BRANDEFENSE COUNTRY REPORT · SWITZERLAND 2026

Brandefense Switzerland Cyber Threat Landscape Report 2026

Identity abuse, supplier incidents and recovery across connected services

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

49 of 250
organisations had a credential listed for sale when checked

5
Case studies separating advertised data from verified incidents

97,000
Permit records, not a count of people

41
group labels in the Swiss ransomware listing snapshot

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Switzerland's digital and threat context	10
03	National exposure: the selected organisation universe	15
04	Dark-web offers and their evidence boundaries	23
05	Targeting examples by sector	38
06	Hacktivism and DDoS	54
07	Threat actors and supported relationships	59
08	The fraud economy: identity, trust and payment	70
09	Banking deep dive	75
10	Regulatory and national response	79
11	Outlook	85
12	Action plan	90
	Appendices	96
A	Appendix A. Scope, sources and confidence	97
B	Appendix B. Evidence register	99
C	Appendix C. Sources	101
D	Appendix D. Glossary	106
	About this report	108

Board and CISO	01 05 11 12
SOC and incident response	04 06 07 12
Identity and infrastructure	03 05 07 12
Fraud and banking	08 09 12
Legal and procurement	05 10 12

About this edition

AI-assisted research and drafting. Criminal claims, official accounts and analyst interpretations remain distinct. Appendix A explains scope and confidence.

Switzerland's evidence supports joint investment in identity controls, supplier notification and tested recovery, while keeping underground advertisements separate from confirmed incidents.

122

Swiss ransomware listings in the reporting window

250

selected organisation candidates across thirteen sectors

48 / 100

national Atlas headline for 247 assessed organisation candidates; higher values mean greater observed exposure

4

decisions with named owners and completion evidence

Contents and reading routes

The report moves from decisions to evidence, then to accountable work. Read the evidence boundary with each figure and case.

Chapter	Question	First reader
1 Executive summary	Which decisions follow from the evidence?	Leadership
2 Digital and security context	Which dependencies shape the Swiss picture?	Leadership
3 Organisation exposure	What can the selected universe establish?	Infrastructure
4 Dark-web evidence	What is offered, and what remains unverified?	Threat intelligence
5 Sector incidents	What did organisations and authorities disclose?	Sector owners
6 Hacktivism and DDoS	What separates announcements from service disruption?	Operations
7 Threat actors	Which relationships and attributions are supported?	Threat intelligence
8 Fraud economy	How are identities and trust used in fraud?	Fraud teams
9 Banking	Which controls need joint financial and security ownership?	Banking and identity
10 Regulatory response	Which reporting duties apply to which events?	Legal and compliance
11 Outlook	Which signals would change the assessment?	Leadership
12 Action plan	Who acts, and what demonstrates completion?	All owners

Leadership route: Chapters 1, 5, 10–12. **Operations route**: Chapters 4, 6–7 and 12. **Identity and fraud route**: Chapters 3, 8–9 and 12.

Observed means that the material or measurement is held. **Claimed** means that a poster or listing asserts something. **Officially reported** means an organisation or authority disclosed it, within the stated scope.

An analyst interpretation connects evidence to a decision. It does not supply missing proof about access, attribution, affected people or losses.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which security decisions does the Switzerland evidence support?

4

decisions with accountable owners and evidence of completion

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

Switzerland's evidence joins identity abuse, supplier incidents and recovery risk. Ransompedia records 122 Swiss listings in the reporting window. Credentials associated with 49 of 250 selected organisations were listed for sale when checked. The national Atlas headline is 48 out of 100 for 247 assessed candidates. Official notices preserve separate uncertainties about service impact and data. Prioritise account validation, supplier notification, independent restoration and communications tied to established facts.

This report combines Brandefense Blackhole post evidence, Ransompedia listings, Atlas exposure observations and passive checks with source-checked public reporting. Each population answers a different question. Neither posts nor listings count verified intrusions, and the selected organisations do not represent national prevalence [S1][S2][S3].

1. Extortion listings support continuity planning across sectors. The Swiss total is 122 listings in the stated 2026 window, compared with 50 in all of 2025. The comparison uses unequal periods and does not measure an attack rate. AKIRA accounts for 13 listings, while The Gentlemen and Qilin each account for 9. The remaining listings are spread across many other group labels. A listing does not independently establish encryption, data theft or payment [S2].

The regional snapshot records 457 listings for Germany, 295 for France, 286 for Italy and 61 for Austria. Those larger and smaller populations have different disclosure and observation coverage. They provide context for recovery planning, rather than a ranking of country security [S2].

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

2. Official reporting places identity abuse beside ransomware. The Federal Office for Cyber Security records 27,128 voluntary reports and 200 mandatory notifications in first-half 2026, compared with 29,006 voluntary and 145 mandatory notifications in second-half 2025 [S5][S107]. Its first-half 2025 report recorded 35,727 cyberincident reports under one headline total and 57 ransomware reports, whereas first-half 2026 recorded 79 reported and observed ransomware cases [S5][S108]. These authority populations have period-specific definitions and must not be added to this report's post or listing totals [S5][S107][S108].

The office highlights cloud-account phishing and impersonation of managers or helpdesks. A realistic message can persuade a user to reveal a password, approve a sign-in or install software. The practical control is to verify authority through a separate trusted channel, then investigate sessions and recovery settings when abuse is suspected [S5].

3. Supplier incidents require both technical and notification decisions. An organisation may depend on a processor for pension, health, media, customer or personnel workflows. Its first reliable information can therefore arrive from a provider. The controller still needs to identify its own data, affected processes and reporting duties. Chapter 5 preserves each official notice's uncertainty about what was accessed or removed.

