BRANDEFENSE COUNTRY REPORT · IRELAND 2026

Brandefense Ireland Cyber Threat Landscape Report 2026

Identity, shared suppliers and the continuity of everyday services

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

250
selected estates across eleven sectors

6
detailed claim dossiers, separate from public disclosures

10
detailed disclosure dossiers, with separate occurrence and publication dates

32
Ireland-labelled extortion listings in the research window

CONTENTS

Contents

01	Executive summary	06
	Report map	10
02	Ireland's digital services and shared dependencies	11
03	The selected organisation portfolio and security controls	15
04	What the retained dark-web evidence establishes	26
05	Incident disclosures and sector decisions	43
06	Hacktivist claims, disruption and public communications	56
07	Threat actors and extortion listing claims	62
08	Identity, accounts and the fraud economy	71
09	Financial services: data, suppliers and customer trust	76
10	Regulatory duties and national response	81
11	Outlook and assessment-change signals	86
12	A 30/60/90-day action plan	90
A	Appendix A. Scope, sources and interpretation	98
B	Appendix B. Post evidence register	102
C	Appendix C. Sources	103
D	Appendix D. Plain-language glossary	107
	About this report	110

Board	01 05 11 12
CISO	03 04 05 12
SOC and intelligence	04 06 07 B
Fraud and customer teams	05 08 09
Legal and privacy	05 10 A
Facilities and operations	05 06 12

About this edition

English master edition. No translated edition accompanies this report.

AI-assisted research and drafting. Observations, actor claims, original disclosures and analyst judgements are distinguished.

Irish disclosures connect supplier-held information, identity decisions and interrupted services; the response begins with verified scope and recoverable operations.

32

Ireland-labelled extortion listing claims, not confirmed intrusions

45/100 (B)

National Atlas headline for 250 selected estates

12

public incident families with Irish relevance and explicit date limits

4

listing claims dated 8–22 November in the retained snapshot

Contents and reading routes

Chapter	Question	First reader
1. Executive summary	What should leaders decide first?	Board and CISO
2. Ireland's digital services and shared dependencies	Which identities and dependencies matter?	Security leadership
3. The selected organisation portfolio and security controls	What do exposure signals and public controls establish?	Exposure and service owners
4. What the retained dark-web evidence establishes	What is claimed, held and unverified?	Threat intelligence
5. Incident disclosures and sector decisions	What do original accounts establish by sector?	Business and data owners
6. Hacktivist claims, disruption and public communications	What separates impact, cause and responsibility?	Operations and communications
7. Threat actors and extortion listing claims	Which labels and comparisons have evidence?	SOC and intelligence
8. Identity, accounts and the fraud economy	How do data and apparent trust affect authorisation?	Fraud and customer teams
9. Financial services: data, suppliers and customer trust	Which decisions need coordinated ownership?	Financial security leaders
10. Regulatory duties and national response	Which scope and clock apply?	Legal and privacy
11. Outlook and assessment-change signals	What evidence would change the assessment?	Leadership and planning
12. A 30/60/90-day action plan	Who acts and what demonstrates completion?	All owners
Appendix A. Scope, sources and interpretation	What do the evidence populations mean?	All readers
Appendix B. Post evidence register	Which retained posts support the evidence cards?	Threat intelligence
Appendix C. Sources	Which sources support each statement?	All readers
Appendix D. Plain-language glossary	What do technical and reporting terms mean?	All readers

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

Observed means the relevant post, record or observation is held. **Claimed** means an advertiser or listing asserts something. **Officially disclosed** means the identified organisation or authority published or supplied the stated account. **Analyst judgement** identifies an implication while preserving missing proof.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which decisions follow from Ireland's evidence and what should leaders validate first?

4

decisions with accountable owners

Four decisions for leaders 08

The year in numbers 08

CHAPTER 01

Executive summary

IN SHORT

Ireland's disclosures connect supplier-held information, identity decisions and service continuity. The report covers twelve public incident families with date and scope limits, plus six detailed underground claim dossiers. Ransompedia adds thirty-two Ireland-labelled listing claims. Across 250 selected estates, the national Atlas headline is 45/100 (B), 48 have a current credential listing, and 176 publish quarantine or reject DMARC policies. Validate relevant accounts, establish provider scope, strengthen mail and DNS controls, protect recovery and prove restoration of an important service.

The report combines retained Brandefense Blackhole posts, Ransompedia listings, a selected-estate portfolio and source-checked public reporting. These are different populations. A country tag, an advertisement, a listing and a confirmed disclosure cannot be added into one national attack count [S1][S2][S3][S4].

1. Supplier boundaries determine the first useful question. Financial, education, healthcare and hospitality disclosures concern different provider-held information and services. The relevant question is which tenant, data and operation were affected. Several customer notices can describe one provider event. They do not independently demonstrate an intrusion into every customer's own network [S24][S26][S33][S53].

2. Recent disclosures require chronology as well as urgency. November financial-supplier notices describe earlier October activity. The hospitality case has a November event, statement and regional report. A recent publication can change customer protection without establishing a newly started attack. The 8–22 November section preserves those dates [S26][S30][S53].

3. Visible market claims need proposition-level validation. The retained material includes service-provider data allegations, website records, commercial communications, administration access and recent phishing advertising. Some record previews predate their claim year. Some apparent offers are comments under older threads. Neither a confident title nor repeated publication supplies independent authentication [S1].

4. Operational disruption requires service-specific recovery evidence. Irish grocery refrigeration impact and the Irish consequences of global manufacturing incidents support different continuity decisions. A controller returning online, an account returning and a production line returning are different tests. Keep the business owner involved in the recovery decision [S20][S22][S31].

5. Exposure signals and public controls identify concrete ownership gaps. Forty-eight of 250 selected estates had a credential listed for sale when checked, and the national Atlas headline is 45/100 (B). Across all 250 estates, 176 (70.4%) publish quarantine or reject DMARC policies while 74 remain in monitoring mode or lack valid records, and only 7 (2.8%) publish DNSSEC delegation. Ransompedia separately records thirty-two Ireland-labelled listing claims, including four dated 8–22 November [S2][S3].

Four decisions for leaders

1. **Assign current-account validation.** Route credible owned-account signals to identity operations. Record account status, relevant activity and previous remediation before choosing containment. Escalate when unauthorised activity is corroborated.
1. **Make supplier scope usable early.** For providers holding important information or service permissions, agree a named incident contact and an initial information checklist. Test a notice that arrives before every forensic question is settled.
1. **Protect recovery and payment decisions.** Test an informed impersonator against contact-centre recovery, registered-device changes and beneficiary changes. Preserve an independent verification route and a controlled path for legitimate customers.
1. **Prove a complete service restoration.** Restore an important service through protected recovery access. Reconcile its information and permissions, then obtain business-owner acceptance against the service's own recovery objective.

The year in numbers

These rows describe separate populations and must not be added together.

32

Ireland-labelled extortion listings in the 2026 window [S3]

WHAT IT IS NOT

Confirmed intrusions, distinct victims or complete national ransomware activity

21

Ireland-labelled listing records in the whole of 2025 [S3]

WHAT IT IS NOT

A matched-duration growth baseline

4

Listing claims dated 8–22 November [S3]

WHAT IT IS NOT

Four attacks that necessarily began during the recent window

35,915

Reported Ireland-tagged post volume [S1]

WHAT IT IS NOT

Verified targeting or successful attacks

49,723

Distinct retained narrative posts [S1]

WHAT IT IS NOT

Unique sellers, datasets or transactions

45/100 (B)

National Atlas headline for the selected portfolio [S2]

WHAT IT IS NOT

A breach percentage, intrusion probability or sector ranking

250

Selected domain estates across eleven sectors [S2]

WHAT IT IS NOT

Independent legal entities, an official ranking or national prevalence

176 / 250

Selected estates publishing quarantine or reject DMARC policies [S2]

WHAT IT IS NOT

Proof of message-level enforcement or national prevalence

10

Detailed public-disclosure dossiers in Chapter 5

WHAT IT IS NOT

A census of Irish victims or attacks beginning in 2026

6

Detailed claim dossiers in Chapter 4 [S1]

WHAT IT IS NOT

Six independently authenticated incidents

12

Public incident families with Irish relevance

WHAT IT IS NOT

Twelve new intrusions with fully established occurrence dates

12

Public post evidence cards [S1]

WHAT IT IS NOT

Twelve independent incidents or original sellers

The twelve public families include the ten detailed dossiers, a scoped police social-account disclosure and a public-authority employee-contact supplier disclosure. One outage with a disputed cause and historical enforcement events remain outside that family count [S36][S55][S57].

KEY TAKEAWAYS

01

Keep claims, listings, selected estates and public disclosures separate.

02

Validate provider and account scope before inferring a wider incident.

03

Fund recovery, customer protection and timely factual reporting with named owners.

Report map

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

Board	Which service risk needs investment or acceptance?	01 05 11 12
CISO	Which credible signals or dependencies lack an owner?	03 04 05 12
SOC and intelligence	Which proposition is supported and how can it be checked?	04 06 07 B
Fraud and customer teams	Which recovery or payment request needs independent verification?	05 08 09
Legal and privacy	Which scope, awareness time and reporting duty apply?	05 10 A
Facilities and operations	Which remote connection or provider can interrupt safe service?	05 06 12

01 Summary
Leadership decisions and the evidence behind them

02 Context
Identity, supplier, institutional and geographic boundaries

03 Portfolio
Selected-estate exposure signals and passive security controls

04 Dark web
Advertisements, record dates and claim validation

05 Disclosures
Public service and data scope with separate date types

06 Disruption
Impact, cause, responsibility and trusted communications

07 Actors
Listing labels and supported evidence relationships

08 Fraud
Data demand, impersonation and payment decisions

09 Finance
Provider, recovery, customer and reporting ownership

10 Regulation
Applicable duties, clocks and historical enforcement

11 Outlook
Conditional scenarios and assessment-change evidence

12 Actions
Accountable owners and reviewable completion

CHAPTER 02

Ireland's digital services and shared dependencies

THIS CHAPTER ANSWERS

Which features of Ireland change the decisions that security leaders need to make?

79%

surveyed internet users used electronic identification in the 2025 CSO baseline

2.1 Digital adoption makes recovery part of service delivery 12

2.2 A supplier can hold data without controlling the whole service 12

2.3 Connected equipment joins security to physical operations 13

2.4 Institutions and reporting routes have different jobs 13

2.5 Geographic and political boundaries remain explicit 13

CHAPTER 02

Ireland's digital services and shared dependencies

IN SHORT

Ireland's public services, finance, education and manufacturing depend on identities and suppliers that cross organisational boundaries. Disclosures in this report concern several different failure modes, including supplier-held information, interrupted production and connected refrigeration. A service can stop without evidence that its own core network was accessed. Build separate maps of data, access and recovery dependencies, then test the person responsible for each decision.

2.1 Digital adoption makes recovery part of service delivery

The Central Statistics Office published its digital public-service findings on 11 February 2026 using 2025 survey experience. Among internet users, 79% used electronic identification. Among those users, 92% used it for public services. These are adoption figures with different denominators, rather than measurements of security failures during 2026 [S5].

The planning consequence is straightforward. A citizen who cannot regain a trusted identity may also lose practical access to an important service. A fraudulent recovery decision can expose that service even where normal sign-in is well protected. Identity recovery should therefore have a business owner, an exception process and an independently verified contact route.

Do not make recovery depend entirely on information that other organisations legitimately hold. Names, addresses and account relationships can appear in administrative records or commercial databases. Possession of those details should not, by itself, authorise a new device, a new contact number or a payment change.

The CSO also reports that 94% of internet users in its relevant 2025 population used internet banking. That population is people who had used the internet in the preceding three months. It is not every resident or every household [S6]. Security and fraud teams should assess the complete customer journey, including enrolment, support, payments and recovery.

2.2 A supplier can hold data without controlling the whole service

The financial, education and healthcare cases in Chapter 5 show different supplier relationships. A platform may hold saved beneficiary information, a learning service may hold staff and student information, and an administrative supplier may receive records. These are distinct data and operational dependencies.

A useful supplier map records four questions. Which information does the provider receive? Which permissions can it exercise? Which business process stops if access is suspended? What evidence permits reconnection? The answers should identify operational contacts as well as contractual counterparties.

Group ownership complicates the same analysis. This report's selected estates can include parent groups, operating brands and international services. A record associated with a group domain cannot automatically be assigned to an Irish employee or an Irish legal entity. That boundary applies to both exposure observations and public incident reporting.

For a multinational incident, this report requires evidence of Irish relevance before describing an Irish operational consequence. A global announcement can establish a company incident. It cannot supply a country-specific data total merely because the company has a local office.

2.3 Connected equipment joins security to physical operations

NCSC's November refrigeration advisories describe the risk of public-facing management interfaces and unauthorised configuration changes. Its later advisory distinguishes continuing incidents from separately published vulnerability research. This distinction matters when assessing the Irish grocery disruption [S13][S14].

A facilities owner may need a different response from a desktop administrator. Removing remote access can affect maintenance, alarms and operating conditions. The decision should involve the person who understands safe equipment operation, the network owner and the service provider.

An inventory limited to employee computers can miss these dependencies. Ask who can change operating parameters, who receives alarms and how an operator notices a harmful change when a digital alarm is also altered. Record a safe fallback before making a remote-management change.

2.4 Institutions and reporting routes have different jobs

NCSC provides technical coordination and guidance. Its incident-reporting page distinguishes cybersecurity incidents from cybercrime, and identifies An Garda Síochána as the reporting route for cybercrime. It also explains that incident support depends on constituency and circumstances [S42].

The Data Protection Commission addresses personal-data obligations. The Central Bank of Ireland provides reporting arrangements for financial entities within DORA's scope. Contacting one of these bodies does not automatically complete every other reporting duty [S8][S10]. Chapter 10 separates the relevant decisions.

Ireland's NIS2 transposition should not be described as complete merely because the European directive exists. Re-checked on 27 November 2026, NCSC's NIS2 page still carries a 24 June 2025 update date. It notes that registration and incident-reporting portals are not yet available and that the earlier regime continues for already designated operators. This report does not infer a new Irish commencement date from that page [S7].

2.5 Geographic and political boundaries remain explicit

Ireland and the United Kingdom are separate comparison populations in this report. A cross-border supplier can support customers in both jurisdictions. Its location does not decide where each customer's data or service impact belongs. Northern Ireland-only events do not enter the Ireland incident set without an established Irish nexus.

State responsibility, ideological alignment and motivation require their own evidence. Language, a country tag, a slogan or a claimant's chosen name does not establish any of them. Where a source supplies an attribution, the report identifies that source and preserves its limits.

The report takes no position on Northern Ireland, UK relations, elections, foreign conflicts or government decisions. Actor rhetoric is omitted where it adds no technical or defensive value. Events appearing near one another in time are not treated as a common campaign without a concrete evidential connection.

KEY TAKEAWAYS

01

Identity recovery is part of delivering a dependable digital service.

02

Map supplier data, permissions and recovery responsibilities separately.

03

Preserve geographic scope and source attribution when describing cross-border incidents.

CHAPTER 03

The selected organisation portfolio and security controls

THIS CHAPTER ANSWERS

What do exposure signals and public security controls establish across Ireland's 250 selected estates?

250

selected estates across eleven sectors

3.1 Universe card 16
3.2 The sector scope remains visible 17
3.3 Exposure categories need separate validation 19
3.4 Public security controls across 250 selected estates 21
3.5 Signals and configuration findings need owned verification 24
3.6 What a supported future result must preserve 24

CHAPTER 03

The selected organisation portfolio and security controls

IN SHORT

The portfolio contains 250 selected domain estates across eleven sectors. It is a purposive service-relevance sample, not an official ranking or national prevalence study. The national Atlas headline is 45/100 (B), with 48 estates carrying a current credential listing. Passive security-control checks show 176 estates publishing quarantine or reject DMARC policies, 233 of 242 checked presenting valid TLS, and 7 publishing DNSSEC delegation. Keep estate scope clear, validate relevant account evidence and move monitoring or missing mail policies to enforced handling.

3.1 Universe card

Item	Definition
Selected population	250 Irish-relevant public, commercial and service-provider domain estates
Sector cells	Eleven sectors
Selection	Purposive institutional, service and market relevance; not a turnover ranking
Unit	Selected primary domain estate, not necessarily an independent organisation
Ownership limits	Related brands, parent groups and international services can overlap
Country limit	A domain association does not establish Irish residence or employment
Observation dates	Exposure observations recorded on 23 November 2026; passive security-control checks completed on 27 November 2026
Security-control coverage	All 250 estates resolved and checked for DNS, mail policy, TLS (242 checked, 8 unavailable) and web headers (207 available, 43 unavailable)
Exposure coverage	Snapshot associations and estates with current credential listings; separate category units
Interpretation	Unavailable TLS or HTTP responses are neither zero exposure nor evidence of a failed control

[S2]

The sample includes government services, local authorities, education, healthcare, finance and commercial operations. It identifies a portfolio for bounded analysis. Inclusion is not a finding of a weakness or an incident.

For an international provider, a global domain can serve customers and employees in several countries. An association with that domain does not automatically identify a local user. A domain can also represent several legal entities, while one organisation can operate several domains.

3.2 The sector scope remains visible

SCOPE OF THE CARD FIGURES

These exposure figures describe 250 selected Irish-relevant domain estates checked on 23 November 2026, paired with passive security-control checks on 27 November 2026. They are not national prevalence estimates or independent legal entities.

48 of 250 selected estates had a credential listed for sale when checked. Across the same portfolio, 195 estates (78.0%) had device associations and 129 (51.6%) had employee-device associations. In addition, 244 estates (97.6%) had historical credential records, 102 (40.8%) had document associations and 171 (68.4%) had similar-domain associations [S2].

The table keeps the selected-estate denominator beside each signal. Device and credential associations can overlap across related estates and historical records. They are not unique devices, people or newly occurring Irish intrusions. No sector ratings are published.

Sector	Selected estates	Current credential listings	Estates with device associations	Estates with employee devices	Estates with document associations	Device associations	Credential records
Public services	30	4	23	16	11	1,798	68,706
Local government	31	1	21	12	5	477	35,854
Financial services	30	9	28	16	15	55,695	430,729
Education and research	25	3	23	19	16	9,328	855,546
Healthcare	20	1	13	11	6	1,183	126,031
Transport and logistics	20	4	14	11	7	23,847	54,792
Energy and utilities	15	3	13	7	3	4,010	29,690

Sector	Selected estates	Current credential listings	Estates with device associations	Estates with employee devices	Estates with document associations	Device associations	Credential records
Telecom and digital services	15	7	15	12	11	22,830	215,610
Retail and consumer services	20	12	19	6	6	11,149	43,231
Industry food and construction	20	1	12	11	12	340	76,221
Media and tourism	24	3	14	8	10	1,118	43,970
ALL	250	48	195	129	102	131,775	1,980,380

Device figures are minimum observed counts. They do not establish the full number of associated devices [S2].

Current credential listings and exposure signals across 250 selected Irish estates

	Current listings	With devices	Employee devices	With credentials	With documents
Public services	4/30	23/30	16/30	27/30	11/30
Local government	1/31	21/31	12/31	31/31	5/31
Financial services	9/30	28/30	16/30	30/30	15/30
Education and research	3/25	23/25	19/25	25/25	16/25
Healthcare	1/20	13/20	11/20	20/20	6/20
Transport and logistics	4/20	14/20	11/20	18/20	7/20
Energy and utilities	3/15	13/15	7/15	15/15	3/15
Telecom and digital services	7/15	15/15	12/15	15/15	11/15
Retail and consumer services	12/20	19/20	6/20	20/20	6/20
Industry food and construction	1/20	12/20	11/20	20/20	12/20
Media and tourism	3/24	14/24	8/24	23/24	10/24

Current credential listings by sector (coral). Each cell shows estates with the signal / selected estates; signals overlap. Source: Brandefense exposure observations for 250 selected Irish estates, 23 November 2026 snapshot [S2]. Cumulative associations can overlap across related estates; device figures are minimum observed counts, not unique people or confirmed intrusions.

[S2]

The selected portfolio's national Atlas headline is 45/100 (B). Higher values indicate greater observed exposure in this selected portfolio. This is not a breach percentage, a probability of intrusion or a certification of effective controls. Only the national rating is published; sector rows describe separate signal counts [S2].

Separate from the national Atlas headline, §3.4 presents passive email, DNS, TLS and web-header observations across all 250 estates alongside the analytical passive hygiene index [S2].

