statement: https://www.professionalstandards.org.uk/ (article URL withheld). Original notice and related source verified on 22 November 2026.

S40: A university. Teaching-platform supplier incident update. Original notice URL withheld to protect a role-described organisation. Related supplier analysis: https://cybermonitoringcentre.com/ (article URL withheld). Original notice and related source verified on 22 November 2026.

S41: A public-service body. Filing-service security issue and dated investigation update. https://www.gov.uk/ Article URL withheld to protect a role-described organisation. Verified on 22 November 2026.

S42: A police force. Original non-emergency systems incident statement. Original notice URL withheld to protect a role-described organisation. Related reporting: https://www.sans.org/ (article URL withheld). Original notice and related source verified on 22 November 2026.

S43: Reuters. ASOS customer-notice reporting. https://www.reuters.com/business/retail-consumer/uks-asos-says-breach-exposed-some-customer-personal-data-2026-10-08/ Verified on 22 November 2026.

S44: NCSC. Email security and anti-spoofing. https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing Verified on 22 November 2026.

S45: RFC Editor. RFC 4034: DNSSEC resource records. https://www.rfc-editor.org/rfc/rfc4034.html Verified on 22 November 2026.

S46: A local authority. School-support platform ransomware response decision. Original notice URL withheld to protect a role-described organisation. Related reporting: https://www.itpro.com/ (article URL withheld). Original notice and related source verified on 22 November 2026.

S47: A fashion retailer. Original customer-data incident FAQ. Original notice URL withheld to protect a role-described organisation. Related reporting: https://www.retailgazette.co.uk/ (article URL withheld). Original notice and related source verified on 22 November 2026.

S48: A fashion retailer. Related group-brand incident FAQ. Original notice URL withheld to protect a role-described organisation. Related reporting: https://www.retailgazette.co.uk/ (article URL withheld). Original notice and related source verified on 22 November 2026.

S49: RFC Editor. RFC 6797: HTTP Strict Transport Security. https://www.rfc-editor.org/rfc/rfc6797.html Verified on 22 November 2026.

S50: NCSC. Recommended types of multi-factor authentication. https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/recommended-types-of-mfa Verified on 22 November 2026.

S51: W3C. Content Security Policy Level 2, Introduction. https://www.w3.org/TR/CSP2/ Verified on 22 November 2026.

Appendix D. Glossary

Term	Plain meaning
Account recovery	The process for regaining account access after normal sign-in fails or credentials are lost
Actor claim	An assertion by a poster or criminal service that has not been independently established merely by publication
Atlas	Brandefense external exposure rating; this report publishes its national headline for the selected portfolio [S2]
APP fraud	Authorised push payment fraud, where a person is deceived into transferring money to a fraudster [S18]
Combolist	A collection of login details whose origin, age and validity may vary
Credential-record association	A record linked to a selected domain, with current account validity and unique person counts unestablished
Credential stuffing	Attempting account access with credentials reused from other services [S26]
CRM	Customer relationship management, a service holding contact and relationship records
CSP	Content Security Policy; restricts the content sources a browser may load [S51]
DDoS	Distributed denial of service, activity intended to exhaust a service so legitimate users cannot use it [S6]
DKIM	Email signatures that help a recipient check the signing domain and message integrity [S44]
DMARC	A domain's published email-authentication policy and reporting framework [S44]
DNSSEC	DNS security extensions that support authentication of DNS data [S45]
DS record	A delegation signer record linking a DNS delegation to its signing key [S45]
Domain estate	The selected public domain and services associated with it, rather than every system in a corporate group
Employee-device association	A device record associated with an employee-classified account, whose ownership and current state require validation
Extortion listing	A public criminal claim associating an organisation with an extortion demand or alleged data exposure

Term	Plain meaning
HSTS	A web policy telling supporting browsers to use HTTPS for the covered host [S49]
Impact tolerance	The maximum tolerable disruption to an important business service, assessed against potential harm [S17]
Important business service	A service whose disruption could cause intolerable customer harm or relevant market or financial-system harm [S17]
In short	The opening decision summary for a chapter
Listing label	The group or country classification attached to a source record, rather than independent attribution
MFA	Multi-factor authentication, sign-in requiring more than one authentication factor
NIS	The UK's Network and Information Systems regulatory framework, with service-specific applicability [S12][S13]
OT	Operational technology used to monitor or control physical processes [S25]
Payment diversion	Fraud that changes where a legitimate payment is sent [S28]
PECR	Privacy and Electronic Communications Regulations, including separate communications-provider breach reporting [S11]
Post card	A redacted evidence excerpt with source context, what is held and what remains unestablished
Relay	A third party's repetition of another source's claim
SPF	A domain's record identifying authorised email-sending systems [S44]
TLP:CLEAR	A sharing label permitting unrestricted distribution, subject to other applicable obligations
UK GDPR	The UK data-protection framework, including risk-based personal-data-breach notification [S11]

About this report

Prepared by Odin by Brandefense. Version 1.0 · Brandefense Country Report · United Kingdom 2026.

The intended post window is 1 January–22 November 2026. The observation snapshot reflects material available when checked on 22 November, with coverage limits stated in Appendix A. This edition distinguishes advertisements, extortion listings, public control observations, original disclosures and analyst interpretations.

The report takes no political position. State links and motives remain attributed to the cited source or claimant. Recommendations are proposed actions for readers; they do not state that an assessed organisation has or has not implemented them.

This is the English master. No translated edition is produced for this package. The AI-assisted notice on the cover applies to research and drafting.

© 2026 Brandefense. All rights reserved.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

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

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

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

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

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

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

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

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

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

TÜRKIYE

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

BRANDEFENSE.IO