A provider's investigation should not delay a customer's initial risk assessment. Equally, an attacker advertisement should not become the organisation's public account of an incident. Preserve the notice, establish the affected service, and identify what evidence supports each statement about data.

4. The recent canton disclosure distinguishes records from people. The 20 November notice describes approximately 97,000 records in an administrative application. Repeated permits or extensions mean that the record count is not the number of people affected. The same notice describes isolation of the platform and continued processing through alternative forms. This is a service and data-management case, not a basis for a broader count of affected residents [S16].

5. External identity observations require account validation. The assessed portfolio records at least 172,240 device associations and 11,072,599 historical credential associations. Credentials associated with 49 of 250 selected organisations were listed for sale when checked. Observations cover 247 candidates; 3 have no exposure result. None of these populations counts confirmed intrusions or unique people. Validate current accounts, relevant activity and previous remediation before disruptive action [S3].

6. Reporting clocks require a prepared decision tree. Critical-infrastructure notifications, personal-data notifications and financial supervision have different triggers and deadlines. A single generic notification checklist can miss those differences. The legal and incident teams should decide which duties may run together before a real event forces that discussion [S6][S7][S8].

Four decisions for leaders

1. **Validate identity signals against real activity.** Assign identity operations to match new offers and phishing alerts to active accounts, sessions and recovery changes. Preserve evidence before resetting access. Escalate corroborated unauthorised use through the incident process.
1. **Exercise notification with essential suppliers.** Procurement, service owners and legal should rehearse an initial provider alert. Confirm which data and workflows depend on the provider, who can preserve records, and who starts each reporting assessment.
1. **Restore an essential service independently.** Give continuity and infrastructure teams a restoration test using protected backups and separate recovery credentials. Require business validation of the recovered service and its data, alongside the technical restoration result.
1. **Separate claim handling from public incident communications.** Assign a communications lead, an evidence owner and an alternate service-status channel. Record what is claimed, what service impact is observed, and what the organisation can establish about data.

The year in numbers

The figures describe separate populations. An unavailable measure is not a zero.

122

Swiss ransomware listings in the reporting window [S2]

WHAT IT IS NOT

Verified intrusions, unique victims or national prevalence

50

Swiss listings dated in all of 2025 in the same snapshot [S2]

WHAT IT IS NOT

A matched-duration baseline

250

Selected organisation candidates across thirteen sector cells [S3]

WHAT IT IS NOT

An official ranking or a representative national sample

49 of 250

Selected organisations with a credential listed for sale when checked [S3]

WHAT IT IS NOT

Validated accounts, completed sales or confirmed intrusions

48 / 100

National Atlas headline for 247 assessed candidates [S3]

WHAT IT IS NOT

National prevalence or a sector rating

60,475

Distinct retained posts used in this edition [S1]

WHAT IT IS NOT

The full universe of Swiss cybercrime or unique incidents

27,128

Voluntary reports received by the federal cyber office in the first half of 2026 [S5]

WHAT IT IS NOT

Confirmed attacks or a measure comparable to underground posts

200

Mandatory notifications in that authority's first-half account [S5]

WHAT IT IS NOT

A complete count of every Swiss cyber incident

79

Swiss ransomware cases in the authority's first-half reporting and observation [S5]

WHAT IT IS NOT

A subset that can be joined directly to the 122 listings

97,000

Approximate application records in the November canton notice [S16]

WHAT IT IS NOT

The number of distinct people or confirmed theft of every attachment

KEY TAKEAWAYS

01

Keep advertisements, listings and official disclosures in separate decision tracks.

02

Validate identity and supplier evidence before describing an incident's scope.

03

Require demonstrable recovery and a rehearsed reporting decision tree.

Report map

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

Board and CISO	Which risks justify investment now?	01 05 11 12
SOC and incident response	When does an external claim require investigation?	04 06 07 12
Identity and infrastructure	Which access paths and dependencies need validation?	03 05 07 12
Fraud and banking	Which personal facts should never authorise a transaction?	08 09 12
Legal and procurement	Who must notify whom, and under which instrument?	05 10 12

Evidence track	What it answers	Boundary
Underground posts	What people advertise, request or announce	Authenticity and outcomes need separate proof
Ransomware listings	What appears in the retained listing snapshot	Listing dates can differ from intrusion dates
Passive observations	What public-facing configurations show	No proof of intrusion or control effectiveness
Official disclosures	What an organisation or authority reports	Estimates and investigations can change
Official threat assessments	Which threats an authority assesses	Its attribution remains its own assessment

CHAPTER 02

Switzerland's digital and threat context

02

THIS CHAPTER ANSWERS

Which features of Switzerland shape the threats that leaders should prepare for?

3

distinct settings: sensitive information, shared services and public events

2.1 Information value matters more than a country label 11
2.2 Espionage assessments need a named attributor 12
2.3 Shared services can connect otherwise separate incidents 13
2.4 Hosting location does not establish operator nationality 13
2.5 International events are a continuity planning context 13
2.6 Reporting changes what can be counted 14

CHAPTER 02

Switzerland's digital and threat context

IN SHORT

Switzerland combines international organisations, research institutions, financial services and shared digital infrastructure. The Federal Intelligence Service identifies these settings as intelligence targets, while cyber reporting duties cover designated critical services. International events also create occasions for availability claims. These are different problems with different evidence requirements. Identify the information, supplier and service dependencies that matter to your organisation before choosing controls.