3.3 Exposure categories need separate validation

Observation type	What a relevant observation could support	What it would not establish alone
Current credential offer	An account-validation lead for the named owned service	Working access or completed sale
Employee-device association	A check against managed assets and current identities	Current infection or device ownership
Other device association	Customer, shared-service or historical investigation	Employee infrastructure involvement
Credential record	Freshness and previous-remediation review	An active password or a new 2026 event
Document association	Data-owner review of sensitivity and availability	Unauthorised access or confidential contents
Similar domain name	Ownership and possible impersonation review	Malicious registration or actual abuse
Organisation mention	Context for a particular public statement or claim	Targeting or an incident

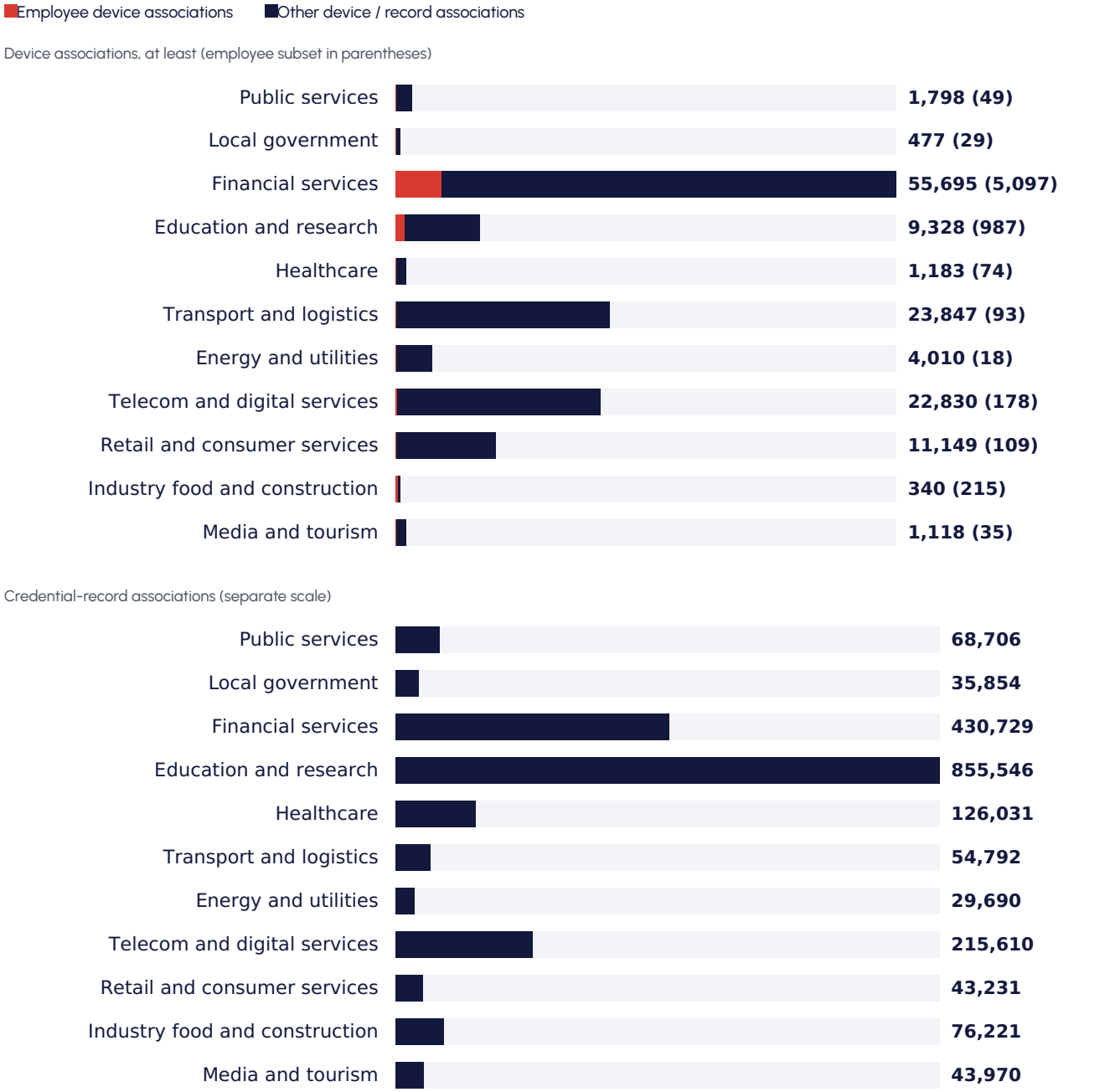
The snapshot contains at least 131,775 device associations: 6,884 employee-device associations (5.2%) and 124,891 other device associations (94.8%). Associated devices hold at least 2,043,630 credential records across all services. This device-held total counts credentials for any service on associated devices and is a different measure from the 1,980,380 estate-linked credential records below. The snapshot also holds 793 document associations across 102 estates [S2].

Historical credential-record associations total 1,980,380 across 244 estates. Combolist entries account for 946,283 records (47.8%), breach-database entries account for 891,940 (45.0%) and stealer-log entries account for 142,157 (7.2%). Each category retains its own unit and may overlap across related estates [S2].

Totals are heavily skewed by a few large estates. The median estate holds 10.5 device associations and 943 credential records. Across the portfolio, the top two estates hold 35.2% of credential records, rising to 84.7% in telecom, 82.5% in financial services and 80.0% in healthcare [S2].

The similar-domain population contains 13,587 associations across 171 estates for 19 October–18 November. Some name matches can be unrelated. A similar name is not proof of malicious ownership, and several selected brands can relate to the same name. That period differs from the main post window [S2].

Device and credential-record associations concentrate in financial services, education, telecom and transport



Panels use independent scales; overlapping populations are never added together. Source: Brandefense exposure observations for 250 selected Irish estates, 23 November 2026 snapshot [S2]. Cumulative associations can overlap across related estates; device figures are minimum observed counts, not unique people or confirmed intrusions.

Rolling 365-day mention context (19 November 2025–18 November 2026) records 428 chat mentions across 28 estates (11.2%) and 266 web mentions across 36 estates (14.4%). Financial services (230), healthcare (75) and transport (69) lead chat mentions; media and tourism (69), financial services (68) and education (67) lead web mentions. Mentions can repeat across estates and do not establish targeting or incidents [S2].

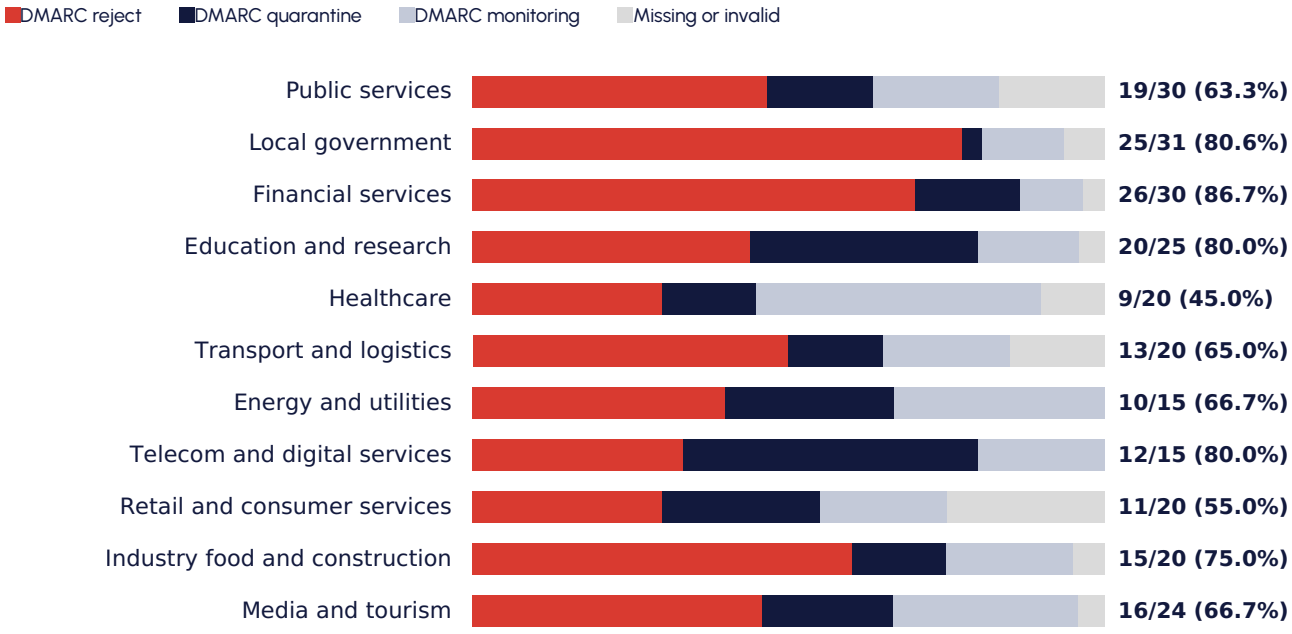
A cumulative record can be useful without being current. The identity team should establish the relevant account and service, compare the signal with past remediation and identify present activity. The response depends on that assessment, rather than on the apparent size of an external record collection.

Device associations also require an ownership decision. A customer device and an employee device lead to different response functions. Do not assign every reference to a financial-service domain to the bank's internal endpoint estate.

3.4 Public security controls across 250 selected estates

Passive DNS, mail-policy, certificate and web-header observations completed on 27 November 2026 cover all 250 selected estates. Published policies and public responses show baseline configuration posture, with strict interpretation limits [S2].

Financial services and local government lead enforced DMARC policies while healthcare and retail lag



Bar lengths show sector share; labels show enforced (reject or quarantine) / selected estates. Source: passive DNS and mail-policy observations for 250 selected Irish estates, 27 November 2026 snapshot [S2]. Published policies do not establish message-level enforcement or national prevalence.

Sector	Estates	DMARC reject	DMARC quarant-ine	DMARC monitor-ing	DMARC missing	SPF	DKIM	DNSSEC DS	Valid TLS	HSTS (of avail-able)
Public services	30	14	5	6	5	28	21	0	25	16 of 19
Local govern-ment	31	24	1	4	2	29	22	0	29	18 of 28

Sector	Estates	DMARC reject	DMARC quarant-ine	DMARC monitor-ing	DMARC missing	SPF	DKIM	DNSSEC DS	Valid TLS	HSTS (of avail-able)
Finan-cial ser-vices	30	21	5	3	1	29	19	2	28	16 of 24
Educa-tion and re-search	25	11	9	4	1	25	24	1	25	15 of 22
Health-care	20	6	3	9	2	18	11	0	18	9 of 18
Trans-port and lo-gistics	20	10	3	4	3	17	16	0	19	14 of 17
Energy and util-ities	15	6	4	5	0	15	13	0	15	13 of 15
Tele-com and di-gital services	15	5	7	3	0	15	14	0	14	9 of 13
Retail and con-sumer services	20	6	5	4	5	20	15	1	19	8 of 11
Industry food and con-struc-tion	20	12	3	4	1	19	14	2	18	10 of 17
Media and tourism	24	11	5	7	1	24	24	1	23	11 of 23
ALL	250	126	50	53	21	239	193	7	233	139 of 207

DMARC missing combines 20 estates with no DMARC record and 1 with an invalid record. TLS validation covers 242 checked estates (233 valid, 9 failed validation and 8 unavailable). HSTS uses 207 estates with available HTTP responses (43 unavailable) [S2].

Email policy. Across 250 estates, 176 (70.4%) publish DMARC policies requesting rejection (126, 50.4%) or quarantine (50, 20.0%) [S2][S44]. Another 53 estates (21.2%) remain in monitoring mode, and 21 (8.4%) have no valid DMARC record (20 missing, 1 invalid). Financial services (26 of 30, 86.7%) and local government (25 of 31, 80.6%) lead enforcement. Healthcare (9 of 20, 45.0%), retail and consumer services (11 of 20, 55.0%) and public services (19 of 30, 63.3%) carry the largest gaps. Public services (5) and retail (5) account for 10 of the 21 missing or invalid records [S2].

Foundational prerequisites are widely deployed. SPF appears on 239 of 250 estates (95.6%): 157 publish hard-fail records, 73 publish soft-fail records and 9 use other qualifiers, leaving 11 missing [S2][S45]. Public DKIM records were observed on 193 estates (77.2%) [S2][S46]. On mail routing, 111 estates (44.4%) use Microsoft 365, 11 (4.4%) use Google, 121 (48.4%) use other or self-managed gateways and 7 (2.8%) publish no MX record [S2]. A published policy is not proof of alignment or message-level enforcement, and missing public DKIM records do not prove mail goes unsigned.

DNS and certificates. DNSSEC delegation records (DS) appear on only 7 of 250 estates (2.8%), with zero across public services, local government, healthcare, transport, energy and telecom [S2][S47]. Certification Authority Authorization (CAA) records appear on 22 estates (8.8%) [S2]. TLS handshakes completed on 242 of 250 estates (8 unavailable). Of those 242, 233 (96.3%) presented valid certificates (189 using TLSv1.3 and 44 using TLSv1.2; zero deprecated protocols). Nine estates (3.7%) failed certificate validation: 3 expired certificates, 3 hostname mismatches, 2 incomplete certificate chains and 1 self-signed certificate [S2].

Web policy. Available HTTP responses were recorded for 207 of 250 estates, while 43 were unavailable [S2]. Among those 207 responses, 139 (67.1%) set HTTP Strict Transport Security (HSTS) and 96 (46.4%) set Content Security Policy (CSP) [S2][S48][S49]. X-Content-Type-Options appeared on 141 responses (68.1%) and X-Frame-Options on 136 (65.7%). Unavailable TLS or HTTP responses are not misconfigurations, and a valid certificate or header does not establish application security. Owners should test browser-policy changes with dependencies and preserve a rollback route before deployment.

Passive hygiene index. The Odin passive hygiene index is an analytical composite of email, DNS, TLS and web-header checks on a 0–100 scale, where higher values indicate weaker hygiene. It is a model, not an Atlas rating. Across the 250 estates, the national index value is 36 [S2]. Across sectors, hygiene index values are strongest in financial services (29) and education and research (29), followed by energy and utilities (31) and local government, industry and telecom (33 each). Values are weakest in healthcare (47) and public services (40), followed by retail (38), transport (37) and media and tourism (36) [S2].

3.5 Signals and configuration findings need owned verification

Question	First owner	Useful evidence
Does an advertised account belong to an active owned service?	Identity operations	Account status, relevant activity and previous remediation
Does a device association identify a managed endpoint?	Endpoint response	Asset inventory, user relationship and incident evidence
Is a mail-policy observation the effective policy?	Messaging	Current configuration and representative authorised messages
Does a web change protect the intended service safely?	Application owner	Tested behaviour and dependency acceptance
Does a provider hold information that changes customer risk?	Data and supplier owners	Service-specific records and confirmed information categories
Can an important service be restored safely?	Business and infrastructure owners	Complete recovery exercise with integrity checks

The board should ask for unresolved relevant tasks and their owners, rather than interpret an empty table as a low-risk result. A good closure record can explain that a signal was historical, unrelated, remediated or still unresolved.

3.6 What a supported future result must preserve

A later observation needs its date, population and unit. A device-association volume, a count of estates with a signal and a count of unique people are different quantities. They must not share a headline without the necessary qualification.

Sector results should remain signal counts with a clear denominator. Related organisations and international services can overlap, so a portfolio total must not become an estimate of national prevalence. The narrative, cards and chart data should carry the same limits.

This is an evidence boundary, rather than a reason to postpone essential controls. The public disclosures already justify testing supplier access, identity recovery and operational continuity. Each organisation can perform those authorised checks with its own records.

KEY TAKEAWAYS

01

The national Atlas headline of 45/100 (B) describes the selected 250 estates.

02

Exposure associations need current-account validation, while 74 estates remain in monitoring or missing DMARC and only 7 publish DNSSEC delegation.

03

Give current-account, configuration and recovery questions separate owners and completion evidence.

CHAPTER 04

What the retained dark-web evidence establishes

04

THIS CHAPTER ANSWERS

Which Ireland-associated offers deserve investigation, and which apparent events are older material or geographic ambiguity?

6

detailed claim dossiers, separate from public disclosures

4.1 Universe card 27
4.2 Monthly visibility and its limits 28
4.3 Platforms, languages and themes 30
4.4 Dataset claims and older record dates 33
4.5 A website is not an entire operational service 35
4.6 Recent phishing advertising and a separate access claim 37
4.7 Older lists, demand and secondary reporting 39
4.8 What the chapter adds to a response programme 41

CHAPTER 04

What the retained dark-web evidence establishes

IN SHORT

The retained posts include service-provider data allegations, website material, communications claims, access advertising and recent bank-themed phishing offers. Some previews contain older record dates, and several apparent leaks are replies to older threads. An Ireland label can also describe a cloud region or a multinational service. Validate the specific proposition behind an offer before assigning an incident date, affected organisation or customer response.

4.1 Universe card

Item	Scope
Window	Posts dated 1 January through 22 November 2026
Recent activity	Posts dated 8–22 November
Retained narrative corpus	49,723 distinct posts within the stated collection scope
Retained forum posts	767 distinct forum posts
Recent retained posts	About 1,190 within the recent window
Ireland-tagged volume	35,915 reported posts across the year-to-cutoff window
Timestamp	Publication time, not collection, intrusion or data-acquisition time
Unit	Post, including advertisements, comments, quoted replies, news and relays
Limits	Not unique offers, verified datasets, successful attacks or independently identified people

[S1]

The country-tagged population and retained narrative corpus have different coverage. They are not added together or presented as a complete incident census. Platform labels describe where the post appeared; they do not authenticate its contents.

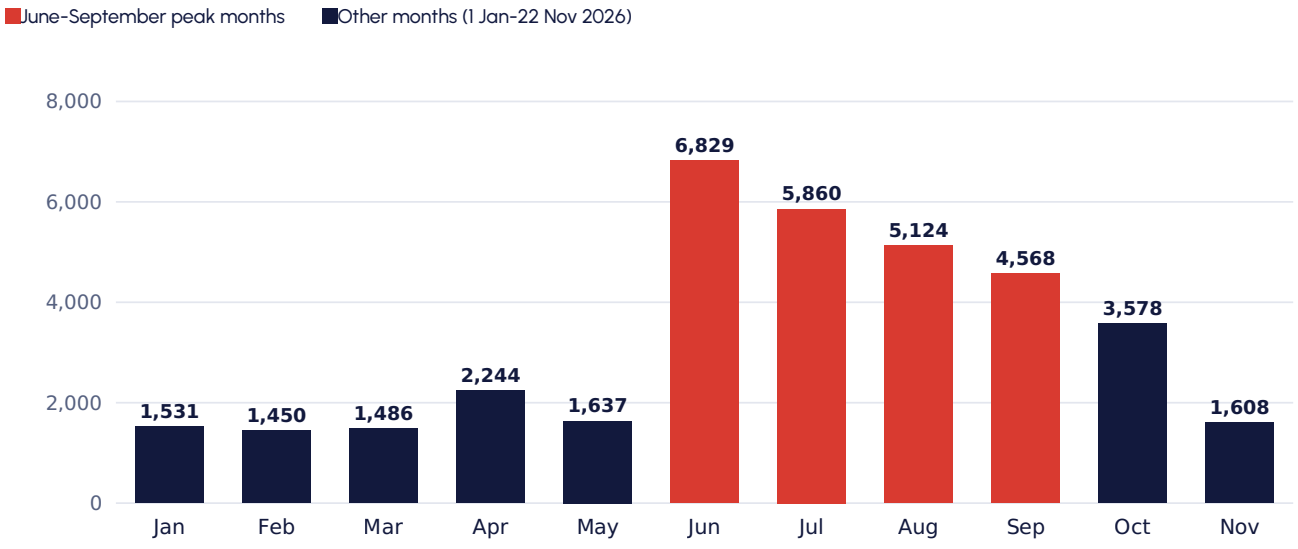
A reply is especially easy to misread. Its date can be recent while its quoted offer is old. A title can contain an asserted quantity even when the retained body contains only a comment. The report preserves those distinctions in the card and case assessments.

4.2 Monthly visibility and its limits

The monthly series describes the source's post population. November ends at the cut-off and is not a full month. Movement in this series does not establish movement in successful attacks [S1].

Month	Ireland-tagged posts
2026-01	1,531
2026-02	1,450
2026-03	1,486
2026-04	2,244
2026-05	1,637
2026-06	6,829
2026-07	5,860
2026-08	5,124
2026-09	4,568
2026-10	3,578
2026-11	1,608

Ireland-tagged monthly posts peak in June–September rather than during the winter bulk wave



Source: Brandefense Blackhole, Ireland-tagged posts, 1 January–22 November 2026; November partial [S1]. Separate from the 49,723-post retained narrative corpus; posts are not confirmed incidents.

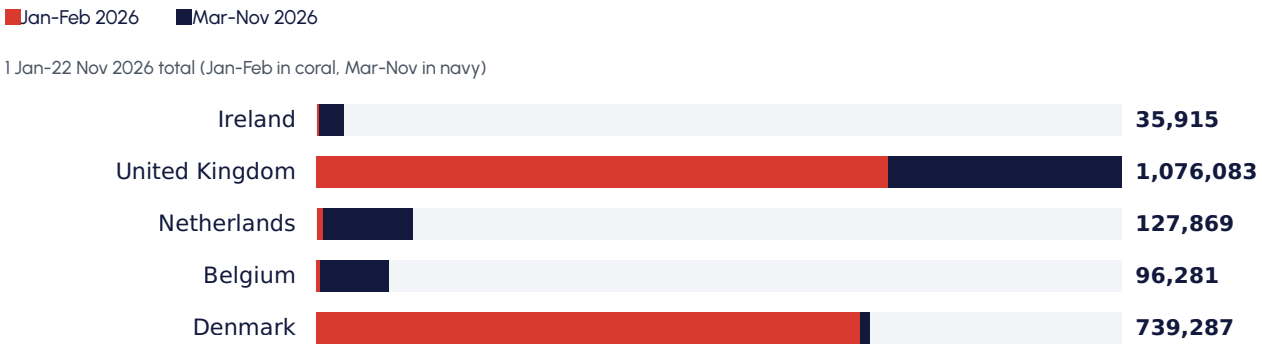
Comparing monthly country tags across the four peer countries shows a distinct seasonal shape. Between 1 January and 22 November 2026, country-tagged volume totalled 35,915 for Ireland, 1,076,083 for the United Kingdom, 127,869 for the Netherlands, 96,281 for Belgium and 739,287 for Denmark [S1].

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

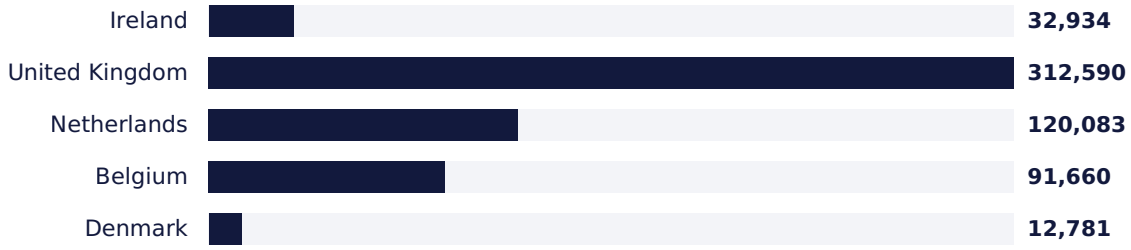
Month	IE	GB	NL	BE	DK
2026-01	1,531	429,222	3,703	2,299	411,285
2026-02	1,450	334,271	4,083	2,322	315,221
2026-03	1,486	29,563	7,006	2,659	1,149
2026-04	2,244	34,411	4,345	3,405	1,640
2026-05	1,637	28,609	4,986	1,610	878
2026-06	6,829	45,166	11,355	2,141	1,251
2026-07	5,860	37,153	17,267	3,356	1,785
2026-08	5,124	34,839	28,279	44,206	1,366
2026-09	4,568	38,487	17,062	18,132	1,289
2026-10	3,578	51,083	19,870	14,312	2,039
2026-11	1,608	13,279	9,913	1,839	1,384
Total	35,915	1,076,083	127,869	96,281	739,287

Ireland did not absorb the January–February bulk wave that accounted for 71.0% of United Kingdom volume (763,493) and 98.3% of Denmark volume (726,506). January and February represented 8.3% of Ireland-tagged posts (2,981). Instead, June through September produced 62.3% of Ireland's tagged volume (22,381), peaking at 6,829 in June [S1].

Ireland avoided the January–February bulk wave observed in United Kingdom and Denmark tags



March-November 2026 only (separate scale)



Country-tagged raw posts across monitored channels; not adjusted for population or source coverage. Source: Brandefense Blackhole, Ireland-tagged posts, 1 January-22 November 2026; November partial [S1]. Separate from the 49,723-post retained narrative corpus; posts are not confirmed incidents.

A high month needs an explanation of its content, rather than an assumption of greater damage. Marketplace promotions, repeated discussions, news and cloud-region references can contribute to visibility. None independently supplies an Irish victim count.

The corpus includes access advertising that identifies an Ireland cloud region. A region label concerns infrastructure location. It does not establish that the account owner is Irish or that an Irish organisation's systems were accessed. Such material is retained as geographically ambiguous advertising, outside confirmed Irish incident conclusions [S1].

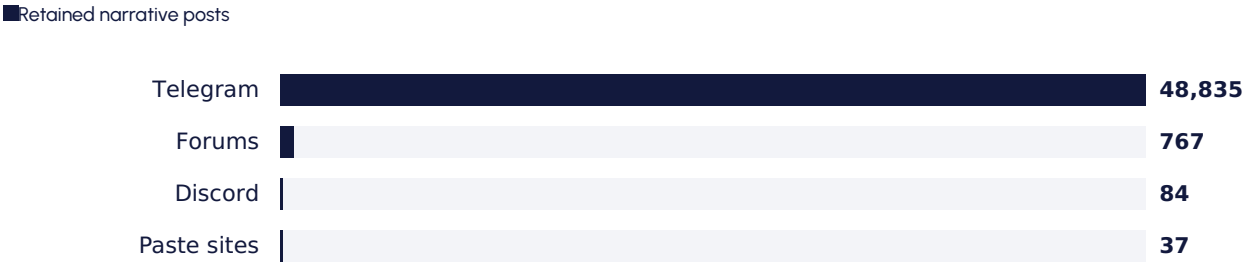
4.3 Platforms, languages and themes

The following counts describe the retained corpus used for narrative review. They are separate from the wider country-tagged series.

Platform	Retained posts
Telegram	48,835
Forum	767
Discord	84
Paste	37

In the separate 35,915-post Ireland-tagged series, Telegram accounts for 35,556 posts (99.0%), forums for 314 (0.9%), Discord for 36 (0.1%) and paste sites for 9 (under 0.1%) [S1].

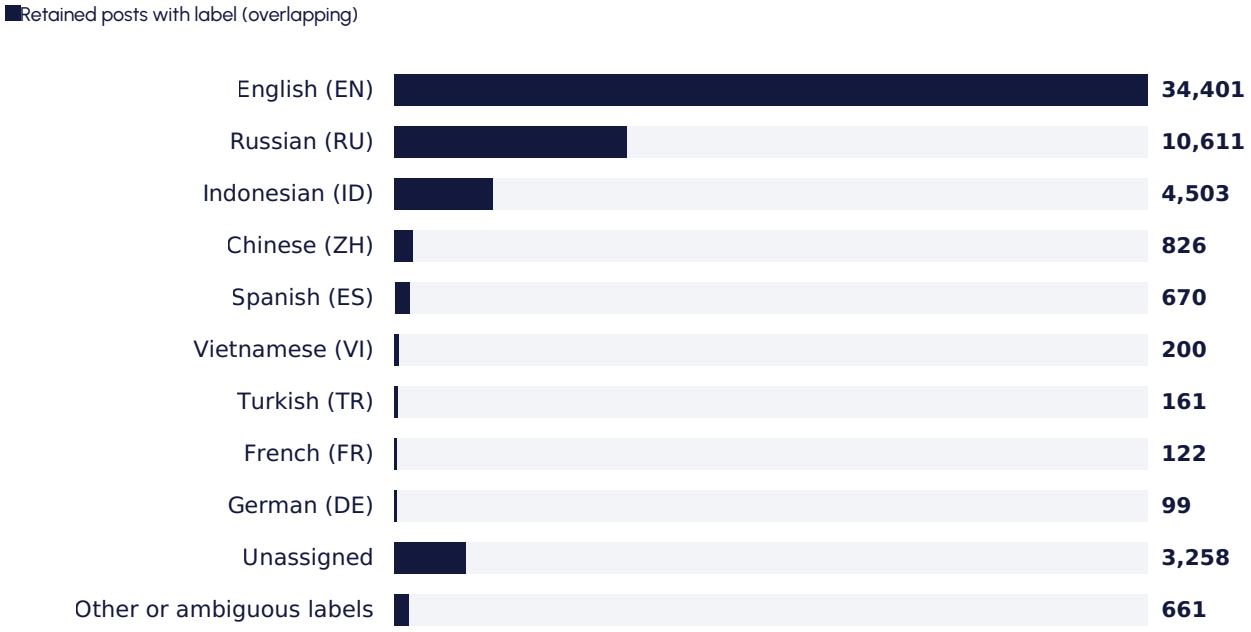
Telegram accounts for 98.2% of the retained narrative corpus while forums carry the detailed claim dossiers



Source: Brandefense Blackhole, 49,723 distinct retained narrative posts, 1 January–22 November 2026 [S1]. Separate from the 35,915-post Ireland-tagged series; posts are not confirmed incidents.

Language label	Retained posts
EN	34,401
RU	10,611
ID	4,503
ZH	826
ES	670
VI	200
TR	161
FR	122
DE	99
Unassigned	3,258
Other or ambiguous labels	661

Overlapping language labels describe message text rather than actor nationality



Language labels overlap; row counts are not additive and do not identify actor nationality. Source: Brandefense Blackhole, 49,723 distinct retained narrative posts, 1 January–22 November 2026 [S1]. Separate from the 35,915-post Ireland-tagged series; posts are not confirmed incidents.

Language labels are unverified, can overlap and include ambiguous values. They should not be added as if they identified disjoint people. A Russian-language post can describe Irish services or another market. An English-language advertisement can include many countries. Neither language nor an Ireland tag establishes the author's location or targeting intent.

The material supports descriptions of advertised data, credentials, identity documents, account services, phishing capability and access. It does not support a national market-share claim for those activities. The detailed cases below identify exactly what the held content establishes.

4.4 Dataset claims and older record dates

Evidence card B01 — Jan 2026

Forum poster (alias withheld) | Forum | Forum | English

ORIGINAL

[Paraphrase: the author alleges a 2026 database incident at an Irish services provider.]

TRANSLATION

[Paraphrase, not a verbatim quotation.]

Note. 2021 record dates; 2026 post/claim; record dates are not attack dates.

Held
A forum author alleges a database breach at an Irish services provider. The displayed record dates fall in July 2021 despite the 2026 assertion.

Not established
Allegation only; sample authenticity, acquisition date and actual affected population unestablished.

Evidence card B02 — Feb 2026

Forum poster (alias withheld) | Forum | Forum | English

ORIGINAL

Available for acquisition

TRANSLATION

Source English; authentic excerpt.

Note. Repeated January 2026 record values do not independently establish freshness.

Held
A seller offers what it describes as Irish membership-related records, with contact and account-activity fields.

Not established
Seller claim only; provenance, validity, unique people, completeness and freshness unestablished. Generic-looking sample schema warrants caution.

CASE K

K

A services-provider database allegation

Evidence card B01 | Jan 2026 | Forum | Professional services

Claim unverified

CLAIM	A January forum post alleges a 2026 incident at an Irish services provider. Later posts repeat the allegation and add an asserted dataset quantity [S1].
HELD EVIDENCE	The retained material includes customer-table-style fields, mirrored threads and replies. Some displayed record dates fall in July 2021. Those record dates differ from the post's claimed event year.
NOT ESTABLISHED	The record preview is not independently authenticated. Neither the original acquisition date nor a current affected-person population is established. Repeated posts do not create independent corroboration.
ALTERNATIVES	Plausible explanations include older information, a later copy, repeated advertising or an inaccurate allegation. The older record dates do not, by themselves, prove fabrication.

RESPONSE	A relevant organisation should compare an authorised alert with its own data and previous notifications. Record whether the claim matches current information, historical material or no owned system.

Bottom line

Validate source and record age before assigning affected information or an event date.

The case matters because a strong perpetrator-style assertion can coexist with much older record dates. The correct response is to validate both the claimed source and the relevant chronology. Neither accepting the asserted year nor dismissing the whole offer solely because of old entries is justified.

CASE L

L A membership-services dataset offer

Evidence card B02 | Feb 2026 | Forum | Membership services

Claim unverified

CLAIM	A February seller offers Ireland-related membership information and describes contact and account-activity fields [S1].
HELD EVIDENCE	An offer and a structured-looking preview are present. The sample uses repetitive or generic-looking elements, which warrant caution but do not establish that every record is synthetic.
NOT ESTABLISHED	Provenance, valid membership data, freshness, unique people and completed sale remain unverified. An asserted row count cannot be interpreted as an independently measured population.
ALTERNATIVES	The material could be a sample assembled for advertising, older data, inaccurately described records or genuine information with an unverified origin. The report cannot decide between those explanations from the offer alone.
RESPONSE	Validate actual data ownership through an authorised process. Assess contact and recovery risks only for the information that can be corroborated.

Bottom line

Validate provenance and actual data before acting on an advertised quantity.

4.5 A website is not an entire operational service

Evidence card B03 — Apr 2026

Forum poster (alias withheld) | Forum | Forum | English

ORIGINAL

Wordpress Database

TRANSLATION

Source English; authentic title fragment.

Note. Preview contains 2019–2020 user-record dates; post date is not compromise date.

Held
A forum post claims a public-facing website database and displays a WordPress users-table-style SQL preview.

Not established
Website-data allegation only; no proof of valid credentials, operational compromise, customer database breadth or disruption.

Evidence card B04 — Apr 2026

Forum poster (alias withheld) | Forum | Forum | English

ORIGINAL

[Paraphrase: the author alleges theft of internal correspondence at an Irish commercial service organisation.]

TRANSLATION

[Paraphrase, not a verbatim quotation.]

Note. No acquisition date established from retained preview.

Held
A forum author alleges theft of internal correspondence and customer-service records at an Irish commercial service organisation.

Not established
Actor allegation only; authenticity, acquisition date, scope, impact and official confirmation unestablished.

CASE M

M

A public-facing website database claim

Evidence card B03 | Apr 2026 | Forum | Public-facing website

Claim unverified

CLAIM	An April post presents a website database attributed to an Irish public-facing service. The retained preview resembles a WordPress user table [S1].
HELD EVIDENCE	The post displays schema and record-style material. Its user-record dates include 2019–2020. Those values do not establish the data-acquisition date or the start of any intrusion.
NOT ESTABLISHED	The report establishes neither valid credentials nor the authenticity or complete scope of the database. Core service operations, operational equipment and service interruption are not demonstrated.
ALTERNATIVES	A historical website copy, a limited web administration record or inaccurate attribution remain possible. A website allegation should not become a claim of operational access.

RESPONSE	The relevant owner should review the specific web application, account history and prior remediation. Keep the investigation bounded until additional evidence supports wider scope.

Bottom line

Keep the investigation bounded to the relevant web service until wider evidence exists.

N

CASE N

A commercial-service communications allegation

Evidence card B04 | Apr 2026 | Forum | Commercial services

Claim unverified

CLAIM	An April post alleges theft of internal correspondence and customer-service records from an Irish commercial service organisation [S1].
HELD EVIDENCE	The retained post contains the allegation and record-style examples. It is more specific than a general country tag, but the examples have not been independently authenticated.
NOT ESTABLISHED	There is no verified acquisition date, complete customer population, access route, service disruption or completed sale. The post date is not an intrusion date.
ALTERNATIVES	A supplier copy, older information, an inaccurate label or a deliberately misleading offer could explain parts of the material. The report does not select one without evidence.
RESPONSE	Validate relevant communications and customer-data scope against owned records. Assess possible follow-up impersonation without assuming the claimant's full narrative is accurate.

Bottom line

Validate communication and customer-information scope against owned records.

Public labels deliberately remain broad. Detailed route, programme, locality or record-count combinations can identify an organisation even when its name is removed. Those details are unnecessary for the response decisions in these cases.

4.6 Recent phishing advertising and a separate access claim

Evidence card B05 — Nov 2026

Forum poster (alias withheld) | Forum | Forum | English

ORIGINAL

[kit name] is a live panel

TRANSLATION

Source English; authentic excerpt.

Note. Observed in the 8–22 November window; repeated two days later in B06.

Held
A seller advertises a live phishing panel listing an Irish retail bank among several European themes.

Not established
Capability advertisement, not a confirmed deployed campaign, victimisation or bank-system breach.

Evidence card B06 — Nov 2026

Forum poster (alias withheld) | Forum | Forum | English

ORIGINAL

[kit name] is a live panel

TRANSLATION

Source English; authentic excerpt.

Note. Observed in the 8–22 November window; repeat of B05.

Held
The same forum account repeats the Irish-bank-themed panel advertisement two days later.

Not established
Same advertised capability as B05; no independent incident established. No deployment or successful compromise established.

CASE O

An Irish-bank-themed phishing panel

Evidence card B05 | Nov 2026 | Forum | Financial impersonation

Offer unverified

CLAIM	The same forum account advertises a panel twice, two days apart, during the 8–22 November window (B05 and B06), listing an Irish bank among several European themes. The copies share the same capability description [S1].
HELD EVIDENCE	The two advertisements establish repeated advertising of one capability. Their relationship concerns the visible copy and posting account, rather than a verified common deployment.
NOT ESTABLISHED	No working panel, deployed Irish campaign, customer population, stolen account or bank-system incident is established. An advertised feature is not an observed use.
ALTERNATIVES	A functional tool, a copied sales pitch or a non-working offer remain possible. Two advertisements do not become two bank incidents.

RESPONSE

Use a relevant alert to review customer impersonation and account-recovery protections. Escalate when owned-service evidence corroborates a campaign or unauthorised activity.

Bottom line

Look for corroborating campaign and account activity; do not infer a bank-system incident.

Evidence card B07 Jan 2026

Chat reposter (alias withheld) Chat repost Discord English

ORIGINAL

store admin access to an Ireland-based PHP + Laravel online shop (no shell access)

TRANSLATION

Source English; authentic excerpt.

Note. Date shown is the repost publication month; acquisition date remains unestablished. Alleged seller alias is withheld.

Held

An intelligence reposter attributes an Irish online-shop admin-access auction to a separate alleged seller.

Not established

Secondary repost; original seller evidence, target identity, working access, completed sale and acquisition date unestablished. No shell access is expressly stated.

P

CASE P

Online-retail administration offered through a repost

Evidence card B07 Jan 2026 Chat repost Online retail

Secondary claim

CLAIM	A January intelligence repost attributes an Ireland-based shop administration auction to an alleged seller. The description expressly excludes shell access [S1].
HELD EVIDENCE	The preserved item is a secondary repost. It reports an access claim; it is not a retained original demonstration of valid access.
NOT ESTABLISHED	The target's identity and Irish ownership, usable access, actual orders, acquisition date and completed sale remain unverified. The claimed administration boundary must not expand into server-level access.
ALTERNATIVES	An inaccurate country label, older access, a copied claim or fabricated advertising could explain the item. None is established as the definitive explanation.

RESPONSE	A relevant retailer should validate current administrator assignments and recent authorised-service activity. Preserve the difference between a role in a shop application and a role on its server.

Bottom line

Validate current shop administrators; do not expand the claim into server access.

4.7 Older lists, demand and secondary reporting

The retained February reply under an Ireland-labelled list quotes a December 2025 post. Other country-labelled credential titles also carry earlier dates. They establish circulation in 2026, without establishing a new 2026 theft or a unique-account total [S1].

Evidence card B08 — Feb 2026

Forum commenter (alias withheld) | Forum | Forum | English

ORIGINAL

Thanks bro

TRANSLATION

Source English; authentic retained reply excerpt.

Note. Quoted original: December 2025. Retained reply: February 2026.

Held

A 2026 comment appears under an Ireland-labelled data-list title and quotes a December 2025 post.

Not established

Retained content is a reply; does not establish a new 2026 leak, new supply, authenticity or unique accounts.

Evidence card B09 — Apr 2026

Forum poster (alias withheld) | Forum | Forum | English

ORIGINAL

buying firsthand uk/irish b2b data

TRANSLATION

Source English; authentic excerpt.

Note. 2026 post-date observation only.

Held

A buyer requests UK/Irish business-to-business data.

Not established

Evidence of expressed demand only; no proof of supply, theft, victim compromise or completed transaction.

The buyer request in B09 expresses demand for UK and Irish business data. It does not establish supply. B10 is a reply within an identity-document thread, rather than an authenticated original offer. B11 advertises contact leads without establishing provenance or a record population.

Evidence card B10 — Feb 2026

Forum commenter (alias withheld) | Forum | Forum | English

ORIGINAL

Ireland - Passport + Selfie

TRANSLATION

Source English; authentic title fragment.

Note. Retained reply date is not source-document date.

Held
A retained reply sits in an Ireland-labelled passport-and-selfie thread.

Not established
Reply only, quoting another user; no authenticated document set, original offer date, sale or new compromise established.

Evidence card B11 — Sep 2026

Forum poster (alias withheld) | Forum | Forum | English

ORIGINAL

Ireland Citizen Phone Number Leads

TRANSLATION

Source English; authentic title fragment.

Note. 2026 advertising observation; source-record date unestablished.

Held
An advertisement offers Ireland-labelled phone/email leads, with contact solicitation in the retained body.

Not established
No demonstrated source, population size, breach mechanism, data validity or completed sale.

B12 illustrates a geographic question in secondary ransomware reporting. A feed labels an alleged organisation UK and Ireland. That label alone cannot establish which Irish legal entity, data or operation was affected. It is kept separate from the Ireland-labelled listing population in Chapter 7.

Evidence card B12 — Feb 2026

Monitoring relay (alias withheld) | Monitoring relay | Telegram | English

ORIGINAL

#Ransomware #UnitedKingdom #Ireland

TRANSLATION

Source English; authentic excerpt.

Note. No attack date is established by this secondary relay.

Held
A secondary monitoring relay attributes a ransomware listing to an extortion label and tags the organisation across the United Kingdom and Ireland.

Not established
Feed claim only. Irish legal victim, affected Republic of Ireland operations, actual compromise, scope and impact remain unresolved.