2.1 Information value matters more than a country label

The national setting creates several distinct reasons for targeting. The Federal Intelligence Service's 2026 assessment identifies government, international organisations, diplomatic institutions, internationally active companies, universities and research institutes among the country's intelligence targets [S9]. This is the FIS assessment. It does not establish that every organisation in those categories suffered an incident during the report window.

For a security leader, the useful question is which information would retain value after access was lost. Negotiating positions, research findings, customer relationships and operational designs can require different protection. A generic country alert does not answer that question. The information owner must identify the sensitive work and who can reach it.

The FIS describes particular interest in foreign, trade and security policy, military capabilities, the armaments industry and advanced research [S9]. Its list concerns intelligence priorities. A seller's advertisement for customer data is a separate proposition, even where the same sector appears. Neither population can be used to estimate the other.

This distinction changes the response. A customer-data claim calls for evidence preservation, record validation and fraud preparation. Suspected access to sensitive research also calls for review of collaboration accounts, project repositories and external sharing. Both require verification of the affected system and access period. The country label alone does not establish either.

The table connects national context to an internal question, rather than assigning a threat score to a sector.

Setting	Source assessment	Internal question	Accountable owner
Government and diplomacy	FIS identifies political information as an intelligence objective [S9]	Who can read sensitive briefing material remotely?	Information owner and identity team
Universities and research	FIS identifies scientific institutions and advanced technology [S9]	Which external collaborators retain access after a project ends?	Research leadership and IT
International businesses	FIS includes internationally active companies among intelligence targets [S9]	Which commercial decisions depend on confidential information?	Business leadership and security
Shared digital services	FIS identifies telecommunications and IT suppliers as possible access routes [S9]	Which supplier can reach several critical services?	Procurement and service owners

2.2 Espionage assessments need a named attributor

The federal 2026 assessment summary identifies Russian and Chinese intelligence services as the principal espionage threat in Switzerland, alongside FIS-described state cyber threats from Russia, China, Iran and North Korea [S9][S110]. In that official assessment, Russian activity is linked to political, diplomatic and critical-infrastructure pressure, while Chinese activity is also linked to technology, economic and research collection [S9] [S110]. Those attributions belong to the federal authorities; this report does not assign a country of origin to an unverified data offer or website disruption.

The same assessment identifies several access patterns: exploitation of internet-facing network equipment, tailored phishing and contact through messaging applications [S9]. It says known vulnerabilities in outdated software are used more often than previously unknown vulnerabilities. This supports an operational priority for asset ownership, supported software and prompt remediation. It does not identify the entry route in an individual Swiss incident.

Research and development require particular attention because the information can remain valuable over a long period. The FIS includes both academic work and private-sector research within its assessment [S9]. A response plan should therefore cover persistent access and inappropriate sharing, alongside obvious service outages.

A practical review starts with the systems that carry sensitive work across organisational boundaries. Assign an owner to remote access, external identities, shared repositories and supplier support channels. Ask for evidence that access ends when the business relationship ends. Treat this as control validation, not as a claim that those systems were attacked.

2.3 Shared services can connect otherwise separate incidents

Supplier dependence joins business processes that appear separate on an organisation chart. The FIS identifies IT service providers as important access routes and describes telecommunications providers as both intelligence targets and potential routes to customers [S9]. FINMA also emphasises institution-specific cyber scenarios and third-party dependencies [S61].

A supplier incident can create several consequences at once. Staff may lose access to a service while customer information remains available elsewhere. Recovery may depend on the supplier's identity service, support staff or subcontractor. Whether data was accessed remains a separate question from whether the service stopped working.

This is why the service inventory should record more than the supplier's name. It should link the service to a business process, sensitive information, alternative working arrangements and an incident contact. The completion evidence is a tested dependency record. A contract saying that the provider handles security is insufficient evidence of recoverability.

For financial institutions, accountability also remains with the supervised institution. FINMA's guidance states that responsibility for supervisory requirements cannot be transferred to a service provider [S8]. Chapter 10 explains how the reporting clock can begin when an outsourced provider identifies an incident.

2.4 Hosting location does not establish operator nationality

The FIS describes the use of Swiss server infrastructure through resellers and intermediaries in operations against targets abroad [S9]. It also explains that actors change infrastructure and use several intermediate systems. A server's Swiss location therefore does not establish a Swiss operator, Swiss victim or Swiss state involvement.

For hosting and cloud providers, the decision is operational. Preserve tenancy and administrative records when a credible incident requires investigation. Ensure that the service can identify the relevant customer relationship and respond through established legal and security channels. Avoid treating every customer on shared infrastructure as connected to the activity.

For other organisations, the lesson concerns attribution. Network location can support investigation, but it cannot establish who directed an operation. A language, hosting country or claimed political motive should remain a separately labelled observation. An actor relationship needs evidence of that relationship, rather than a shared country reference.

2.5 International events are a continuity planning context

The June 2024 Summit on Peace in Ukraine is relevant historical context, outside this report's incident window. In its initial review, the NCSC attributed DDoS activity around the summit to NoName057(16) [S42]. It reported minor disruption to infrastructure. It also said the summit's systems and data, and those of its organisers, were not threatened.

The source distinguishes several phenomena. It reported attempted digital intrusions and phishing separately from DDoS. It said the broadcast problems and a power outage were not cybersecurity incidents [S42]. That distinction matters whenever technical disruption occurs during a highly visible event.