A global-company listing described as Ireland-related has the same limitation. A business presence, a country suffix or an Irish customer example does not authenticate an Irish organisational incident.

4.8 What the chapter adds to a response programme

Evidence	First useful question	Unsupported shortcut to avoid
Database preview	Does it match owned information and its known history?	Every displayed row is a new affected person
Website table	Which application and accounts are actually involved?	A web claim means operational control
Communications offer	Is the source, age and custody established?	The post date is the theft date
Phishing advertisement	Is there corroborating campaign or account evidence?	An advertised feature was used successfully
Secondary access report	Is an original source and relevant owned service available?	A repost demonstrates working access
Country-labelled list or region	What does the geographic label describe?	Ireland was the target

Phishing-panel advertiser

Forum poster (alias withheld)

Advertising persona | No state or organisational attribution

IN IRELAND, 2026

Late November

Repeated bank-themed capability advertising in the 8–22 November window

CLAIMED TARGETS

An Irish financial-service theme among several countries; institution withheld

IN THEIR WORDS

"[kit name] is a live panel" B05

SEEN IN PUBLIC REPORTING

[S1] Two retained advertisements, B05 and B06

OUR ASSESSMENT

Shared text and posting account connect the two advertisements. They do not establish a working tool, live deployment, account theft or seller identity.

CONFIDENCE

High for advertising observation; capability and use unverified

KEY TAKEAWAYS

01

The held evidence establishes advertising and circulation, with proposition-specific limits.

02

Old record dates, quoted replies and region labels require separate interpretation.

03

Validate owned data, application scope and current account activity before escalating an allegation.

CHAPTER 05

Incident disclosures and sector decisions

05

THIS CHAPTER ANSWERS

What did original disclosures establish, and which decisions follow for Irish services?

10

detailed disclosure dossiers, with separate occurrence and publication dates

5.1 A financial supplier incident becomes visible in November 44
5.2 A financial portal shutdown and restoration 45
5.3 Refrigeration crosses the digital and physical boundary 46
5.4 Global manufacturing incidents with Irish operational relevance 47
5.5 Education depends on provider-held information 49
5.6 Administrative fulfilment at a supplier 50
5.7 A public-service access record needs careful handling 51
5.8 Further supplier and publishing disclosures 52
5.9 Other disclosures, historical events and exclusions 53
5.10 Recent activity: 8–22 November 54

CHAPTER 05

Incident disclosures and sector decisions

IN SHORT

The disclosures concern customer information, shared education systems, health administration, production and connected equipment. Some were published weeks after the underlying activity; others describe global incidents with an evidenced Irish consequence. Historical enforcement decisions belong in a separate category. Establish the affected service and data, preserve the chronology and assign the owner who can make a safe restoration decision.

5.1 A financial supplier incident becomes visible in November

A

CASE A

Saved-payee information at a financial-service supplier

Financial supplier

Official notice

DISCLOSURE	A community lender's mid-November notice says an external provider notified it days earlier that saved-payee information had been retrieved. The notice dates the underlying activity to October and says the weakness was closed days later [S26].
ESTABLISHED SCOPE	The lender identifies beneficiary information rather than member balances or login credentials. It says it could not determine the information involved for each individual. The notice supports this lender's account; it does not establish identical impact at every customer.
CHRONOLOGY	November reporting describes recognition and notifications after earlier October activity. RTÉ reported dozens of lender notifications to the DPC. Notifications, provider customers and affected people are different units [S27].
NOT ESTABLISHED	The available material does not supply a final affected-person total, proof that every advertised figure is accurate or a confirmed loss at every institution. Closure of a weakness does not reverse earlier data retrieval.
ALTERNATIVES AND LIMITS	The provider's cross-border location and its customers' jurisdictions must remain separate. Several customer notices can describe one supplier incident. They are not separate evidence of independent intrusions into every lender's core systems [S28].

RESPONSE	Establish the affected tenant and information fields with the provider. Protect customer communications against convincing payment-related impersonation, and assess notification duties from the institution's own facts.

Bottom line

Validate institution-specific saved-payee information and customer-protection decisions.

The practical risk extends beyond a stolen login. Accurate beneficiary details can make a fraudulent call sound plausible. Customer-support staff should have a route to handle concerns without asking the caller to repeat sensitive details to an unverified contact.

A provider's technical notice and a controller's customer notice answer different questions. The first should describe what happened in the provider's service. The second should explain what is known for that institution's customers. Neither should fill a remaining gap with another organisation's headline estimate.

For incident managers, the key record is a chronology of awareness, supplier messages, validation and decisions. Preserve the first notice even if later information changes the assessment. A well-maintained record allows an early factual report followed by a supported update.

5.2 A financial portal shutdown and restoration

B

CASE B

A financial-services customer portal

Financial services

Press report

DISCLOSURE	Mid-November national reporting quotes a financial-services firm's client update acknowledging a recently identified incident and a precautionary portal shutdown. The company said it had found no evidence of an effect on client funds or accounts [S29].
FOLLOW-UP	Follow-up reporting several days later says the portal returned and quotes a spokesman confirming notification to the DPC and Central Bank. Press reporting added a limited data-exposure figure that the company's quoted response did not confirm [S30].
ESTABLISHED SCOPE	An incident and interruption are company-confirmed through the quoted account. Restoration and regulator notification have their own dates. They do not independently establish the complete data-access history.
NOT ESTABLISHED	The inspected statements do not support a published claim of stolen assets, a verified initial access route or a complete affected-client population.

ALTERNATIVES AND LIMITS	A precautionary shutdown can affect more users than the underlying data question. Treat service availability, client assets and information confidentiality as separate propositions.
RESPONSE	Test portal suspension and customer access to essential records. Require a restoration decision that covers identity, permissions and residual information risk, with a usable alternative contact route.

Bottom line

Restore a controlled customer route while keeping data-scope questions assigned.

Avoid treating a portal's return as a declaration that every investigation question is closed. Operations may restore a service under changed controls while privacy specialists continue assessing records. Communications should explain the status of each question in plain language.

5.3 Refrigeration crosses the digital and physical boundary

CASE C

C

Grocery refrigeration disruption

Grocery operations

Company confirmed

DISCLOSURE	RTÉ's 2 November report quotes Musgrave's confirmation that the incident affected a specific refrigeration model in thirteen SuperValu stores in Ireland. Chilled and frozen products were removed as a precaution before stores returned to normal operation [S31].
ESTABLISHED SCOPE	The company's account establishes a bounded Irish operational impact. It does not establish that every store, other business system or customer database was affected.
TECHNICAL CONTEXT	NCSC's 3 November advisory addresses remotely accessible controllers. Its 13 November update discusses continuing European incidents and separate new research. The research does not establish the precise access route used at the Irish stores [S13][S14].
NOT ESTABLISHED	Online posts described by RTÉ claimed an attack on an equipment vendor, not the Irish stores, and involvement in the supermarket incidents remains unestablished. No actor or state attribution is independently established by the material used for this case [S32].

ALTERNATIVES AND LIMITS	A temperature excursion requires operational investigation even when its cause is unclear. The confirmed Irish case must not inherit loss totals or attribution from events in other countries.
RESPONSE	Remove unnecessary public management access, review settings and alarms with authorised operators, and verify safe temperatures before resuming normal stock handling.

Bottom line

Verify safe equipment settings and protected management access before resuming normal operation.

The business owner needs evidence of safe operation, rather than a screenshot showing that a controller is online. An alarm path, a maintenance account and a remote-management connection can fail independently. Record who verified each of them.

A managed equipment provider should also have an emergency contact and an approved access-restriction process. Waiting for normal procurement escalation can leave the operating team without the authority needed to isolate a dangerous connection.

5.4 Global manufacturing incidents with Irish operational relevance

D

CASE D

Stryker's global network disruption

Medical manufacturing

Company notice

DISCLOSURE	Stryker dates its global disruption to 11 March. Its updates describe effects on ordering, manufacturing and shipping. Irish reporting establishes an operational connection to Cork [S20][S21].
CHANGED ASSESSMENT	The company's 23 March update says investigators identified a malicious command file after an earlier assessment found no indication of malware. It describes that file as unable to spread. The later account supersedes the earlier wording [S20].
RESTORATION	On 1 April, the company reported that its global manufacturing network was fully operational. That is a company statement about recovery, rather than an independent audit of every production dependency.
NOT ESTABLISHED	This report does not derive an Irish victim-device count, data-loss figure or state attribution from the global incident. It preserves the company's distinction between internal disruption and its product-safety assessment.

ALTERNATIVES AND LIMITS	Local consequences can arise from global identity and service dependencies. An Irish operational interruption does not establish that the initial access occurred in Ireland.
RESPONSE	Test manufacturing dependencies on central identity, device administration and order systems. Protect recovery administration separately, and require the production owner to accept restored work.

Bottom line

Test central identity dependencies and complete production recovery with business acceptance.

This case illustrates why initial statements need version control. A cautious early assessment can be reasonable and still change as investigation progresses. The useful assurance record identifies which statement is current and what evidence supports it.

For a manufacturing service, restarting authentication is only one part of recovery. Orders, production instructions, scheduling and shipment records also need reconciliation. A service test should include a complete business transaction and a documented integrity check.

CASE E

E

Boston Scientific's August incident and Irish workforce effects

Company notice

Medical manufacturing

DISCLOSURE	Boston Scientific identified its incident on 25 August. Its 22 September update publishes a summary of the external investigation, describing entry through a network device and access to a limited on-premises environment [S22].
IRISH NEXUS	Local reporting describes interrupted production shifts at Clonmel. That establishes a reported Irish operational consequence of the global incident. It does not supply an Irish data-loss total [S23].
ESTABLISHED SCOPE	The company reports no evidence of continuing actor activity after its containment measures. Its no-evidence findings for specified cloud and business systems retain the investigation's system boundaries [S22].
NOT ESTABLISHED	An absence finding for the listed systems is not a universal statement that no information was accessed anywhere. This report makes no additional actor attribution.
ALTERNATIVES AND LIMITS	Precautionary isolation and restoration dependencies can interrupt work beyond the directly accessed environment. Workforce effects and technical intrusion scope require separate evidence.

RESPONSE	Validate externally accessible devices, containment boundaries and reconnection criteria. Include operational managers in the recovery exercise, and keep staff communications consistent with the verified service state.

Bottom line

Preserve the investigated system boundaries and validate reconnection with operational owners.

A technical team may reasonably isolate a broad environment while investigating a narrower intrusion. Leaders should ask whether the chosen boundary is still necessary, what evidence permits a change and which business process has a safe fallback. These questions support recovery without minimising the incident.

5.5 Education depends on provider-held information

CASE F

F

Munster Technological University and the Canvas supplier incident

Education supplier

Official statement

DISCLOSURE	MTU's 8 May statement says Instructure confirmed that the university was among institutions affected by the supplier incident. The university said it was investigating the nature and extent of potential impact [S24].
ESTABLISHED SCOPE	National reporting describes interruptions to learning tools at several Irish institutions. The MTU statement establishes MTU relevance. It does not establish an identical data population at each institution mentioned in press reporting [S25].
NOT ESTABLISHED	Global data quantities and an actor's claimed responsibility are not used as an Irish affected-person total. The available university statement does not establish a separate intrusion into MTU's core estate.
ALTERNATIVES AND LIMITS	A supplier platform can affect teaching and communications while local systems remain operational. This May 2026 case is separate from historical university ransomware events.
RESPONSE	Identify provider-held learning data and integrations. Review staff and student communications, preserve suspicious-message reporting and agree evidence for restoring affected connections.

Bottom line

Establish institution-specific provider data and safe integration recovery.

An education response needs to cover people who may not use an institution's usual employee support channels. Students, temporary teachers and former users can have different contact details and data histories. The communication plan should identify the applicable population rather than copy a global provider's total.

A restored teaching interface also needs a trust decision about its integrations. Confirm which applications can read records, send messages or create accounts. Record changes in those permissions during response, with an owner for returning them to normal.

5.6 Administrative fulfilment at a supplier

CASE G

A service provider's administrative supplier

Service administration

Press report

DISCLOSURE	July reporting quotes a service provider confirming that an administrative supplier suffered an attack and that a small amount of records was accessed [S33].
ESTABLISHED SCOPE	The quoted account describes an administrative fulfilment interruption with alternative service arrangements. It says the organisation's own systems were not affected [S33][S34].
DATE BOUNDARY	The publication date is established. This report does not assign a precise intrusion date from an unverified derivative chronology.
NOT ESTABLISHED	A supplier record exposure does not establish a new incident in the customer's core network. No final individual count is inferred from the phrase describing a small amount.
ALTERNATIVES AND LIMITS	An administrative interruption and loss of the underlying service are different conditions. Public communications should distinguish them clearly.
RESPONSE	Inventory information sent to fulfilment providers, minimise unnecessary retention and test an accessible alternative when normal fulfilment stops.

Bottom line

Verify alternative service arrangements and supplier-held information.

The service owner should confirm that a fallback works for the person at the receiving desk as well as for the responsible organisation. A customer should not have to rely on the very channel that is unavailable. Exercise the complete process with the teams expected to use it.

5.7 A public-service access record needs careful handling

CASE H

H

An Irish public-service information platform

Public services

Official notice

DISCLOSURE	An autumn official notice from a public-sector online service describes exposed email addresses and passwords, disabled logins and contact with affected users. A subsequent update says the affected credential storage was removed [S35].
ESTABLISHED SCOPE	The issuer confirms a bounded service incident. Its update distinguishes primary sign-in changes from secondary credential retention across account workflows. That distinction matters when checking whether remediation addressed every relevant path.
NOT ESTABLISHED	The notice does not establish that every associated public database was accessed or that every exposed password remained usable. A precise intrusion-start date is not supplied here.
ALTERNATIVES AND LIMITS	The organisation remains anonymous because broad reporting sufficient for this report's naming test was not established. Its own domain and identifying article address are omitted from the public references.
RESPONSE	Inventory every location that can retain authentication material, including registration and recovery processes. Confirm that removal applies across those paths, and warn affected users about relevant password reuse.

Bottom line

Review authentication-material retention across registration and recovery paths.

Changing the main sign-in screen does not necessarily remove older data stores or secondary processing. An assurance request should ask the service owner to demonstrate the final data flow and disposal outcome. Use an authorised review of the organisation's own environment.

5.8 Further supplier and publishing disclosures

CASE I

A hospitality booking provider

Hospitality supplier

Press report

DISCLOSURE	Mid-November regional reporting quotes a hospitality property's confirmation of unauthorised access through its booking provider, with the incident and property statement occurring days apart in November [S53].
ESTABLISHED SCOPE	The account describes reservation details, including guest names, email addresses, references and stay dates. The property said payment information and passwords were not involved, and that it had warned affected guests.
NOT ESTABLISHED	The account says a file was believed to have been exported. It does not supply a validated affected-person total or establish that fraudulent use occurred. The provider's exact initial access route remains unestablished here.
ALTERNATIVES AND LIMITS	A guest can receive a convincing payment request based on genuine booking details without a payment-card record being involved. That is a protection scenario, not an assertion that the disclosed information was used.
RESPONSE	Confirm the affected reservation population, secure provider administration and establish a known route for guests to verify payment requests. Customer communications should preserve the property statement's data exclusions.

Bottom line

Protect guests against plausible follow-up messages using known verification routes.

This case falls within the recent-publication window and the recent-event window. Those dates happen to align; the other November disclosures show why the report cannot assume that they always do. A booking record also needs its own sensitivity assessment, independent of whether payment data is present.

CASE J

J

An externally managed healthcare publishing service

Healthcare publishing

Press report

DISCLOSURE	Spring reporting quotes a healthcare organisation's statement describing unexpected activity detected earlier in the year on a web-content server managed by an external vendor. Information sites were taken offline [S54].
ESTABLISHED SCOPE	The statement places that server outside the main network and describes work to republish information. The report documents a public-information service consequence, rather than a demonstrated clinical-network intrusion.
DATE BOUNDARY	The detection occurred earlier in the year than the spring disclosure. Neither date is evidence of a new spring attack or a precisely known intrusion start.
NOT ESTABLISHED	The source does not establish the cause of every unavailable page, a personal-data total or an access route into the main service network.
RESPONSE	Separate public information publishing from clinical and administrative systems in the dependency map. Keep protected copies of essential content and test a trusted publishing alternative.

Bottom line

Restore trusted essential information without inferring clinical-network access.

Public information has continuity value even where it contains no confidential records. A service user needs to find the correct operating information during an interruption. Recovery should verify current content and trusted links, rather than restore obsolete material indiscriminately.

5.9 Other disclosures, historical events and exclusions

One further early-2026 precautionary IT shutdown at an Irish public body was acknowledged by the body without a confirmed data or attribution finding [S77].

July reporting on a global services provider quotes the company describing an isolated and remediated matter with no impact on operations or service delivery. The inspected account does not establish an Irish operational or data consequence. It remains outside the Irish incident-family count [S78].

Spring reporting quotes a public authority confirming that employee business contacts were involved in a supplier incident. The quoted account concerns employee business contacts rather than service-user records, and says the authority's own systems were not breached. The report is relevant to staff impersonation and password-reuse advice, without establishing a new core-network incident [S36].

Several 2026 decisions concern earlier events. Their publication dates do not change their occurrence dates.

Development	Established boundary	Decision
Healthcare ransomware enforcement	A 2026 decision concerns an earlier ransomware event [S37]	Test security, processor agreements and notification records; exclude from new 2026 attacks
Physical-record storage enforcement	A 2026 publication concerns older physical-storage failures [S38]	Review retention and physical access; do not call it a new cyberattack
Financial contact-centre decision	A 2026 decision concerns earlier impersonation-related events [S39]	Test recovery decisions and logging; keep enforcement separate from current intrusion counts
Earlier public-service recovery	2026 updates describe an incident first reported in late 2025 [S52]	Preserve the original chronology; do not count each update as a new event
Higher-education mail history	2026 reporting describes older email-forwarding activity [S51]	Preserve occurrence uncertainty and investigate relevant forwarding rules

A March prosecution update describes alleged malware-assisted access at an education provider after an earlier complaint and investigation. Charges are not a conviction or a new 2026 occurrence count [S67].

A further higher-education enforcement publication and a healthcare physical-record decision published in 2026 both concern earlier underlying events. Both remain governance context rather than new 2026 intrusions [S68] [S69].

A port incident-response page reviewed for this report concerned an oil spill, not a cyberattack. A Northern Ireland school-network lead lacked an established Irish impact. Both were excluded. These exclusions prevent broad incident searches from inflating the country narrative.

5.10 Recent activity: 8–22 November

The recent window contains new disclosures, follow-up guidance and campaign reporting. The dates below identify the development in the window, rather than assume the incident began then.

Date	Development	Evidence boundary	Immediate owner
Mid-November	Financial-services portal interruption and restoration	Company statements through national reporting; data scope remains qualified [S29][S30]	Service owner and privacy
11 November	School email-threat reporting	Threat messages and response; no established network intrusion [S58]	Security and physical safety
13 November	Revised refrigeration-controller advice	Separate vulnerability research and continuing European incidents; no new Irish victim total [S14]	Facilities and network

Date	Development	Evidence boundary	Immediate owner
Mid-November	Financial-supplier notices and customer warnings	October activity disclosed in November; saved-payee scope, not assumed account theft [S26][S27]	Supplier, fraud and privacy
November	Financial-identity clone warning	Official warning about impersonation, not intrusion into the legitimate firm [S63]	Fraud and customer protection
19 November	Financial Stability Review	Official assessment of interconnected cyber risk; no new Irish attack total [S72][S76]	Financial resilience and suppliers
20 November	New PHP advisory	New remediation requirement; no Irish exploitation count established [S15]	Application and platform
20 November	OpenSSL advisory	Application-path conditions remain important; no Irish exploitation established [S74] [S75]	Application and platform
Mid-November	Hospitality booking-provider disclosure	November event and statement; guest information scope remains bounded [S53]	Supplier and customer operations
8–22 November	4 Ireland-labelled listing claims	Listing dates and source labels; outcomes unverified [S3]	Threat intelligence and response

A recent publication can materially change a response plan without representing a newly started attack. Use the recent window as a decision update: which supplier notices need validation, which warnings change remediation and which customers need a clear contact route.

KEY TAKEAWAYS

01

Disclosures establish specific service and data boundaries, not uniform national impact.

02

November publication dates often describe earlier activity or a changed assessment.

03

Restore services with business-owner acceptance and keep privacy questions open until evidence resolves them.

CHAPTER 06

Hacktivist claims, disruption and public communications

THIS CHAPTER ANSWERS

What separates an availability incident, a responsibility claim and demonstrated operational impact?

3

questions: service state, cause and attribution

6.1 A timeline of different evidence types 57
6.2 Responsibility claims around the refrigeration incidents 58
6.3 A disputed outage is not a settled cyberattack 60
6.4 Official communications accounts need their own recovery plan 60
6.5 Threat emails require a coordinated safety response 60
6.6 Readiness without accepting a political narrative 61

CHAPTER 06

Hacktivist claims, disruption and public communications

IN SHORT

Irish refrigeration disruption, police social-account access, emailed threats and a disputed service outage require different responses. Their proximity in time does not establish a common operation. A claimant's message can be recorded without accepting its figures or explanation. Establish the service state, preserve the original statement and use a separate decision for attribution before publishing a response.

6.1 A timeline of different evidence types

The timeline distinguishes organisation statements, press reporting and official guidance. It is not a sequence of linked attacker operations.

11 Mar 2026	**Stryker** Global network disruption begins; company updates assessment on 23 March and reports manufacturing restored on 1 April, with reported Cork impact [S20][S21]
8 May 2026	**Munster Technological University** University confirms involvement in the Canvas learning-platform supplier incident and opens a local scope review [S24][S25]
25 Aug 2026	**Boston Scientific** Global incident identified; 22 September update reports bounded on-premises access, alongside reported Clonmel shift disruption [S22][S23]
15 Oct 2026	**An Garda Síochána** Police confirm control of official X accounts restored and limit unauthorised access to the social platform [S57]
2 Nov 2026	**Musgrave through RTÉ** Company confirms refrigeration impact at thirteen SuperValu stores in Ireland; responsibility not established here [S31]
3 Nov 2026	**NCSC Ireland** Advice on public-facing refrigeration management and remote access [S13]
6 Nov 2026	**RTÉ reporting** Equipment-vendor attack claims and emailed threats described with attribution limits [S32]
11 Nov 2026	**National reporting** Garda response to emailed school threats; no network intrusion established [S58]
13 Nov 2026	**NCSC Ireland** Revised refrigeration advice distinguishes separate vulnerability research from incident observations [S14]

20 Nov 2026 **NCSC Ireland**
Advisories published for PHP vulnerabilities and OpenSSL CVE-2026-121481 [S15][S74]

A communications lead should not flatten these rows into a single attack count. A device advisory concerns a class of systems. A company statement concerns its own impact. A threat email concerns an asserted threat. Each can justify action without supplying the proof needed for another category.

6.2 Responsibility claims around the refrigeration incidents

RTÉ described online posts attributed to NoName057(16) and Z-Pentest Alliance claiming an attack on a refrigeration-equipment vendor whose systems were used at some affected stores. RTÉ said their involvement in the supermarket incidents had not been independently established [S32]. This report retains that evidential boundary and does not treat an actor's claim as a forensic conclusion.

The confirmed business effect and the attribution question can be handled independently. An operator can verify safe temperature settings, remove unnecessary access and issue customer advice without waiting for an actor identity. Investigators can preserve evidence while communications avoid repeating an unverified political story.

Point	Claim or report	Organisation or official account	What remains open
Irish operational impact	Wider European refrigeration disruption reported	Grocery parent confirmed thirteen Irish stores affected [S31]	Exact Irish access route and complete technical scope
Responsibility	Posts claimed an attack on an equipment vendor, not the Irish stores [S32]	NCSC guidance supplies protective actions, not a verified Irish actor attribution [S13] [S14]	Whether either claimant was involved in the Irish store incidents
Newly reported flaws	Later research described additional controller weaknesses	NCSC treated that research separately [S14]	Whether those flaws were used in any specific Irish case
Business recovery	Equipment and stock handling required review	Each operator must verify its own safe service state	A universal Irish financial-loss or recovery-duration figure

The panel deliberately avoids an actor-versus-authority ratio. Store counts, device counts, traffic claims and affected people measure different things. A numerical comparison would imply a relationship the evidence does not establish.

NoName057(16)

Claimant label reported by RTÉ

Vendor-attack claimant as reported by RTÉ | No independent state attribution in this report

IN IRELAND, 2026

November

Vendor-attack claim described in RTÉ reporting

CLAIMED TARGETS

Refrigeration-equipment vendor claim; Irish store responsibility unestablished

SEEN IN PUBLIC REPORTING

[S32] RTÉ reports the vendor-attack claim and notes supermarket involvement is not independently established

OUR ASSESSMENT

Treat vendor claims separately from store impact; store involvement and attribution remain unestablished.

CONFIDENCE

Reported claim; Irish store involvement unestablished

Z-Pentest Alliance

Claimant label reported by RTÉ

Vendor-attack claimant as reported by RTÉ | No independent state attribution in this report

IN IRELAND, 2026

November

Vendor-attack claim described in RTÉ reporting

CLAIMED TARGETS

Refrigeration-equipment vendor claim; Irish store responsibility unestablished

SEEN IN PUBLIC REPORTING

[S32] RTÉ reports the vendor-attack claim and notes supermarket involvement is not independently established

OUR ASSESSMENT

Treat vendor claims separately from store impact; store involvement and attribution remain unestablished.

CONFIDENCE

Reported claim; Irish store involvement unestablished

6.3 A disputed outage is not a settled cyberattack

One 2026 press report linked a service outage to a supplier's ransomware incident, while the affected organisation denied a cyber cause [S55].

The available accounts do not establish causality to the standard needed for a confirmed cyberattack count. This edition records the disagreement and excludes the outage from its confirmed malicious-incident set. It does not declare either account false.

6.4 Official communications accounts need their own recovery plan

On 15 October, An Garda Síochána said control of its official X accounts had been restored. It said the accounts would remain inactive during investigation and limited the unauthorised access to X. The inspected update said Garda ICT systems were not involved [S57].

The scope matters. A social-platform account can publish convincing material while the organisation's operational network remains unaffected. Conversely, normal internal systems do not make an unauthorised public message harmless. The organisation needs a known alternate channel and a process for disavowing misleading posts.

Communications teams should inventory platform administrators, recovery contacts, delegated tools and emergency authority. Test how to remove an obsolete administrator and how to reach the platform when normal access is unavailable. The exercise should establish both who can act and where the public can find a trusted update.

6.5 Threat emails require a coordinated safety response

November reporting describes emailed threats to schools and other organisations. The Garda response described in national reporting did not treat those messages as credible threats. The messages themselves do not establish access to a school's network or responsibility for a separate infrastructure incident [S58].

Preserve the message and its delivery information through an authorised reporting route. Physical-safety decisions belong with the responsible safety and law-enforcement teams. The cyber team should support evidence preservation without turning a threatening message into an unsupported technical attribution.

A useful public statement has four parts: what is affected, what is known, what remains under investigation and where to obtain the next update. Keep internal technical identifiers and personal information out of that statement. Correct an earlier assessment explicitly when evidence changes.

6.6 Readiness without accepting a political narrative

A new target list or responsibility claim can justify checking public-service availability and contacting a mitigation provider. It does not require endorsing the claimant's description of government policy, foreign relations or motive. Preparedness follows the operational signal.

For DDoS readiness, identify which services need continuity, how to distinguish legitimate demand from abnormal load and who can authorise mitigation. Agree an exercise with the service provider and a fallback status channel. An actor's success screenshot is not an acceptable availability test.

KEY TAKEAWAYS

01

Service impact, cause and responsibility need separate evidence.

02

Preserve official scope limits when discussing social accounts and disputed outages.

03

Prepare trusted status communications and safe operational recovery before a claimant creates urgency.

CHAPTER 07

Threat actors and extortion listing claims

THIS CHAPTER ANSWERS

Which actor labels and relationships are supported, and what do the listing comparisons establish?

32

Ireland-labelled extortion listings in the research window

7.1 Universe card 63
7.2 Four regional peers 64
7.3 Group labels in the Irish listing set 65
7.4 The relationship map represents evidence relationships 68
7.5 State attribution remains a source-specific question 69
7.6 The defender's actor question is operational 70

CHAPTER 07

Threat actors and extortion listing claims

IN SHORT

Ransompedia records thirty-two Ireland-labelled extortion listings in the window. Qilin leads with seven listings, followed by The Gentlemen with five; INC Ransom and Akira each have three. Listing labels do not identify every affiliate, entry route or outcome. Separate the observed publication from any independently disclosed incident, and use a relevant listing to start validation and recovery preparation.

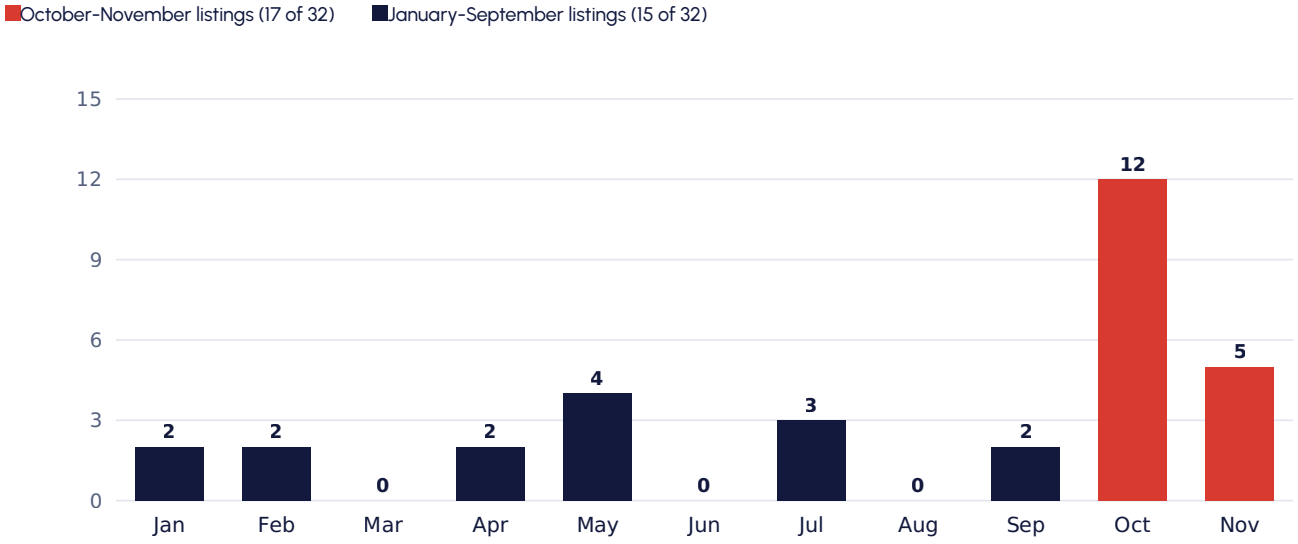
7.1 Universe card

Item	Definition
Population	Listing records labelled Ireland in the retained Ransompedia snapshot
Window	Listing publication dates from 1 January through 22 November 2026
Snapshot	Records read on 23 November 2026
Unit	Listing record, not independently confirmed incident or distinct victim
Window count	32, associated with 17 group labels
Earlier baseline	21 Ireland-labelled records in the whole of 2025
Recent window	4 listing records dated 8–22 November
Limits	Labels, repeated organisations and unlisted incidents affect interpretation; publication is not the intrusion date

[S3]

Listing publication was heavily back-loaded. Seventeen of the thirty-two Ireland-labelled records (53.1%) appeared in October (12) and November (5), compared with fifteen records across the first nine months of the year [S3].

October and November account for 17 of the 32 Ireland-labelled ransomware listings



Source: Brandefense Ransompedia, 32 Ireland-labelled extortion listings by publication month, 1 January–22 November 2026; November partial, 23 November 2026 snapshot [S3]. Publication dates are not intrusion dates; claims remain unverified.

Raw listing totals also overstate distinct claimed subjects. Across the thirty-two records, at most twenty-eight distinct subjects appear. Some subjects appear more than once, including repeated listings under one label and the same subject under two labels. Where source industry tags appear more than twice, retail and commerce (4), consulting (3) and construction (3) lead the aggregate counts [S3].

A publication can be an allegation of theft, encryption or threatened disclosure. It may repeat an earlier incident or use information whose age is unclear. Inclusion in Ransompedia does not provide independent confirmation of the allegation.

Where a listing and a company disclosure appear related, compare the particular propositions. The disclosure may confirm an interruption while saying nothing about a claimed archive size. Do not let the listing supply missing data fields, an access route or a victim total.

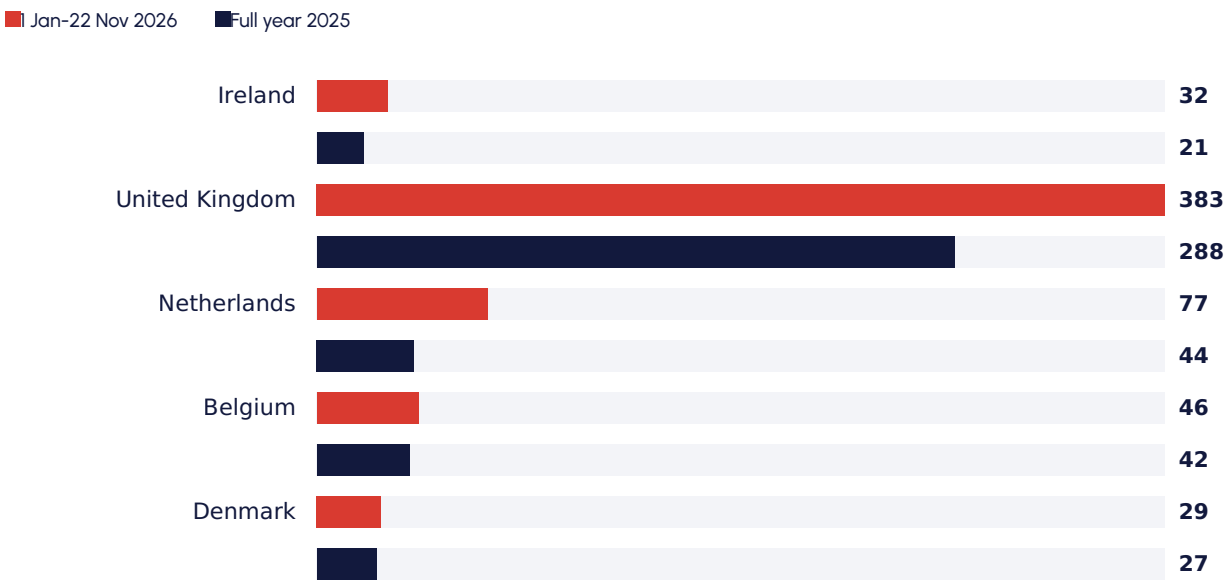
7.2 Four regional peers

The same publication window is used for the Ireland and peer-country listing totals. The earlier column is a complete calendar year, so it is not a matched-duration growth baseline.

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

Country	2026 window	Whole 2025	Group labels in window
Ireland	32	21	17
United Kingdom	383	288	80
Netherlands	77	44	29
Belgium	46	42	22
Denmark	29	27	19

Extortion listing counts describe different national publication populations



Source: Brandefense Ransompedia, 1 January-22 November 2026 versus full-year 2025, 23 November 2026 snapshot [S3]. Unequal periods and different populations; country-labelled claims, not unique victims, confirmed intrusions or a national security ranking.

[S3]

The peers provide nearby financial, digital-service and supplier contexts. Differences in country size, disclosure practices, source visibility and market participation remain. These figures support descriptive comparison, rather than an estimate of an organisation's chance of attack.

Ireland's 32 listings and Denmark's 29 are not evidence of equivalent national risk. The UK's larger number is not an adjusted comparison of security performance. A defender should use the country's listing presence to justify continuity and information-risk preparation, then validate its own exposure.

7.3 Group labels in the Irish listing set

The most frequent labels are Qilin with seven records, The Gentlemen with five, INC Ransom with three and Akira with three. Together these labels account for eighteen of the thirty-two listing records. That concentration concerns publications, not a verified division of operational work [S3].

Label	Listings	What the label does not establish
Qilin	7	A single operator, common affiliate or uniform access route
The Gentlemen	5	Every claimed dataset's authenticity or a completed sale
INC Ransom	3	Encryption at each named organisation
Akira	3	The identity of an initial-access provider
Other labels	14	Fourteen separate teams or fourteen unique incidents
Total	32	A complete national extortion census

This report keeps derivative public claims distinct from official disclosures. A listing without a verified original response remains a claim. Recent publication of an older allegation does not establish a new intrusion.

Secondary monitoring feeds also echoed listings already present in the thirty-two-record Ransompedia population. Those echoes supply no official organisation confirmation and are not counted as separate public incidents [S1][S3].

Qilin

Label in the retained listing population

Extortion listing label | No state attribution made in this report

IN IRELAND, 2026

1 January–22 November

7 Ireland-labelled listing records

CLAIMED TARGETS

Listing subjects labelled Ireland; identities withheld

SEEN IN PUBLIC REPORTING

[S3] 7 retained listing associations; own data, not incident confirmation

OUR ASSESSMENT

Validate claims internally; no affiliate, encryption, loss or access established.

CONFIDENCE

High for retained label count; incident outcomes unverified

The Gentlemen

Label in the retained listing population

Extortion listing label | No state attribution made in this report

IN IRELAND, 2026

1 January–22 November

5 Ireland-labelled listing records

CLAIMED TARGETS

Listing subjects labelled Ireland; identities withheld

SEEN IN PUBLIC REPORTING

[S3] 5 retained listing associations; own data, not incident confirmation

OUR ASSESSMENT

Validate claims internally; no affiliate, encryption, loss or access established.

CONFIDENCE

High for retained label count; incident outcomes unverified

INC Ransom

Label in the retained listing population

Extortion listing label | No state attribution made in this report

IN IRELAND, 2026

1 January–22 November

3 Ireland-labelled listing records

CLAIMED TARGETS

Listing subjects labelled Ireland; identities withheld

SEEN IN PUBLIC REPORTING

[S3] 3 retained listing associations; own data, not incident confirmation

OUR ASSESSMENT

Validate claims internally; no affiliate, encryption, loss or access established.

CONFIDENCE

High for retained label count; incident outcomes unverified

Akira

Label in the retained listing population

Extortion listing label | No state attribution made in this report

IN IRELAND, 2026

1 January–22 November

3 Ireland-labelled listing records

CLAIMED TARGETS

Listing subjects labelled Ireland; identities withheld

SEEN IN PUBLIC REPORTING

[S3] 3 retained listing associations; own data, not incident confirmation

OUR ASSESSMENT

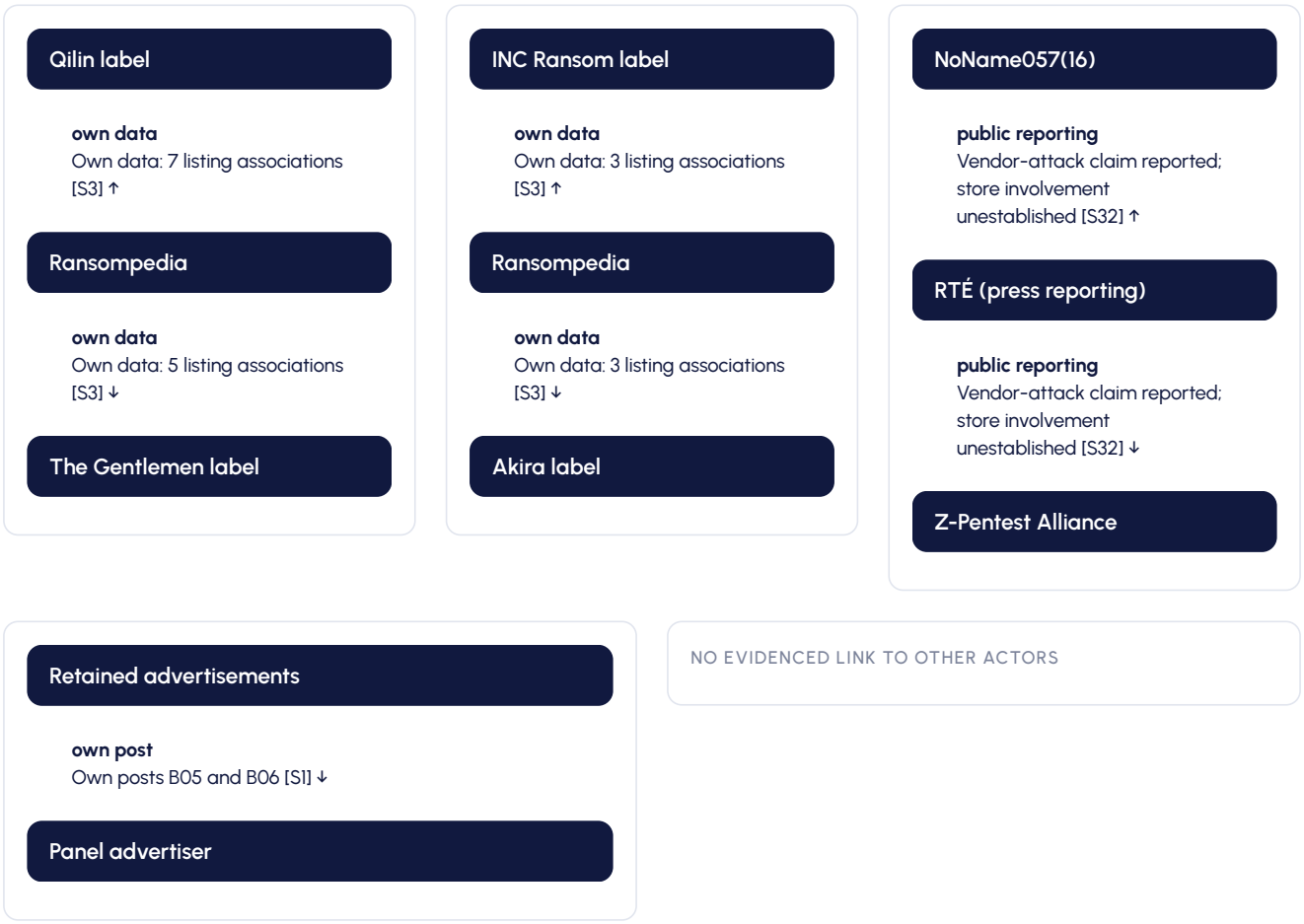
Akira ties INC Ransom for third place; treat each entry as an unverified claim.