The historical account supports preparation for public-service interruption around major events. It does not establish that a similar campaign happened in 2026. The FIS separately assesses overload attacks around international conferences and major events as highly likely [S9]. That is a source assessment, rather than a report-specific forecast or a position on the event.

Use the event calendar to rehearse service continuity, provider escalation and public statements. A statement should distinguish an actor's claim, the service impact that the organisation observed, and what remains unknown. Do not infer data access from a website outage. Do not infer a political cause from timing alone.

2.6 Reporting changes what can be counted

The critical-infrastructure reporting obligation started on 1 April 2025 [S60]. In its semi-annual reports, BACS recorded 35,727 combined cyberincident reports in first-half 2025, then separated 29,006 voluntary and 145 mandatory notifications in second-half 2025 and 27,128 and 200 in first-half 2026 [S5][S107][S108]. A year-on-year comparison must reconcile that terminology change and the April 2025 start of mandatory reporting before interpreting trend direction [S60][S107][S108]. Reports under that duty cannot be equated with dark-web posts, ransomware listings or all incidents experienced by Swiss organisations.

The report's separate evidence populations should guide decisions without being combined into a national total. Public warnings can identify a campaign pattern. An extortion listing records a claim. Exposure associations and passive configurations describe different observations. Each needs its own validation and owner.

No statement about banking confidentiality or foreign relations is needed to turn those observations into a causal explanation. The relevant questions are whose information was involved, which service was affected, and what the evidence supports. Chapter 10 turns the different reporting duties into an incident decision record.

KEY TAKEAWAYS

01

Attribute national intelligence assessments to the FIS and keep them separate from individual incident claims.

02

Shared services connect business impact, recovery and reporting duties; test those dependencies with the supplier.

03

The 2024 summit account is historical context; event timing and website interruption do not establish data access.

CHAPTER 03

National exposure: the selected organisation universe

03

THIS CHAPTER ANSWERS

Which identity observations need validation across the selected organisations?

49 of 250

organisations had a credential listed for sale when checked

3.1 Universe card 16

3.2 Passive observations and their limits 17

3.3 Current listings and the national Atlas headline 19

3.4 Device, credential and document observations 20

3.5 Turning an external signal into a defensible decision 22

CHAPTER 03

National exposure: the selected organisation universe

IN SHORT

49 of 250 selected organisations had a credential listed for sale when checked. Exposure observations cover 247 candidates; 3 remain unassessed. The national Atlas headline is 48 out of 100 for that assessed portfolio. Device and historical credential associations can concern customers, employees or older material. Passive configuration has a separate denominator. Validate current listings, investigate relevant employee-device evidence, and check intended mail and web controls.

3.1 Universe card

Selection and measurement are separate. Inclusion identifies a candidate for assessment; it does not establish exposure, a current incident or an independently operated corporate group [S3].

Item	Definition
Selected universe	250 organisation candidates with a principal public domain
Selection basis	Public authorities, official financial and education directories, and prominent sector organisations
Purpose	Describe selected external signals and support questions for service owners
Coverage	Thirteen sector cells
Organisation boundary	Some separately operated subsidiaries share a corporate parent
Time basis	Exposure read 21–22 November 2026; passive observations have their own snapshot date
Public results	Sector signal counts and the national Atlas headline; individual organisations withheld
Inference limit	No national prevalence estimate, security ranking or certification of individual controls

The sector table describes the selected universe. These cells are analytical groupings and do not determine whether an organisation has a legal critical-infrastructure reporting duty.

Sector	Candidates	Defensive question
Banking and finance	40	Can identity, fraud and payment teams validate the same event?

Sector	Candidates	Defensive question
Public administration	35	Can a service continue while an application is isolated?
Education and research	25	Who can export research or identity records through shared services?
Healthcare	20	Can clinical workflows continue during restoration?
Energy and utilities	20	Which business dependencies can affect essential operations?
Transport and logistics	20	Can customer and operating workflows recover separately?
Industrials and construction	21	Are supplier access and production dependencies understood?
Telecoms and technology	15	Who can reset identities or publish trusted communications?
Life sciences and chemicals	15	Which partners handle research and personnel information?
Retail, food and agriculture	15	Which customer and supplier accounts authorise transactions?
Consumer media and property	9	Which outsourced platforms hold customer information?
Trade and business services	5	Which shared services support critical transactions?
Insurance	10	Can claim and pension records be traced to each processor?
Total	250	A purposive selection, with different institutional boundaries

3.2 Passive observations and their limits

The passive snapshot covers 246 of the 250 selected candidate domains, omitting one candidate each in banking and finance, public administration, education and research, and healthcare. These four omissions do not overlap with the three unassessed candidates in the 247-organisation exposure population, leaving 243 candidates assessed in both checks. Inconclusive responses are not treated as a control failure [S3].

Observation	Count	Denominator
Assessed candidate domains	246	246
DMARC reject or quarantine policy observed	164	246

Observation	Count	Denominator
SPF observed	233	246
DKIM records observed	168	246
DNSSEC delegation record observed	69	246
TLS certificate check valid	243	246
TLS certificate validation unsuccessful	2	246
TLS check unresolved	1	246
Response recorded	216	246
HSTS observed	182	216

The mail-policy observation records a published policy, rather than measured rejection of every fraudulent message. The presence of a DKIM record does not establish signing on every legitimate mail stream. HSTS findings use the response denominator.

A policy observation is a question for the service owner. A monitoring-only mail policy can be intentional while legitimate senders are being assessed. A missing observation can also result from an inconclusive response. Neither establishes that an attacker used that condition.