CONFIDENCE

High for retained label count; incident outcomes unverified

7.4 The relationship map represents evidence relationships

Own post Relay Official statement Public reporting Our observation



Analytical model of evidence relationships. Edges identify listing associations or reported claims, not cooperation, shared infrastructure or a common operator.

The map connects Ransompedia to listing labels as own data. It connects RTÉ press reporting to vendor-attack claimants and retained advertisements to an advertising persona. These are source-to-subject relationships. They do not depict an attacker alliance, a payment flow or a shared operator.

A forum persona, a ransomware label, a dataset title and a delivery venue are different entities. A matching title supports a relationship between advertisements. It does not prove file identity, original theft or a transaction between the advertisers.

The same principle applies to repeated political branding. A shared slogan may be easy to copy. Without a concrete common element, it cannot establish that two claims came from the same operational team. An inferred chain would be an analytical model, rather than a demonstrated relationship.

7.5 State attribution remains a source-specific question

The original company notices used for the Irish manufacturing cases establish disruption and scoped investigation findings. They do not, by themselves, establish a state actor. This report does not fill that gap with a claimant's alignment, a news headline or a language label [S20][S22].

The refrigeration vendor-attack claims likewise remain attributed claims. They are not converted into state attribution for Ireland [S32]. Political descriptions are retained only when needed to understand a source's statement, and the source remains attached to the description.

No Ireland-specific APT technique matrix is asserted from this evidence set. A global advisory can be relevant to an Irish organisation without establishing local exploitation. Inventing an Irish victim population or applying a technique list without matching evidence would reduce the report's value.

NCSC also published warnings about global Axios and developer supply-chain incidents. They are relevant to dependency and credential review, but the inspected advisories do not establish an Irish downstream victim total. Their inclusion is technical context, rather than an additional Irish incident family [S70][S71].

7.6 The defender's actor question is operational

A useful intelligence request identifies the decision that would change. Does a credible listing match the organisation's data? Does an advertised service correspond to an active account? Does the provider's investigation identify a persistence risk that changes restoration?

The answer should identify its evidence level. An actor profile can help a responder prepare questions, but it cannot replace the organisation's own investigation. Preserve alternative explanations, especially older data, a supplier copy, repeated advertising and an unrelated organisation with a similar name.

KEY TAKEAWAYS

01

Thirty-two listings describe claims published in a defined source population.

02

The peer and group comparisons do not establish attack probability or common operators.

03

Require proposition-level evidence before an actor label changes containment, attribution or customer communications.

CHAPTER 08

Identity, accounts and the fraud economy

THIS CHAPTER ANSWERS

How can advertised information become a fraud opportunity without establishing a new intrusion?

4

separate decisions: identity, recovery, payment and customer protection

8.1 A record offer and an access offer are different 72
8.2 Requests show demand, not fulfilment 72
8.3 Bank-themed phishing advertising in the recent window 73
8.4 Personal information can bridge separate services 73
8.5 Narrow payment-card observations 73
8.6 Prices measure asking terms 74
8.7 Official campaigns add evidence beyond named organisations 74
8.8 Joint ownership makes fraud signals useful 75

CHAPTER 08

Identity, accounts and the fraud economy

IN SHORT

The retained material includes identity and credential offers, buyer requests and bank-themed phishing advertising. These establish visible market activity, rather than working accounts or completed fraud. Public financial disclosures also show why accurate personal and payment details can make impersonation more persuasive. Test recovery and payment changes against an informed caller, and require independent verification before authorising a new trusted route.

8.1 A record offer and an access offer are different

A database advertisement asserts that information is available. A credential offer asserts a relationship between an account and a secret. An access advertisement asserts an ability to enter a service. The presence of one does not establish the others.

The corpus includes country-labelled credential lists whose 2026 posts repeat older offers. Those dates describe circulation. They cannot establish when information was first obtained, whether it remains usable or whether it concerns the organisation suggested by a title [S1].

Identity and fraud teams should assess relevance before choosing a response. A historical record already remediated may require a closed disposition. An active account with corroborating unauthorised activity requires containment. A name and contact detail can matter for impersonation even when no password is present.

Information age affects the decision differently for each field. A changed password can remove one route. A person's identity or past service relationship may continue to sound convincing. Avoid equating an old dataset with either a current account incident or a harmless record.

8.2 Requests show demand, not fulfilment

Some posts request Irish databases, business contacts or verification material. These are buyer statements. They do not establish that a supplier held matching data or completed a transaction. A reply expressing interest is not proof of payment [S1].

For a business-to-business contact offer, potential fraud relevance includes supplier impersonation and payment diversion. The organisation should validate a payment-instruction change through a previously established channel. It should not infer that the advertised contacts came from a newly accessed internal system.

Verification-document advertising has a separate evidential limit. An advertised passport image or selfie does not establish a usable identity package, successful onboarding or the real identity of the person operating the account. Customer-protection controls should test document and recovery decisions through authorised synthetic exercises.

8.3 Bank-themed phishing advertising in the recent window

The recent corpus includes an advertiser offering a phishing panel that lists an Irish bank among supported themes. That demonstrates advertising on the stated dates. It does not demonstrate that the bank's systems were accessed, that its customers received the kit or that an account was used [S1].

The appropriate first question is whether an owned service or customer population has corroborating evidence of abuse. A kit title can justify preparing a customer warning and reviewing relevant controls. It cannot supply a successful-login count.

Review suspicious communications alongside sign-ins, session changes, recovery events and payment activity. A page can collect information without producing a usable session. A session can be abused after the original page is gone. Preserve those distinctions in the investigation record.

For customer communications, explain how to reach the organisation through a known route. Avoid repeating a live phishing link, a criminal contact or an exposed record. The warning should help the recipient make a safe decision without amplifying the advertiser.

8.4 Personal information can bridge separate services

The saved-payee supplier disclosure concerns information that can make a payment-related conversation credible. The financial-services portal case separately concerns portal availability and an unconfirmed press report of limited data exposure. The report does not establish that either dataset was used in fraud [S26][S30].

Their shared planning implication is to reduce reliance on easily learned details. An employee or customer who knows a name, address or beneficiary relationship should still need an authorised route to change access or payments. A support agent should be able to stop and escalate an unusual recovery request.

Businesses should test this through the full workflow. A caller can fail normal sign-in but persuade a support team to change a telephone number. A fraudulent invoice can pass a mailbox check but request a new beneficiary. The exercise should follow the final authorisation decision.

8.5 Narrow payment-card observations

SCOPE OF THE CARD FIGURES

These limited, unverified payment-card observations do not measure national card theft, active cards, issuer prevalence or fraud losses.

The limited payment-card observations comprise 298 distinct Ireland-labelled cards, 313 posts and 350 appearances. Labels remain unverified. These are not national card-theft, active-card or fraud-loss figures [S4].

The issuer and country descriptions in a post are not independent validation. No card number, personal detail or criminal contact is reproduced. A public report cannot establish that an advertised card works or that a payment was authorised [S4].

An issuer receiving a relevant alert should use its authorised account and transaction evidence. Assess freshness, actual authorisation activity and prior remediation before deciding on customer contact or replacement under issuer policy. A broad country label alone is an insufficient basis for disruption.

8.6 Prices measure asking terms

The case cards preserve a limited set of asking terms where they aid interpretation. They are not transaction records. A seller's price can change between posts or apply to an unclear quantity. It cannot establish criminal income or what an authentic record would cost [S1].

Advertised item	Quoted asking terms	Evidence boundary
Retail-admin access repost	$500 opening; $3,500 immediate-purchase term	Secondary auction claim; no completed sale established [S1]

A price should therefore be read with its unit and evidence status. A request for a negotiated quote is different from a fixed asking price. A paid forum's access condition is different from a sale of the claimed underlying data.

8.7 Official campaigns add evidence beyond named organisations

The Central Bank's April warning describes comparison sites that collect prospective investors' details before callers impersonate banks. A spring warning describes impersonation abusing cloned financial and official-looking identities. Neither warning establishes an intrusion into the impersonated organisation [S60][S61].

An early-year notice also describes advance-fee loan impersonation. A November warning adds a cloned investment identity. These warnings establish reported scam activity and the regulator's caution, rather than a count of successful transactions [S62][S63].

Period	Officially described activity	Defender decision
Early 2026	Advance-fee loan impersonation [S62]	Verify the provider independently before supplying money or documents
April	Investment comparison forms followed by bank impersonation [S61]	Confirm both authorisation and the actual contact route
Spring 2026	Cloned financial and official-looking identities [S60]	Treat apparent official branding as insufficient proof
November	Investment-identity cloning [S63]	Warn relevant customers without alleging a legitimate-firm incident

Garda enforcement adds a different population. Operation Skein's February notice describes searches, not victim incidents. Another February action involved Irish investigative work concerning Maltese victims. May cross-border action records arrests in Ireland and Northern Ireland separately [S64][S65][S66].

These actions show why geography and units matter. An investigation conducted in Ireland can concern losses elsewhere. A device seizure, arrest or charge is not a confirmed intrusion or a finding of guilt. No actor alliance is inferred across the separate notices.

The Central Bank's September statistical release reports €179.04 million in fraudulent payments across Irish-resident providers in 2025, up 27.2% from €140.80 million in 2024. Cross-border payments accounted for 69.8% (€124.89 million), up 6.3 percentage points from 2024, while fraud affected roughly one in 10,000 payment transactions. This is a prior-year payment population, not national cybercrime losses in 2026, and is kept separate from post counts and listing claims [S59].

8.8 Joint ownership makes fraud signals useful

Signal	First owner	Validation	Completion evidence
Credible employee credential offer	Identity operations	Active account, relevant service and prior remediation	Dated disposition and session review
Customer identity or beneficiary information	Fraud and privacy	Actual data fields and plausible misuse	Customer-protection and notification decision
Bank-themed kit advertising	Threat intelligence and fraud	Matching campaign or owned-service evidence	Relevant warning or closed intelligence lead
Payment-change request	Treasury or accounts payable	Confirmation through a known separate route	Verification record before authorisation
Verification-document offer	Customer onboarding	Relevant identity and authorised fraud evidence	Escalation or documented non-match

The common objective is a supported decision. Measure unresolved relevant signals, time to validation and the owner accepting residual risk. Advertisement volume alone cannot show whether the organisation improved its controls.

KEY TAKEAWAYS

01

Advertising, demand, usable access and completed fraud are separate propositions.

02

Older information can still support impersonation without establishing a new intrusion.

03

Join identity, fraud, privacy and payment owners around the actual authorisation decision.

CHAPTER 09

Financial services: data, suppliers and customer trust

THIS CHAPTER ANSWERS

Which financial-service decisions need security, fraud and operational owners together?

30

selected financial-service estates; not thirty licensed banks or card issuers

9.1 Define the financial population before using a number 77
9.2 Saved beneficiary details require an impersonation response 78
9.3 A portal interruption needs an accessible alternative 78
9.4 Historical contact-centre findings remain relevant 79
9.5 DORA creates a separate reporting sequence 79
9.6 Five questions for a financial-service exercise 79

CHAPTER 09

Financial services: data, suppliers and customer trust

IN SHORT

The Irish financial evidence concerns supplier-held beneficiary information, an interrupted financial portal, identity offers and phishing advertising. The selected finance cell includes several types of institution and international service, so it is not a bank-licence or card-issuer population. Establish the particular service, customer information and reporting duty before choosing containment, communications or customer protection.

9.1 Define the financial population before using a number

The selected portfolio contains thirty financial-service estates. It includes banking, insurance, investments, payment services and other activities. Related estates and international operators can overlap. The unit is a domain estate selected for relevance, rather than an independent legal entity [S2].

Passive security-control observations on 27 November 2026 show strong baseline email authentication alongside narrower DNS and web-header gaps. Across the 30 selected financial estates, 26 (86.7%) publish reject (21) or quarantine (5) DMARC policies, the highest share across all eleven sectors, leaving 3 in monitoring mode and 1 missing [S2][S44]. SPF appears on 29 of 30 estates, public DKIM records on 19 and DNSSEC delegation on 2 [S2][S45][S46][S47]. Valid TLS appeared on 28 estates, with 1 validation failure and 1 unavailable; among 24 available HTTP responses, 16 set HSTS and 10 set Content Security Policy [S2][S48][S49].

The financial subset contains 30 selected estates. Its snapshot records 9 estates with a credential listed for sale, alongside at least 55,695 device associations. These are service-domain associations, not proof of infected bank infrastructure or Irish customer losses. No financial-sector rating is published [S2].

Population	Selected estates	Estates with current credential listings	Device associations	Employee-device associations	Credential-record associations
Selected financial estates	30	9	55,695	5,097	430,729
Card-issuing financial estates	9	3	37,313	77	52,669

Device figures are minimum observed counts. The nine card-issuing financial estates are a subset of the thirty selected financial estates, not a census of licensed banks or card issuers. They account for 67.0% of financial-sector device associations (37,313 of 55,695), almost entirely in non-employee records (37,236, or 99.8%, versus 77 employee-device associations) [S2].

Within the 9 card-issuing financial estates, all 9 publish reject (8) or quarantine (1) DMARC policies, publish SPF and present valid TLS [S2]. Public DKIM records appear on 5 of 9 and DNSSEC delegation on 1 of 9. Among 5 card-issuing estates returning available HTTP responses (4 unavailable), 4 set HSTS and 4 set Content Security Policy [S2].

Identity and fraud teams should coordinate relevant follow-up. Neither population establishes the source of a card record or an issuer infrastructure incident.

The report's limited, unverified payment-card observations are separate from this estate population. They do not measure issuer losses or national card theft. They cannot be used to rank the selected financial organisations [S4].

9.2 Saved beneficiary details require an impersonation response

The November supplier incident should prompt each affected institution to establish its own information scope. A provider's service may hold beneficiary records for many customers, while notifications and data quality differ. A group-level estimate does not identify an individual's affected fields [S26][S27].

The customer-protection decision should account for plausible misuse without claiming that misuse occurred. Accurate information about a payee can support a convincing call. Advise customers to use a known contact route and to question urgent instructions to move money.

Internally, decide which team can issue the first warning while investigation continues. Privacy may own affected-data analysis, fraud may own customer protection and technology may own supplier containment. One incident lead should maintain the shared factual chronology.

9.3 A portal interruption needs an accessible alternative

The financial-services portal disclosure illustrates a continuity question alongside the data question. A customer may need account information while normal portal access is suspended. A safe alternative must preserve identity checks without creating an easily exploited emergency exception [S29][S30].

Exercise the contact centre at realistic volume. Confirm what staff can see, what they can change and how they handle a caller whose registered device is unavailable. Record which transactions require stronger verification and which can wait safely.

Restoration should test more than the ability to sign in. Check that permissions, client records, notifications and relevant audit records remain consistent. A service owner should accept the result, while unresolved privacy questions remain assigned.

A separate 2026 financial-service disclosure described information released after fraudulent requests presented through an apparent official channel. That account concerns the authorisation of a disclosure, rather than established access to the provider's whole infrastructure. This report supplies no Irish affected-person total from it [S56].

9.4 Historical contact-centre findings remain relevant

The DPC's financial-sector contact-centre decision published in 2026 concerns earlier events. Its value is the control question, rather than a new current-year attack count: can a malicious caller turn known customer information into an unauthorised access decision [S39]?

Ask the contact-centre owner to demonstrate both the normal route and its exceptions. Review changes to registered contact details, replacement approval devices, password recovery and delegated authority. Logs should show who authorised a change and the evidence used.

An effective exercise also checks recovery for a legitimate customer. A process that simply refuses every difficult request can encourage informal exceptions later. Measure whether the correct customer regains access through the authorised route while the impersonator is stopped.

9.5 DORA creates a separate reporting sequence

The Central Bank states that DORA has applied since 17 January 2025 and provides a reporting route for in-scope financial entities. Major ICT incidents and voluntary significant-threat notifications are different categories [S9] [S10].

The incident team should preserve awareness and classification times. A supplier's incident is not automatically reportable under every rule, and a service returning does not remove an existing reporting requirement. Chapter 10 gives the sequence and qualifications [S11].

Outsourced operations still need a named internal reporting owner. Ask the provider for information early enough to support classification, with updates when the scope changes. Do not make the first useful notice depend on a completed forensic report.

9.6 Five questions for a financial-service exercise

Question	Owner	Evidence needed
Which customer fields are involved?	Data owner and privacy	Institution-specific scope, with unresolved fields identified
Can a support request create a new trusted route?	Identity and contact centre	Authorised impersonation test and exception log
Can payments continue safely during a portal interruption?	Operations and fraud	Tested alternative with controlled permissions
Can the provider support timely classification?	Supplier owner and incident lead	Initial notice and update timings against the agreed route
Can the institution restore and reconcile service data?	Technology and business owner	Recovery record, integrity checks and acceptance

These are suggested exercise questions, not a statement that every financial organisation failed them. Their priority follows from the disclosed service relationships and the unresolved propositions in the retained claims.

The Central Bank's 19 November Financial Stability Review examines how common technology dependencies could transmit cyber disruption across financial services. Its AI discussion is an assessment of possible systemic risk, rather than a new Irish victim count. It calls for preparation covering containment, recovery and third-party dependencies, alongside prevention. The review also identifies CIISI-IE as a channel for cyber information sharing [S72][S76].

KEY TAKEAWAYS

01

The selected financial estates are not a licensed-bank or issuer census.

02

Treat beneficiary information, portal availability and account recovery as separate customer decisions.

03

Keep supplier evidence, incident classification and reporting ownership in one coordinated exercise.

CHAPTER 10

Regulatory duties and national response

10

THIS CHAPTER ANSWERS

Which duties apply now, and how should an incident team preserve the right reporting clocks?

3

separate assessments: privacy, financial resilience and network-security obligations

10.1 Applicability comes before a deadline 82
10.2 GDPR: authority notification and notice to people differ 83
10.3 DORA: preserve awareness and classification times 83
10.4 NIS2 preparation should not invent Irish commencement 84
10.5 Enforcement dates are not incident dates 84
10.6 Historical statistics need their own denominator 85
10.7 Rehearse one factual record with several reporting decisions 85

CHAPTER 10

Regulatory duties and national response

IN SHORT

A personal-data breach, a major financial ICT incident and an essential-service incident have different scope and reporting tests. Ireland's NIS2 transposition status must not be assumed from the European directive alone. Enforcement decisions also distinguish older events from current obligations. Identify the applicable entity and regime, preserve awareness times and rehearse the first notification with legal, privacy and service owners.

This chapter is an operational reading aid. Applicability and legal interpretation require the organisation's own qualified assessment. Proposed measures, guidance and existing duties are kept separate.

10.1 Applicability comes before a deadline

Regime or function	Verified position	Operational task
GDPR	Personal-data reporting duties depend on the risk to people [S8][S12]	Identify controller and processor roles; preserve awareness and risk assessment
DORA	Applied since 17 January 2025 to in-scope financial entities [S9]	Classify the incident and use the competent-authority reporting route
Existing network-security regime	NCSC states the earlier regime continues for already designated essential-service operators [S7]	Confirm designation and the applicable reporting arrangements
NIS2 transposition	Inspected NCSC material describes work continuing; no new Irish commencement date is established here [S7]	Track enacted measures and commencement; do not present a draft as law
Criminal reporting	NCSC distinguishes cybercrime and directs victims towards An Garda Síochána [S42]	Preserve evidence and coordinate criminal reporting separately

A group may need more than one assessment from a single technical chronology. The relevant legal entity, data-processing role, service and country can differ. A supplier contact or a criminal report should not be treated as automatically completing a separate regulatory duty.

10.2 GDPR: authority notification and notice to people differ

Under Article 33, a controller notifies the competent supervisory authority without undue delay and, where feasible, within 72 hours of awareness, unless risk to people's rights and freedoms is unlikely. Delays require reasons. A processor informs the controller without undue delay [S12].

Article 34 separately addresses communication to affected people where high risk is likely, subject to its qualifications. The DPC's guidance also requires an internal record when an organisation decides a breach presents no risk. A decision not to notify should therefore have an owner, reasons and retained evidence [S8][S12].

Incomplete information does not justify waiting for every forensic question to close. Record what is known and provide supported updates through the applicable process. Avoid unnecessary personal information in the notification record and preserve the authority's case reference [S8].

The awareness record should distinguish the first alert, the organisation's assessment and a later supplier update. An advertisement is not automatically proof of a personal-data breach. Once relevant evidence establishes a breach, the organisation must assess its obligations from those facts.

10.3 DORA: preserve awareness and classification times

The Central Bank provides templates and portal guidance for major ICT-incident reports and significant-threat notifications. Scope and classification depend on the applicable financial framework. A country report cannot classify a particular institution's incident from a press headline [S10].

Article 5 of Delegated Regulation 2025/301 sets the sequence below.

Stage	Time requirement	Qualification
Initial	As early as possible; within four hours of major classification and no later than 24 hours after awareness	Later major classification after that period starts a four-hour reporting period
Intermediate	Within 72 hours after initial notification	Update without undue delay, including when regular activities recover
Final	Within one month after the intermediate report or latest updated intermediate report	Preserve the relevant report date
Delay	Inform the authority by the relevant deadline	Explain the reason

[S11]

Article 5 permits a next-working-day noon adjustment for a deadline on a weekend or bank holiday. For initial and intermediate reports, the adjustment excludes credit institutions, central counterparties, trading-venue operators and other financial entities identified as essential or important under Article 3 of NIS2. This exclusion does not cover final reports. Competent authorities may also exclude other significant or systemic financial entities from the initial and intermediate adjustment [S11].

The practical control is a maintained reporting calendar with an authorised alternate reporter. Preserve both the awareness time and the time of major classification. Test an incident identified outside normal working hours, including an early supplier notice with incomplete data.

10.4 NIS2 preparation should not invent Irish commencement

Re-checked on 27 November 2026, NCSC's NIS2 page still carries a 24 June 2025 update date. It explicitly states that NIS2 registration and incident-reporting portals are not yet available and that the earlier regime remains operational for already designated operators. Because that update predates this report's window and inspected parliamentary records did not establish an enacted bill, this report does not certify the absence of later legislative developments [S7].

The verified conclusion is narrower: no new national commencement date is established by the sources used here. Organisations should confirm their present duties and track the enacted instrument and commencement provisions. A planning date in commentary is not an enforceable deadline.

Preparation can continue without making that legal claim. Maintain service and supplier inventories, assign incident authority, rehearse recovery and keep management informed. These are practical readiness actions in this report, rather than a representation that a particular draft provision already binds every organisation.

10.5 Enforcement dates are not incident dates

A 2026 DPC healthcare ransomware decision concerns an earlier incident and imposed a six-figure administrative fine with corrective measures. This is a 2026 enforcement development, rather than a newly occurring 2026 attack [S37].

Further 2026 decisions concern older physical-record storage failures and earlier financial contact-centre incidents. These sources belong in governance and learning, with their earlier occurrence preserved [S38][S39].

A fine also has a procedural status. The DPC explains that fines require court confirmation before they become payable and that an appeal can affect collection. A published decision or listed amount should not automatically be described as a collected payment [S41].

10.6 Historical statistics need their own denominator

The DPC's 2025 annual report records 6,521 breach notifications, with half arising from correspondence sent to the wrong recipient. It also records 16,160 new cases received (up 45% from 11,091 in 2024) and 11,734 cases concluded (up 12% from 10,510 in 2024). Four large-scale inquiries concluded alongside ten final decisions. Those prior-year figures include non-malicious handling failures and are not a count of Irish cyberattacks in 2026 [S40].

The distinction changes the control question. Secure data handling, retention and recipient verification can matter alongside attack response. A privacy team should not assume that every reported breach requires the same technical containment, or that a ransomware listing covers the wider notification population.

Ireland's May 2026 National Cyber Emergency Plan describes coordination for serious incidents affecting nationally important IT and operational systems. It recognises that a cause may be in an overseas or shared supplier environment and that physical consequences can require sectoral emergency coordination. The plan is guidance, rather than a new source of binding obligations. An organisation's exercise should connect its incident team, service leadership and relevant national contacts without assuming that national coordination replaces its own reporting duties [S73].

10.7 Rehearse one factual record with several reporting decisions

Record	Why it matters	Responsible function
First alert and supporting evidence	Separates observation from confirmed incident facts	SOC and incident lead
Awareness and classification times	Supports the applicable reporting sequence	Incident lead and legal
Data fields and affected service	Supports privacy and operational assessment	Data and service owners
Known facts and unresolved questions	Prevents unsupported public or regulatory statements	Investigation and communications
Notice submissions and updates	Records what was sent and when	Authorised reporter
Restoration and residual risk	Keeps recovery separate from final data scope	Business owner and CISO

KEY TAKEAWAYS

01

Scope and trigger determine the reporting clock.

02

Keep guidance, proposed measures, older incidents and current duties distinct.

03

Rehearse one factual chronology with the reporters responsible for each applicable regime.

CHAPTER 11

Outlook and assessment-change signals

11

THIS CHAPTER ANSWERS

What should an Irish organisation plan for, and what evidence would change that plan?

5

conditional planning judgements with validation signals

11.1 Judgements tied to the actual evidence 87

11.2 What would change the assessment 88

11.3 Conditional scenarios 88

11.4 Evidence that this report cannot supply 89

CHAPTER 11

Outlook and assessment-change signals

IN SHORT

The evidence supports preparation for supplier incidents, identity abuse, operational interruption and extortion claims. It does not support a numerical forecast of Irish attacks or financial loss. The scenarios below depend on specific signals and preserve alternative explanations. Assign an owner to each signal and change the response when the evidence changes.

11.1 Judgements tied to the actual evidence

Confidence applies to the stated proposition. High confidence that a notice exists is not high confidence in every allegation discussed beside it.

Judgement	Confidence	Basis and limit
Supplier relationships deserve a joint data and continuity exercise	High for the observed case set	Finance, education, healthcare and hospitality disclosures describe different dependencies; no national supplier-incident rate inferred
Credential and identity offers warrant current-account validation	High for observed advertising; account status unresolved	Retained posts establish offers and requests, including recirculated material, rather than usable access [S1]
Public-facing operational equipment merits immediate owner review where present	High for the protective decision	Confirmed grocery impact and NCSC advice; precise Irish entry route remains unestablished [S13][S14][S31]
Extortion preparation remains justified across sectors	High for listing presence	32 Ireland-labelled listing claims; publication is not independent incident confirmation [S3]
New disclosures can change customer protection before full technical closure	Medium as a planning judgement	November supplier and portal developments; individual information scope remains qualified [S26][S30]

The selected cases do not provide a representative estimate of what most Irish organisations experience. They show why the next decision may belong to a provider owner, contact centre, facilities manager or communications lead as well as a SOC.

11.2 What would change the assessment

Present boundary	New evidence	Decision changed
A credential offer is unverified	An active owned account and relevant unauthorised activity are corroborated	Escalate to incident response and contain the validated route
A supplier notice has incomplete individual scope	Institution-specific records or confirmed data categories become available	Update notification and customer protection
Refrigeration attribution is unestablished	A competent investigation publishes matching technical evidence	Update attribution and relevant hunting questions
A listing is a publication claim	Original disclosure confirms the relevant access, data or interruption	Move only the confirmed propositions into the incident record
A service interruption has a disputed cause	Authorised logs and investigation establish a cause	Change the incident classification without rewriting the original chronology
Exposure associations need current-account validation	Account and asset owners resolve a relevant signal using their own records	Build supported identity queues and retain the assessed denominator

An assessment should also change when evidence weakens a claim. A record may match an earlier notification, a title may identify the wrong jurisdiction or a customer may show that the advertised account was already closed. Record the reason for downgrading or closing the signal.

11.3 Conditional scenarios

Supplier information, followed by impersonation. If a provider confirms customer-contact or beneficiary information was accessed, prepare for convincing follow-up messages. This is a planning assumption, not a claim that fraud already occurred. The trigger is validated information scope or corroborating abuse. Fraud and communications should provide a known contact route and review recovery decisions.

Connected equipment, followed by unsafe settings. If an owned controller has unnecessary public management access or unexplained operating changes, involve the operational owner immediately. A malicious cause remains a question until investigated. The trigger for protective action can be unsafe operation itself. Verify safe state and approved remote access before returning normal control.

A credible market offer, followed by account evidence. If an offer matches an active owned account, compare it with current sign-ins, sessions and recovery changes. A match to an old password alone does not establish current use. Escalate when relevant unauthorised activity is corroborated, and preserve the evidence supporting containment.

An extortion listing, followed by pressure on communications. If a listing appears to concern the organisation, establish data ownership and service status before responding publicly. An archive quantity or countdown is the claimant's assertion. Use the incident lead's factual record, prepare continuity actions and reassess notification from verified information.

A new platform advisory, followed by dependency discovery. If a critical advisory applies to an owned runtime or embedded supplier component, identify the affected service and supported remediation. Do not wait for proof of local exploitation to assess an applicable weakness. Test the update and verify the running version, while investigating any independently observed suspicious activity.

11.4 Evidence that this report cannot supply

The report does not estimate the probability of intrusion, future ransomware volume or national fraud losses. Its post, listing and selected-estate populations do not provide the design needed for those estimates. A quieter observed month can reflect visibility, posting behaviour or coverage.

Likewise, missing official confirmation is not proof that a claim is false. Some incidents remain private, and some notices leave material questions open. The practical aim is to assign the next verification step without overstating what is known.

KEY TAKEAWAYS

01

Forecasts are conditional scenarios with visible triggers.

02

Change confidence when evidence strengthens or weakens a specific proposition.

03

Use the report to assign verification and recovery decisions, rather than predict a national attack total.

CHAPTER 12

A 30/60/90-day action plan

12

THIS CHAPTER ANSWERS

Who should act, under what condition, and what demonstrates completion?

18

actions with accountable owners and reviewable outcomes

12.1 Actions and completion evidence 91
12.2 Technical remediation that reflects the latest warning 93
12.3 Completion measures for management 94
12.4 First decisions by role 95
12.5 How Brandefense can help 96

CHAPTER 12

A 30/60/90-day action plan

IN SHORT

Begin with the services, providers and identities that matter to your organisation. Validate credible account signals, establish supplier notification routes and remove unnecessary access to operational equipment where it exists. Then test customer recovery, platform remediation and business restoration. Use the plan as a sequence of accountable decisions, and bring a current material incident into the response process immediately.

12.1 Actions and completion evidence

The schedule is a suggested planning sequence, not permission to delay a current incident. Adjust timing to service criticality, applicable duties and evidence. Every deferred action needs a named risk owner and review date.

1Days 1–30		
Identify the important service, its identity provider, data custodian and recovery authority	OWNER CISO and service owners	COMPLETION EVIDENCE Approved service map with operational contacts
Confirm a usable source of relevant credential and access alerts; where absent, establish an authorised route	OWNER Threat intelligence and identity	COMPLETION EVIDENCE Alert owner and first test record
Validate each credible owned-account signal, including freshness and prior remediation	OWNER Identity operations	COMPLETION EVIDENCE Dated active, historical, unrelated or unresolved disposition
For corroborated unauthorised account activity, investigate sessions, recovery changes and delegated permissions	OWNER Incident response and identity	COMPLETION EVIDENCE Evidence record, containment and recovery decision
Identify providers holding customer or beneficiary information and agree an early incident-notification route	OWNER Supplier and data owners	COMPLETION EVIDENCE Provider-specific contact test and information checklist

Where remotely managed operational equipment exists, remove unnecessary public access through a safe change process

OWNER
Facilities, network and provider

COMPLETION EVIDENCE
Reviewed access path and operational acceptance

2Days 31–60

Rehearse a supplier notice with incomplete individual scope

OWNER
Incident lead, privacy and supplier owner

COMPLETION EVIDENCE
Awareness chronology, initial assessment and update decision

Test customer and employee recovery against an informed impersonator

OWNER
Contact centre and identity

COMPLETION EVIDENCE
Authorised test, blocked impersonation and successful legitimate recovery

Require independent confirmation for payment-instruction changes

OWNER
Treasury and accounts payable

COMPLETION EVIDENCE
Sampled verification records and exception owner

Review privileged and recovery access for phishing-resistant authentication [S43]

OWNER
Identity and platform owners

COMPLETION EVIDENCE
Coverage record, supported exception plan and tested recovery

Inventory affected PHP runtimes, including embedded dependencies; apply supported fixes and verify running instances

OWNER
Application and platform owners

COMPLETION EVIDENCE
Branch-specific version evidence and service acceptance

Where mail-policy gaps are confirmed (74 of 250 estates remain in monitoring or missing DMARC), inventory legitimate senders and stage an approved policy change

OWNER
Messaging owner

COMPLETION EVIDENCE
Alignment test, change record and rollback route

Test restoration of an important business service using protected recovery access

OWNER
Infrastructure and business owner

COMPLETION EVIDENCE
Timed restore, integrity checks and business acceptance

Rehearse privacy, financial and other applicable reporting decisions outside working hours

OWNER

Legal, privacy and incident lead

COMPLETION EVIDENCE

Authorised reporters, timestamps and completed exercise reports

3Days 61–90

Review public social-account administrators, recovery contacts and delegated tools

OWNER

Communications and identity

COMPLETION EVIDENCE

Access review and tested alternate status channel

Exercise an availability incident with a simultaneous unverified data claim

OWNER

Operations and communications

COMPLETION EVIDENCE

Separate service, cause and attribution decisions

Validate relevant certificate, DNS and web-control findings with the responsible application owner

OWNER

Network and web owners

COMPLETION EVIDENCE

Tested remediation or dated justified exception

Report unresolved relevant signals and recovery results to management

OWNER

CISO and risk owners

COMPLETION EVIDENCE

Board record with named owners and review dates

12.2 Technical remediation that reflects the latest warning

The 20 November NCSC PHP advisory introduces later remediation than the October advice. The examples below use two November CVEs re-checked on 27 November 2026 against NVD, CNA records and PHP's 19 November security releases. Both NVD records remained in Awaiting Analysis status on 27 November. They are platform guidance, not claims that exploitation occurred in Ireland [S15][S16][S17][S18][S19].

Branch	Affected range in the vendor advisories	Fixed release for these examples
PHP 8.2	8.2.x before 8.2.36; affected historical code also predates this branch	8.2.36
PHP 8.3	8.3.0 to before 8.3.37	8.3.37
PHP 8.4	8.4.0 to before 8.4.28	8.4.28
PHP 8.5	8.5.0 to before 8.5.13	8.5.13

CVE-2026-126714 concerns interrupted writes in the file-based session handler. The vendor describes conditions involving influence over session data and a suitable application path. CVE-2026-129289 concerns unread request data and persistent backend connections. Their conditions differ; the titles are not a claim that every PHP installation has an identical exploitable route [S16][S17].

The listed versions are fixes for these examples, rather than a promise that no later update is needed. Use the current supported vendor release and any applicable distributor backport evidence. For unsupported branches, plan migration rather than assume a listed fix exists [S15].

Verify the runtime actually serving the application. A package record, a dormant container image or a changed build manifest may not identify every running worker. Include supplier-embedded runtimes in the ownership record. The response should establish applicability and completion without testing an exploit against third-party services.

The 20 November OpenSSL advisory concerns CVE-2026-121481 in the library [S74][S75]. Re-checked on 27 November 2026, OpenSSL's official CVE record (updated 25 November) retains Low severity and states that no attacker-triggered path has been identified [S79]. Reaching the defect requires an unusually large application-supplied input. NVD remained in Awaiting Analysis status on 27 November while carrying a contributed secondary CVSS v3.1 score of 5.9 (Medium) [S75].

Branch	Affected range in official CVE record	Fixed-version boundary	Vendor download page on 27 November
OpenSSL 4.0	4.0.0 before 4.0.4	4.0.4	4.0.3 listed [S80]
OpenSSL 4.1	4.1.0 before 4.1.1	4.1.1	4.1.0 listed [S80]

Fixed-version boundaries in the CVE record do not establish release availability, and OpenSSL 3.5.9 LTS is unaffected by this record. Confirm an available supported release or distributor backport for the affected application before remediation. These sources do not establish exploitation in Ireland [S79][S80].

For refrigeration, follow the separate NCSC advice on protected management access and operational settings. Its November update cautions that changing passwords, enabling a session mode or updating firmware alone does not secure a public-facing controller. Treat isolation and safe remote access as their own actions [S14].

12.3 Completion measures for management

These are suggested operational measures. They do not derive a control-success rate from post or listing volumes.

Measure	Suggested completion test
Relevant signals have owners	Every credible open signal has a validation owner and review date
Account decisions are supported	Disposition records distinguish active, historical, unrelated and unresolved evidence

Measure	Suggested completion test
Supplier notices are usable	A test notice reaches the right responder and identifies the affected service and data questions
Recovery is controlled	Legitimate users regain access while an informed impersonation attempt fails
Recovery is operational	Important service restored, reconciled and accepted against its own recovery objective
Reporting is rehearsed	Applicable awareness, classification and submission times retained in the exercise
Operational equipment is safely managed	Approved remote access and independently checked safe settings
Exceptions are governed	Every overdue action has an owner, reason and dated review

A missed target should produce a decision, rather than a cosmetic improvement to a headline. Report why validation remains incomplete, what service depends on it and who accepts the residual risk. These details let management distinguish a temporary evidence gap from an unattended risk.

12.4 First decisions by role

Role	First decision	Evidence to request
Board	Which important service has the least credible recovery evidence?	Last complete exercise and unresolved dependencies
CISO	Which credible signals lack a validation owner?	Current queue with dates and accountable functions
SOC	Which observed activity can be corroborated in owned records?	Relevant identity, endpoint and service evidence
Fraud	Which recovery or payment change can an informed caller influence?	Authorised workflow test and exception log
Privacy	Which actual information and people are involved?	Institution-specific scope and risk assessment
Supplier management	Which provider can materially affect data or service recovery?	Permission map, notification route and reconnection criteria
Facilities	Which remote connection can change safe operation?	Equipment owner, settings, alarm path and approved access
Communications	Where will the public find a trusted update if a normal channel fails?	Alternate channel and publication authority

12.5 How Brandefense can help

Brandefense combines Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management. The evidence in this report illustrates why these questions should connect: what is advertised, which owned services are relevant and what the organisation can validate [S50].

A useful evaluation starts with the organisation's own domains, important services and decision owners. Agree which alert would change an action, who will validate it and how closure will be recorded. Avoid treating a high-volume feed as a substitute for an accountable response.

Request a Brandefense demonstration to discuss relevant threat visibility, exposure validation and a workflow matched to your services. The report does not promise that a demonstration establishes an incident or replaces the organisation's legal and operational decisions [S50].

KEY TAKEAWAYS

01

Prioritise current evidence and important services over a fixed calendar.

02

Completion requires validated accounts, tested suppliers and business-accepted recovery.

03

Give every unresolved question an owner, a reason and a review date.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Appendix A. Scope, sources and interpretation · Appendix B. Post evidence register · Appendix C. Sources · Appendix D. Plain-language glossary

86

sources

Appendix A. Scope, sources and interpretation 98

Appendix B. Post evidence register 102

Appendix C. Sources 103

Appendix D. Plain-language glossary 107

Appendix A. Scope, sources and interpretation

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

A.1 Window and dates

The post window is 1 January through 22 November 2026, using publication time. The recent-activity window is 8–22 November. Available source times use UTC. Exposure and post observations were read on 23 November 2026, after the post-date cut-off; passive security-control checks and external source verification completed on 27 November 2026.

A post's date is not its intrusion date, acquisition date or the date represented by a record. A public disclosure can concern earlier activity. The report separately identifies historical enforcement and recovery updates. A current source page can also contain later revisions to an earlier account.

For a global incident, Irish relevance requires evidence of a local service, data or operational connection. A company's headquarters, an Irish customer example or a cloud-region name does not independently establish that connection.

A.2 Source populations

Source category	Contribution	Main boundary
Brandefense Blackhole posts	Retained advertisements, discussion, claims and relayed reporting	A post is not authentication of its contents
Ransompedia	Country-labelled extortion listing records	Listing publication is not independent incident confirmation
Selected-estate portfolio	Defined scope for exposure and passive security-control observations	Purposive entries, overlapping ownership and unavailable HTTP or TLS responses
Original organisations and authorities	Particular disclosures, guidance, decisions and investigation accounts	Scope and absence findings remain those of the issuer
Press reporting	Quoted statements, local consequences and corroborating chronology	Distinguish attributed reporting from original organisation confirmation
Technical records	Vulnerability and control definitions	Applicability is not evidence of Irish exploitation

[S1][S2][S3][S4]

The country-tagged post population and retained narrative corpus have different coverage. They cannot be added, and neither is represented as a complete view of Irish cybercrime. Monthly visibility and repeated advertising do not provide an incident trend.

Coverage remains limited by unavailable notices, incomplete archives and unresolved original-source access. On 27 November 2026, NCSC's 2026 advisory index was verified across January through November (94 advisories through 20 November, without Irish victim confirmations). Garda monthly press-release archives could not be fully re-verified for this edition; Garda items cite the dates on which their passages were read. Missing public confirmation is neither proof of fabrication nor proof that no incident occurred.

A.3 Selected estates, exposure associations and passive security controls

The portfolio contains 250 selected primary domain estates. It is not an official top-company ranking or a probability sample. Parent groups, brands and international services can overlap. The unit must remain an estate unless independent organisational identity has been established.