For mail authentication, the important operational outcome is whether legitimate services send aligned mail and whether receivers can enforce the organisation's intended policy. Publishing a policy alone does not establish those outcomes. An owner should check delivery reports and approved sending services before changing enforcement.

A DNS delegation observation describes the trust information visible for that domain. It does not audit every resolver, every record or the organisation's internal name service. Similarly, a valid TLS certificate establishes a limited transport-security observation. It does not assess application authorisation, recovery controls or protection of stored customer data.

Header observations have a narrower scope still. A header seen on one response might differ on another application, hostname or route. The appropriate response is to check policy consistency across the services that matter, then validate the user experience after a change.

Passive observations describe configuration across explicit sector denominators

	DMARC	SPF	DKIM	DNSSEC	TLS	HSTS
Banking and finance	25/39	38/39	19/39	21/39	39/39	34/35
Public administration	20/34	30/34	12/34	6/34	33/34	24/30
Education & research	9/24	23/24	21/24	11/24	24/24	16/23
Healthcare	11/19	17/19	11/19	3/19	19/19	14/19
Energy and utilities	15/20	19/20	18/20	0/20	20/20	17/19
Transport and logistics	13/20	19/20	15/20	9/20	19/20	15/17
Telecoms & technology	15/15	15/15	11/15	4/15	15/15	11/14
Life sciences & chemicals	10/15	14/15	13/15	2/15	15/15	9/13
Industrials & construction	17/21	21/21	16/21	5/21	21/21	16/18
Insurance	8/10	10/10	7/10	3/10	10/10	8/8
Retail food & agriculture	12/15	14/15	13/15	2/15	14/15	9/10
Business and consumer services	9/14	13/14	12/14	3/14	14/14	9/10

Source: passive observations, 22 November 2026. Each cell shows observed/assessed domains; HSTS uses recorded responses. Published policies do not establish enforcement for every message [S3].

3.3 Current listings and the national Atlas headline

49 of 250 selected organisations had a credential listed for sale when checked. Exposure observations cover 247 candidates; the 3 unassessed candidates (one each in energy and utilities, transport and logistics, and business and consumer services) all appear in the 246-domain passive snapshot. The national Atlas headline is 48 out of 100 for the assessed portfolio [S3].

Higher Atlas values mean greater observed exposure. The headline describes the selected portfolio, rather than national prevalence or a confirmed incident count. This report publishes only that national Atlas figure. The sector table reports signal counts, with each assessed population visible.

The exposure and passive tables group business and consumer services together. The universe card retains the original selection sectors.

Sector	Assessed	Current listings	Employee-device orgs	Document orgs	Device orgs
Banking and finance	40	7	15	19	36
Public administration	35	4	20	26	29

Sector	Assessed	Current listings	Employee-device orgs	Document orgs	Device orgs
Education and research	25	6	23	24	25
Healthcare	20	0	10	6	14
Energy and utilities	19	1	10	8	15
Transport and logistics	19	7	14	10	17
Telecoms and technology	15	6	13	13	15
Life sciences and chemicals	15	2	12	10	12
Industrials and construction	21	4	16	16	18
Insurance	10	3	7	8	10
Retail, food and agriculture	15	6	10	9	14
Business and consumer services	13	3	8	9	10
All assessed	247	49	158	158	215

A current listing means that a credential associated with the domain was advertised when checked. It does not establish account validity, a completed sale or access to the organisation's internal systems. Preserve the offer and validate the account through the organisation's authorised records.

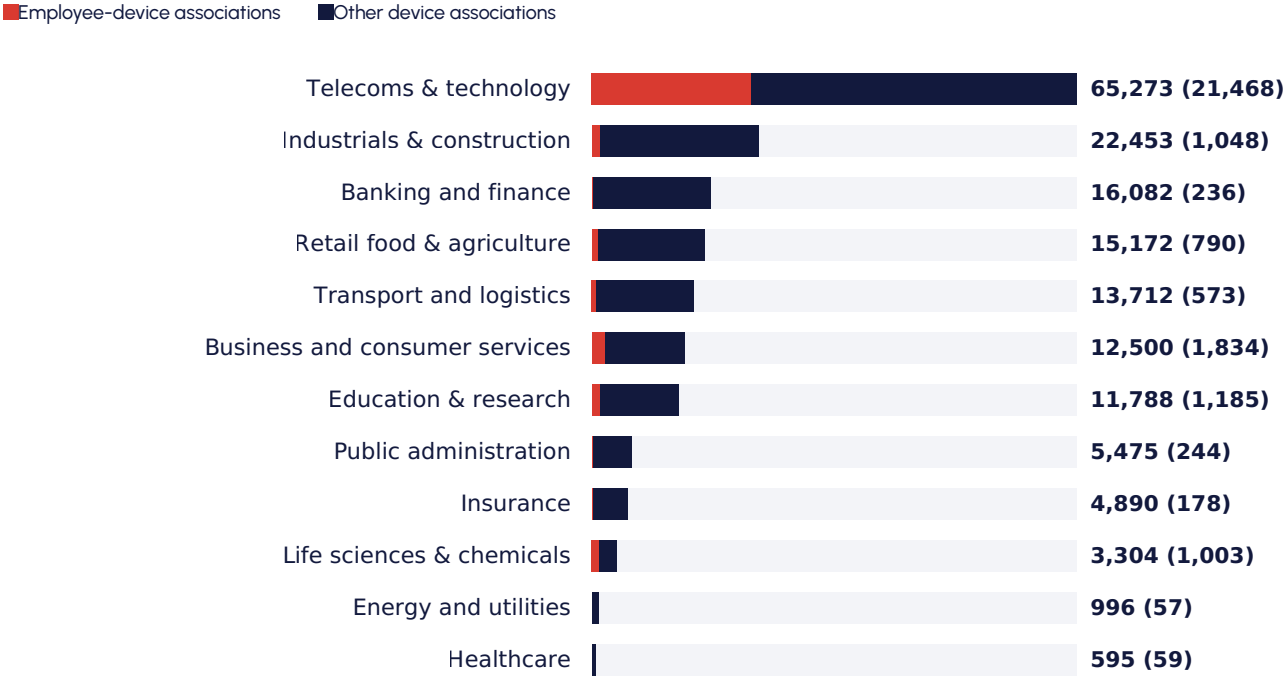
3.4 Device, credential and document observations