This edition publishes selected-estate signal counts for devices, credentials, documents, current credential listings and similar-domain associations (23 November 2026 snapshot). Related estates and records can overlap. These are not national prevalence estimates. Atlas supplies the national portfolio headline of 45/100 (B). No sector or organisation Atlas ratings are published.

Passive DNS, mail-policy, certificate and web-header checks completed on 27 November 2026 across all 250 estates (242 TLS checked, 8 unavailable; 207 HTTP responses available, 43 unavailable). Unavailable TLS or HTTP responses are not treated as misconfigurations. The Odin passive hygiene index is an analytical composite of these public checks on a 0–100 scale, where higher values indicate weaker hygiene; it is a model, not an Atlas rating [S2].

A.4 Listings and peer comparisons

Ransompedia records are interpreted by listing publication within the stated window. Country and group labels describe the retained source population. A label can require further geographic validation, and more than one record can concern related events or organisations.

Whole-2025 counts remain separate from the partial 2026 window. The comparison does not provide a matched-period growth estimate. Country size, service composition, disclosure and source visibility differ. No national attack probability, political judgement or security-performance ranking is inferred [S3].

The four peer countries are the United Kingdom, Netherlands, Belgium and Denmark. They provide nearby service, financial and digital-infrastructure contexts. The comparison remains descriptive, with separate country populations and no assumed equivalence of exposure.

A.5 Claim dossiers, public disclosures and incident families

The six underground dossiers preserve claims, held evidence, unresolved propositions, alternatives and responses. The ten public-disclosure dossiers preserve the issuer's scope and date types. The two dossier populations are not added to listing or post totals.

The twelve public incident families comprise those ten dossiers, the police social-account incident and the public-authority employee-contact supplier disclosure. A family is an analytical grouping of related notices about one event. It is not a national occurrence count or proof of a common entry route.

Earlier ransomware, higher-education, physical-record and recovery enforcement notices remain outside this family count. One outage with a disputed cause and one early-2026 precautionary IT shutdown at an Irish public body without a confirmed data or attribution finding are also excluded. A newly dated enforcement or recovery publication does not create a new intrusion.

A.6 Evidence cards and relationships

The twelve post cards use public identifiers B01–B12. They distinguish the retained statement, title or reply from an analyst paraphrase. Criminal contacts, personal records and withheld organisational identifiers are not reproduced.

Quoted fragments remain attributed to their authors. A small authentic excerpt can demonstrate an advertisement while leaving the surrounding claim unverified. A secondary repost does not become an original seller demonstration.

Relationship edges identify their evidence type. A listing association is own data; a quoted responsibility claim is press reporting; a bounded organisation statement is an official account. No shared operator, file identity, sale or collaboration is inferred solely from matching text.

A.7 Payment-card scope

These limited, unverified payment-card observations do not measure national card theft, active cards, issuer prevalence or fraud losses [S4].

Post-country and issuer descriptions remain unverified. A visible record does not establish successful authorisation or financial loss. The narrow card population is not added to credential, customer or selected-estate populations.

A.8 Confidence and alternatives

Evidence class	Supported statement	Boundary
Observation	The retained post or record contains the stated material	The underlying allegation can remain false or unresolved
Actor claim	An advertiser or listing asserts access, data or impact	Authenticity and outcome need separate evidence
Official disclosure	The identified issuer supplied the bounded account	The report does not extend its scope or absence findings
Analyst judgement	A stated implication follows conditionally from the evidence	It is not additional confirmation or a probability estimate

Alternative explanations include older information, incorrect geography, supplier-held copies, duplicated advertising and inaccurate claims. No absence of a public notice is treated as proof of safety. No actor nationality or state link is inferred from a language, alias or geographic label.

A.9 Neutrality and safe use

The report takes no position on governments, elections, religion, foreign policy or territorial questions. Northern Ireland and the UK retain their own geographic scope. Actor rhetoric and slurs are omitted where they add no defensive value.

Use this report to assign authorised validation, recovery and reporting tasks. It does not authorise testing advertised credentials, contacting sellers or probing third-party systems. The relevant organisation should act through its own evidence and approved incident process.

Appendix B. Post evidence register

These are twelve evidence cards, not twelve independently confirmed incidents. B05 and B06 describe repeated advertising of one capability. All are sourced to the retained post population [S1].

Card	Date	Venue and alias	Language	Shown in
B01	2026-01	Forum; alias withheld	English	§4.4
B02	2026-02	Forum; alias withheld	English	§4.4
B03	2026-04	Forum; alias withheld	English	§4.5
B04	2026-04	Forum; alias withheld	English	§4.5
B05	2026-11	Forum; alias withheld	English	§4.6
B06	2026-11	Forum; alias withheld	English	§4.6
B07	2026-01	Chat repost; alias withheld	English	§4.6
B08	2026-02	Forum; alias withheld	English	§4.7
B09	2026-04	Forum; alias withheld	English	§4.7
B10	2026-02	Forum; alias withheld	English	§4.7
B11	2026-09	Forum; alias withheld	English	§4.7
B12	2026-02	Monitoring relay; alias withheld	English	§4.7

Appendix C. Sources

"Verified on" records when the supporting passage or retained observation was checked. An accessible publisher root does not substantiate an anonymous incident by itself. Where an identifying article address is withheld, the underlying passage is retained privately and the source entry says so.

A withheld organisation's own domain is omitted. Publisher roots appear only for press or official issuers when naming the outlet does not identify or localise the organisation. Each entry records the date on which its supporting passage was read.

S1: Odin by Brandefense · Retained Ireland-associated post observations. Own observations held; private source mapping retained. Verified on 23 November 2026. Posts by publication time; claim outcomes unverified.

S2: Odin by Brandefense · Selected-estate portfolio, national Atlas headline, exposure and passive security-control snapshot. Own observations held; private source mapping retained. Verified on 27 November 2026. Selected domain estates and overlapping record associations (23 November 2026); passive DNS, mail, certificate and web-header checks (27 November 2026); national Atlas rating only; device figures are minimum observed counts.

S3: Odin by Brandefense · Ransompedia listing snapshot. Own observations held; private source mapping retained. Verified on 23 November 2026. Country-labelled publication claims; outcomes unverified.

S4: Odin by Brandefense · Narrow payment-card observations. Own observations held; private source mapping retained. Verified on 23 November 2026. Limited unverified observations; not national card theft or fraud losses.

S5: Central Statistics Office · Digital public-service interactions, 2025 baseline published February 2026. Source. Verified on 27 November 2026. Supporting passage read.

S6: Central Statistics Office · Internet-banking use, 2025 baseline. Source. Verified on 27 November 2026. Supporting passage read.

S7: NCSC Ireland · NIS2 transposition and existing operator regime. Source. Verified on 27 November 2026. Supporting passage read. Page still dated last updated 24 June 2025 with NIS2 portals unavailable; not a commencement certificate.

S8: Data Protection Commission · Personal-data breach notification guidance. Source. Verified on 27 November 2026. Supporting passage read.

S9: Central Bank of Ireland · DORA applicability overview. Source. Verified on 27 November 2026. Supporting passage read.

S10: Central Bank of Ireland · DORA incident reporting arrangements. Source. Verified on 27 November 2026. Supporting passage read.

S11: European Union · DORA incident reporting, Delegated Regulation 2025/301, Article 5. Source. Verified on 23 November 2026. Supporting passage read.

S12: European Union · GDPR, Articles 33 and 34. Source. Verified on 23 November 2026. Supporting passage read.

S13: NCSC Ireland · Remote refrigeration-controller security advice, 3 November 2026. Source. Verified on 27 November 2026. Supporting passage read.

S14: NCSC Ireland · Refrigeration-controller follow-up, 13 November 2026. Source. Verified on 27 November 2026. Supporting passage read. Separate research does not establish the Irish incident access route.

S15: NCSC Ireland · PHP vulnerability guidance, 20 November 2026. Source. Verified on 27 November 2026. Supporting passage read.

S16: PHP project · Session-file write security advisory. Source. Verified on 27 November 2026. Supporting passage read.

S17: PHP project · Unread request-body security advisory. Source. Verified on 27 November 2026. Supporting passage read.

S18: NVD · CVE-2026-126714 record. Source. Verified on 27 November 2026. NVD record read. NVD status Awaiting Analysis; CNA record and PHP 8.2.36/8.3.37/8.4.28/8.5.13 releases (19 November 2026) confirmed.

S19: NVD · CVE-2026-129289 record. Source. Verified on 27 November 2026. NVD record read. NVD status Awaiting Analysis; CNA record and PHP 8.2.36/8.3.37/8.4.28/8.5.13 releases (19 November 2026) confirmed.

S20: Stryker · Company network-disruption chronology, March–April 2026. Source. Verified on 27 November 2026. Supporting passage read. Global company statement; changing assessment preserved.

S21: RTÉ · Irish manufacturing impact in wider cyber reporting. Source. Verified on 27 November 2026. Supporting passage read. Irish operational nexus; supporting passage verified.

S22: Boston Scientific · Company update on August incident, 22 September 2026. Source. Verified on 27 November 2026. Supporting passage read. System-specific absence findings remain bounded.

S23: Ireland Live · Local manufacturing-workforce effects, September 2026. Source. Verified on 23 November 2026. Supporting passage read. Irish operating impact reported; no local data-loss total.

S24: Munster Technological University · University statement on learning-platform supplier incident, 8 May 2026. Source. Verified on 27 November 2026. Supporting passage read.

S25: Irish Examiner · Learning-platform supplier and Irish university scope, 11 May 2026. Source. Verified on 27 November 2026. Supporting passage read. Other institutions mentioned in press are not separately named as victims.

S26: Affected financial institution · Saved-payee supplier incident notice, November 2026. Identifying issuer URL withheld. Verified on 23 November 2026. Official notice read; issuer domain and article address withheld.

S27: RTÉ · Financial-supplier notification chronology, November 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; notifications are not attacks or people.

S28: BleepingComputer · Irish financial-supplier scope and company response, November 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; supporting article read.

S29: Irish Examiner · Financial-service incident and precautionary portal shutdown, November 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; company client update quoted.

S30: The Irish Times · Financial portal restoration and qualified data reporting, November 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; company and press propositions distinguished.

S31: RTÉ · Irish grocery refrigeration impact and Musgrave confirmation, 2 November 2026. Source. Verified on 27 November 2026. Supporting passage read. Musgrave confirmation quoted directly by RTÉ; 13 SuperValu stores and European context.

S32: RTÉ · Disruption, responsibility claims and threat-email reporting, 6 November 2026. Source. Verified on 27 November 2026. Supporting passage read. Vendor-attack claim reported; Irish store involvement not independently established.

S33: The Irish Times · Administrative fulfilment supplier incident, July 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; precise occurrence date not established.

S34: RTÉ · Administrative fulfilment interruption, July 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; supporting corroboration read.

S35: Public-service issuer · Information-service access notice and update, autumn 2026. Identifying issuer URL withheld. Verified on 23 November 2026. Official source read; issuer domain and identifying address withheld.

S36: The Irish Times · Employee business-contact supplier exposure, spring 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; employee business contacts rather than service-user records.

S37: Data Protection Commission · Healthcare ransomware enforcement decision, 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; earlier underlying event.

S38: Data Protection Commission · Physical-record storage enforcement decision, 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; physical and earlier events, not a new network intrusion.

S39: Data Protection Commission · Financial-sector contact-centre enforcement decision, 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; earlier contact-centre events, not a new 2026 occurrence.

S40: Data Protection Commission · Annual Report 2025. Source. Verified on 27 November 2026. Supporting passage read. Statistics concern 2025, not 2026 attacks.

S41: Data Protection Commission · Decisions listing and fine-confirmation explanation. Source. Verified on 27 November 2026. Supporting passage read. A fine imposed is not automatically a collected payment.

S42: NCSC Ireland · Incident reporting and cybercrime distinction. Source. Verified on 27 November 2026. Supporting passage read.

S43: UK NCSC · Recommended authentication methods. Source. Verified on 27 November 2026. Supporting passage read. FIDO2 and code-based methods differ.

S44: RFC Editor · DMARC policy specification. Source. Verified on 27 November 2026. Supporting passage read.

S45: RFC Editor · SPF specification. Source. Verified on 27 November 2026. Supporting passage read.

S46: RFC Editor · DKIM signature specification. Source. Verified on 27 November 2026. Supporting passage read.

S47: RFC Editor · DNS security resource records. Source. Verified on 27 November 2026. Supporting passage read.

S48: RFC Editor · HTTP Strict Transport Security. Source. Verified on 27 November 2026. Supporting passage read.

S49: W3C · Content Security Policy. Source. Verified on 23 November 2026. Supporting passage read.

S50: Brandefense · Platform capabilities and demonstration. Source. Verified on 27 November 2026. Supporting passage read.

S51: Irish press · Higher-education email-forwarding retrospective, 2026. (article URL withheld; publisher withheld because it would localise the organisation). Verified on 23 November 2026. Supporting passage read. Underlying activity predates the 2026 window.

S52: Public-service issuer · Recovery updates concerning a late-2025 incident. Identifying issuer URL withheld. Verified on 23 November 2026. Issuer domain and article address withheld; original access remained limited.

S53: Irish regional press · Hospitality booking-provider disclosure, November 2026. (article URL withheld; publisher withheld because it would localise the organisation). Verified on 23 November 2026. Supporting passage read. Property statement quoted by the press; no final guest total.

S54: The Irish Times · Externally managed healthcare publishing service, spring 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; detection earlier in the year than publication.

S55: Irish press · Service outage with disputed cause, 2026. (article URL withheld; publisher withheld to avoid identifying the organisation). Verified on 23 November 2026. Supporting passage read. Organisation denies cyber cause; not a confirmed attack.

S56: RTÉ · Financial-service third-party information disclosures, 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; individual country and event boundaries remain qualified.

S57: An Garda Síochána · Official X-account update, 15 October 2026. Source. Verified on 23 November 2026. Supporting passage read. Official account access only; no operational-network inference.

S58: The Irish Times · Garda response to emailed school threats, 11 November 2026. Source. Verified on 27 November 2026. Supporting passage read. Threat messages, not established network intrusion.

S59: Central Bank of Ireland · Resident-provider payment-fraud statistics, published September 2026. Source. Verified on 27 November 2026. Supporting passage read. Figures concern reported 2025 payment transactions.

S60: Central Bank of Ireland · Cloned financial-identity impersonation warning, spring 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; abused legitimate firm is not a breached firm.

S61: Central Bank of Ireland · Investment comparison-site impersonation warning, April 2026. Source. Verified on 27 November 2026. Supporting passage read. No criminal site addresses or contacts reproduced.

S62: Central Bank of Ireland · Advance-fee loan impersonation warning, early 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; no criminal contact or abused-firm domain exported.

S63: Central Bank of Ireland · Cloned investment-identity warning, November 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; warning not evidence of legitimate-firm intrusion.

S64: An Garda Síochána · Operation Skein day of action, 24 February 2026. Source. Verified on 23 November 2026. Supporting passage read. Searches are enforcement actions, not victim or attack totals.

S65: An Garda Síochána · International online-fraud action, February 2026. Source. Verified on 23 November 2026. Supporting passage read. Irish investigative role; victim population described is Maltese.

S66: An Garda Síochána · Cross-border online-fraud action, May 2026. Source. Verified on 23 November 2026. Supporting passage read. Arrest jurisdictions remain separate.

S67: An Garda Síochána · University malware investigation update, March 2026. Source. Verified on 23 November 2026. Supporting passage read. Charges and allegations; earlier underlying events; no conviction inferred.

S68: Data Protection Commission · Higher-education enforcement publication, 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; earlier underlying events.

S69: Data Protection Commission · Healthcare physical-record security decision, 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting passage read. Article URL withheld; earlier physical-record events.

S70: NCSC Ireland · Global Axios supply-chain warning, April 2026. Source. Verified on 27 November 2026. Supporting passage read. No Irish downstream victim total established.

S71: NCSC Ireland · Global developer supply-chain warning, March–April 2026. Source. Verified on 27 November 2026. Supporting passage read. Document dated March; index April; no Irish victim count.

S72: Central Bank of Ireland · Financial Stability Review 2026: II, Box B. Source. Verified on 27 November 2026. Supporting passage read. Systemic-risk assessment, not an Irish incident count.

S73: NCSC Ireland · National Cyber Emergency Plan, May 2026. Source. Verified on 27 November 2026. Supporting passage read. Guidance and coordination arrangements; not a new binding reporting duty.

S74: NCSC Ireland · 20 November OpenSSL advisory. Source. Verified on 27 November 2026. Supporting passage read. Application-path restrictions retained; no Irish exploitation established.

S75: NIST NVD · OpenSSL vulnerability record CVE-2026-121481. Source. Verified on 27 November 2026. NVD record read. Status Awaiting Analysis; secondary contributed CVSS v3.1 5.9 Medium distinguished from OpenSSL Low.

S76: Central Bank of Ireland · 19 November Financial Stability Review release. Source. Verified on 27 November 2026. Supporting passage read. Publication date and official resilience assessment.

S77: Irish press · Precautionary IT shutdown report, 2026. (article URL withheld; publisher withheld to avoid identifying the organisation). Verified on 23 November 2026. Supporting press passage read. Body acknowledged a precautionary shutdown; no confirmed data loss.

S78: BleepingComputer · Global services-provider response, July 2026. Source (article URL withheld). Verified on 23 November 2026. Supporting press passage read. Article URL withheld; company response quoted; Irish operational or data nexus not established.

S79: OpenSSL · Official CVE record CVE-2026-121481. Source. Verified on 27 November 2026. Official CVE record read. Updated 25 November 2026; affected ranges and fixed-version boundaries; upstream Low severity; no identified attacker-triggered path.

S80: OpenSSL · Vendor release downloads checked 27 November 2026. Source. Verified on 27 November 2026. Vendor download table read. Listed 4.0.3 and 4.1.0 for the affected branches (3.5.9 LTS unaffected); fixed-version boundaries do not establish availability.

Appendix D. Plain-language glossary

Term	Meaning
Account recovery	The authorised process for restoring a legitimate user's access
Administrative access	Permission to manage a particular application or service; it need not include server control
Advertisement	A published offer or request; not evidence of a completed transaction
Affected population	The people, records or services established as involved; its unit must be stated
Analyst judgement	A reasoned implication that preserves evidence and alternatives
Atlas headline	The single exposure rating for the selected national portfolio; not national prevalence
Awareness time	The time relevant to an organisation's incident or reporting assessment
Beneficiary information	Details saved to identify a payment recipient
Claim	An assertion whose underlying outcome is not independently established
Cloud region	A provider's infrastructure-location label; not the nationality of an account owner
Credential record	Information associated with a login; not necessarily an active account
CSIRT	A computer security incident response team
DDoS	Distributed denial of service, intended to reduce a service's availability
Disclosure	A statement about an incident or information exposure; publication and occurrence dates can differ
DKIM	DomainKeys Identified Mail, a signature linking responsibility for a message to a signing domain [S46]
DMARC	A domain-level mail-authentication policy and reporting mechanism [S44]
DNSSEC	DNS security extensions that support authentication of DNS information [S47]
DORA	The EU Digital Operational Resilience Act for covered financial entities [S9]

Term	Meaning
Estate	The selected domain and its associated service context in this report
Exfiltration	Unauthorised extraction of information; a claimed archive is not proof that this occurred
HSTS	HTTP Strict Transport Security, a browser policy for secure connections [S48]
ICT	Information and communication technology
Incident family	Related notices grouped around one event, without implying a national occurrence count
Listing	A published extortion claim in the stated source population
MFA	Multi-factor authentication; its methods differ in resistance to phishing [S43]
NIS2	The EU network and information security directive; national transposition and commencement require separate verification [S7]
Operational technology	Equipment and controls that affect a physical process
Passive hygiene index	An Odin analytical composite of public email, DNS, TLS and web-header checks (0–100, higher means weaker); not an Atlas rating [S2]
Persona	A public alias; it does not establish a unique person or operational team
Personal-data breach	A security event affecting personal information under the relevant legal definition [S12]
Phishing panel	An advertised interface for impersonation or credential collection; advertising does not establish deployment
Recovery objective	The service owner's required recovery outcome and allowed interruption
Ransomware	Malware associated with extortion, often through encryption; a listing alone does not establish its use
Repost	A repeated or secondary publication; not necessarily independent corroboration
Session	A continuing authenticated interaction that may remain relevant after a password change
SPF	Sender Policy Framework, which authorises sending hosts for covered mail identities [S45]
Supplier scope	The actual provider service, permissions and information involved in an incident

Term	Meaning
Tenant	An organisation's service environment within a shared platform
TLS	Transport Layer Security, used to protect a connection; certificate validity is not application security
Content Security Policy	Browser content restrictions expressed by a web service [S49]

About this report

Odin by Brandefense prepared this English research edition for security leaders, operational teams, fraud owners and organisations responsible for important services. Its purpose is to connect an evidenced proposition with an accountable defensive decision.

Analysis and drafting used AI assistance. Own observations, advertiser claims, public accounts and analyst judgements retain separate labels.

The report does not provide legal advice, a national attack census or an estimate of an individual organisation's likelihood of intrusion. Use the stated source, date, unit and boundary when sharing a finding.

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