The exposure snapshot was read on 21–22 November 2026. Device and credential totals describe records held at that time, including older material. Mention observations cover the preceding 365 days; lookalike observations cover 30 days [S3].

Observation	Count	Assessed organisations
Device associations, at least	172,240	247
Employee-classified device associations	28,675	247
Other device associations	143,565	247
Historical credential associations	11,072,599	247

Observation	Count	Assessed organisations
Breach-database records	4,102,097	247
Stealer-log lines	2,216,250	247
Combolist entries	4,754,252	247
Lookalike-domain observations	109,410	247
Document observations	2,696	247

Device and credential associations across assessed sector populations



Source: exposure observations for 247 assessed organisation candidates, 21-22 November 2026. Cumulative associations, not verified intrusions [S3].

Some device totals are lower bounds. These are associations across selected domains, not distinct Swiss people or employees. One device or credential can be associated with several organisations. Records may be repeated, obsolete or already remediated.

Employee-classified associations require validation against current accounts and managed devices. Associations outside that classification do not establish who owns the device. Education and customer-service domains can include students, customers and other authorised users.

Similar domain names do not independently establish phishing or malicious intent. Document observations require a separate check of ownership, accessibility and sensitivity. Keep those reviews separate from account containment.

3.5 Turning an external signal into a defensible decision

Identity operations should establish whether the account or service belongs to the organisation, whether it remains active, and whether earlier remediation addressed the same evidence. Threat intelligence should preserve the advertisement separately from internal findings.

Assess relevant activity, including sessions, recovery changes, application grants and mailbox rules. Describe an absence of matching telemetry with its retention and coverage limits. A historical password already retired may justify closure; an unauthorised session may require revocation and incident escalation.

A bank-domain association can concern a customer, employee, supplier or historical record. Chapter 9 keeps the full banking cell separate from the issuer-matched subset. Neither population establishes a banking compromise rate.

Record the owner, observed facts, uncertainty, action and reopening condition. Ask the business owner to demonstrate continuity if a service must be isolated. Account validation, configuration assurance and recovery each require their own completion evidence.

KEY TAKEAWAYS

01

Validate current listings against active accounts and relevant behaviour.

02

Keep cumulative associations separate from people and current incidents.

03

Read exposure and passive results with their different assessed denominators.

CHAPTER 04

Dark-web offers and their evidence boundaries

04

THIS CHAPTER ANSWERS

What do Swiss-related underground offers establish, and where should defenders seek corroboration?

5

Case studies separating advertised data from verified incidents

4.1 The observation universe 24
4.2 Different products require different responses 27
4.3 Five cases for validation 28
4.4 Credentials, contacts and demand 34
4.5 Recent activity: 9–22 November 36
4.6 Connect the evidence to an accountable decision 37

CHAPTER 04

Dark-web offers and their evidence boundaries

IN SHORT

Swiss-related posts advertise insurance records, customer information, contact lists and account access. Some describe older material, while others are buyer requests or replies quoting a claim. A contractor-themed offer extends the response question to physical security. None of these advertisements, by itself, establishes an intrusion, a completed sale or current access. Validate the source, date, account and business process before choosing containment or communicating an affected-person total.

4.1 The observation universe

A country label does not establish a Swiss victim. Odin by Brandefense counted 59,956 country-tagged posts associated with Switzerland in the stated window. The combined retained material contains 60,475 distinct posts across the report's source populations. These counts describe posts rather than incidents, people or successful transactions. [S1]

The source populations overlap. The combined total is a separate population, so these rows must not be added together. Retained coverage is incomplete where source material was unavailable.

Population	Posts	Meaning
Country-tagged count	59,956	Reported post population in the stated window
Country-tagged material retained	59,953	Material available for this edition
Forum material retained	1,409	Retained Switzerland-related forum material
Recent material retained	1,595	Posts dated 9–22 November
Combined retained material	60,475	Distinct posts across the source populations

The country-tagged platform counts describe where posts appeared. They do not count unique people, criminal groups or successful transactions [S1].

Platform	Posts	Boundary
Telegram	58,805	Post population, not unique participants
Forum	887	Post population, not unique participants
Discord	240	Post population, not unique participants
Paste	24	Post population, not unique participants
Tor	0	Post population, not unique participants

Language labels describe the material. They do not establish an author's citizenship, a buyer's location or an attacker's identity. More than one label may apply to a post [S1].

Language	Labelled posts	Interpretation
English	35,077	A language observation, without attribution
German	585	A language observation, without attribution
French	492	A language observation, without attribution
Italian	95	A language observation, without attribution
Russian	5,835	A language observation, without attribution
Turkish	2,039	A language observation, without attribution

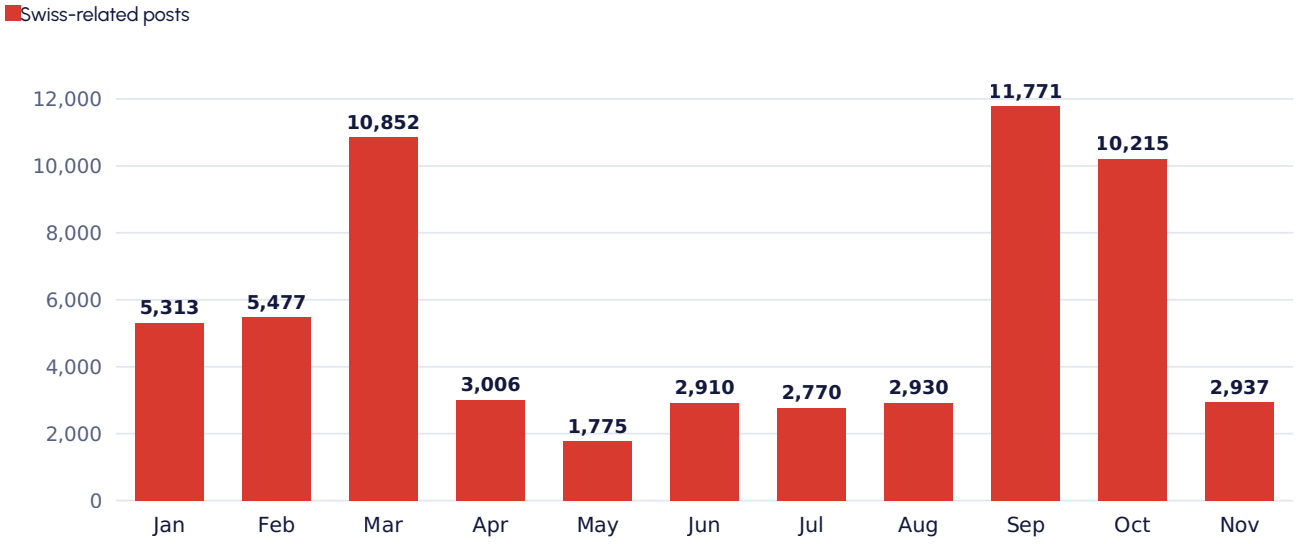
The monthly chart retains the post unit. Automated advertising and repeated material can affect volume. The chart therefore supports evidence review, rather than a conclusion about attack growth.

The distinction matters because Switzerland appears in several kinds of material. A seller can include the country in a global stock list. A buyer can ask for Swiss information without offering anything. A forum reply can repeat an earlier allegation. A post can also describe a service headquartered elsewhere, or an earlier incident involving an internationally operating Swiss brand.

The case studies therefore begin with the proposition that each post actually supports. An advertisement establishes that an offer was observed. A quotation in a reply establishes that the participant repeated the claim. A request for samples establishes an unresolved verification question. None supplies victim-side forensic evidence.

The language of freshness also needs restraint. Seller labels such as "fresh" can describe a newly packaged product, a recent advertisement or an assertion about the underlying records. They do not establish the theft date or the account's current validity. The relevant defensive question is whether the material matches an account, process or dataset still in use.

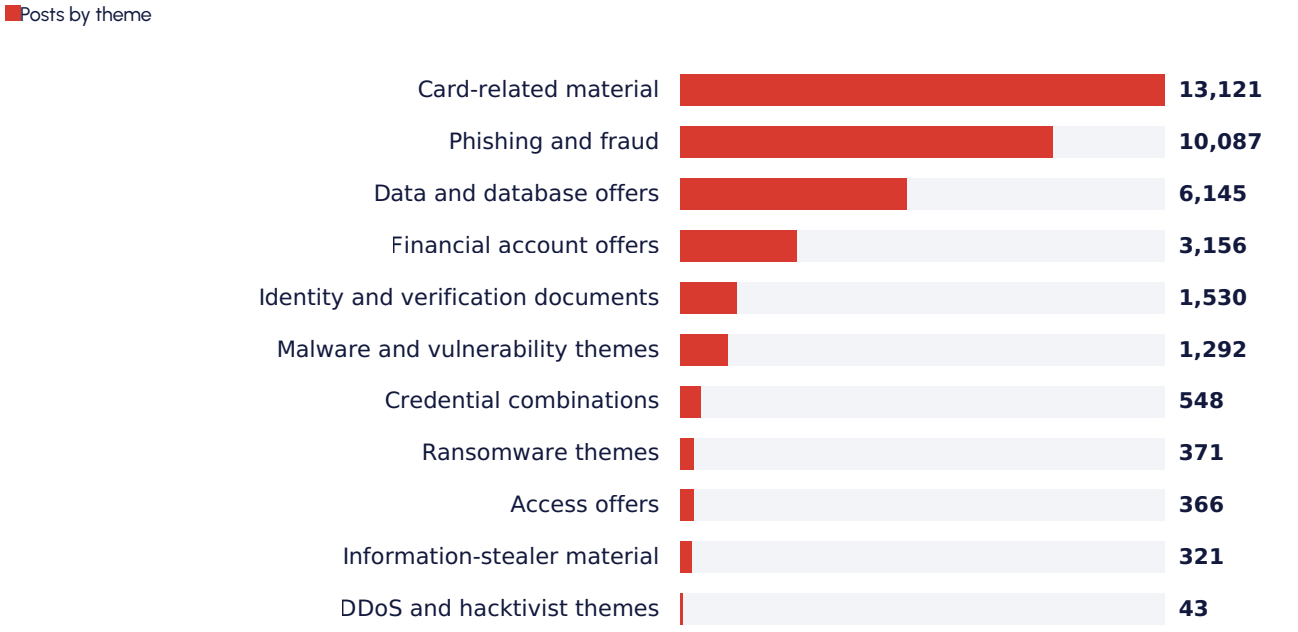
Swiss-related post volume varies without measuring incident frequency



Source: retained Switzerland-related post material, 1 January–22 November 2026 through 07:20 UTC; November partial. Themes can overlap; posts are not confirmed incidents [S1].

Theme counts are overlapping descriptions of retained material. Card-related posts do not measure cards or losses. Use the figure to assign review owners, rather than infer a national fraud market [S1].

Card-related themes are common in the retained post material



Source: retained Switzerland-related post material, 1 January–22 November 2026 through 07:20 UTC; November partial. Themes can overlap; posts are not confirmed incidents [S1].

4.2 Different products require different responses

The following table groups the selected evidence by the response decision it can support. Its rows are examples, not mutually exclusive national crime totals. [S1]

Material	What was observed	Principal limit	First decision
Insurance exports	An offer described contract-related rows and two files	Rows are not unique policy-holders; provenance remains unverified	Reconcile contract fields and authorised exports
Telecommunications records	Replies preserved a large customer-data claim	The quoted allegation and requests for proof do not confirm an incident	Seek provider evidence before using the advertised count
Contractor information	An offer described facility-handling records	Working entry information and present access were not established	Join supplier, cyber and physical-security review
Care workforce data	An offer described staff and business administration data	Patient data, authenticity and current access unverified	Validate workforce and administrative systems separately
Transport business data	An offer described client, payroll and financial records	Origin, age and current access unverified	Check business records and previous remediation
Historical retail material	A later post described an earlier ransomware event	Posting time is not intrusion time	Check previous remediation against the material
Hosted-site exports	An offer alleged a shared cause across several sites	A common technical cause was asserted, not demonstrated	Ask provider and tenants to validate their own systems
Credential combinations	Swiss-labelled email and password material was advertised	Country labels and "fresh" do not establish current validity	Validate accounts through authorised identity processes
Contact information	Posts advertised Swiss-labelled phone or directory segments	Collection origin, age and unique people remain unresolved	Prepare staff for persuasive contact-based impersonation
Buyer requests	Posts sought databases, mailboxes or accounts	Demand is not possession or a completed transaction	Use the demand as context for account protection

The correct response can differ even when the advertised fields overlap. Insurance information calls for contract and customer-service review. Facility-handling information adds a physical-security owner. A historical credential claim calls for a check against earlier remediation before a new reset campaign is considered.

4.3 Five cases for validation

A

CASE A

Insurance records advertised as Swiss

Evidence card B01 | 4 May 2026 | Data-sharing forum | Insurance

Unverified data-sharing claim

CLAIM	A 4 May post described two files as Swiss insurance information. It claimed that one file contained 4,260,757 structured lines relating to contracts, policyholders, vehicles, intermediaries and financial details. [S1]
CHRONOLOGY	The same alias appeared in two retained posts with closely matching wording on 4 May. That supports an observation of repeated advertising language, rather than two independently established incidents.
HELD	The text describes contract-related fields and offers links that are omitted here. The claimed unit is a line in a file. It is not a verified number of policyholders or unique contracts.
ALTERNATIVES	Contract versions, repeated policyholder details and combined administrative exports could account for repeated rows. Repackaged historical information, incorrect labelling or an inaccurate offer also remain possible. The post alone cannot select between these explanations.
LIMITS	This report does not establish the files' contents, provenance, age or authenticity. It does not confirm an intrusion into the insurer, any current access, or a completed transfer to another party.
RESPONSE	Insurance security, privacy and operations teams should compare any authorised alert with their own export schemas and retention records. Confirm the affected business process before issuing a person count or changing customer authentication.

Bottom line

Validate provenance and contract scope before treating an advertised row total as affected people.

A credible-looking field description can help route an investigation. It cannot authenticate the entire file. Validation should establish which system produced the information, which dates it covers and whether the same person or policy appears repeatedly.

Evidence card B01 — 4 May 2026

NormalLeVrai | Data-sharing forum | Forum | English

ORIGINAL

contains 4,260,757 complete lines of structured insurance data [...] information for a contract [...] related to insurance contracts (policies)

Held

An offer describing two files as Swiss insurance information, including a claimed row total and field descriptions.

Not established

The files, the row total, provenance, unique people, current validity, an intrusion date or any completed transfer.

B

CASE B

A telecommunications allegation inside a reply (B02, B03)

Telecommunications

Claim quoted in replies

CLAIM	A 10 March reply quoted an offer attributed to Niphra. The quotation alleged a January 2026 incident at a telecommunications provider and advertised more than 6 million customer details. [S1]
CHRONOLOGY	Another participant asked for samples on the same day. The discussion preserved both the allegation and a demand for supporting evidence. The dates establish the observed discussion, not the alleged intrusion.
HELD	The displayed evidence is a quotation inside a reply and a subsequent challenge. It is weaker than an authenticated original offer, a verified data sample or a statement from the organisation.
ALTERNATIVES	The participant could be repeating a real offer, copying an unsupported allegation or discussing inaccurately labelled material. The request for proof does not establish that the claim is false.
LIMITS	The advertised count, affected fields, origin and date remain unverified. The discussion does not establish current access or an officially confirmed incident. It must not be added to the confirmed cases in Chapter 5.
RESPONSE	Route the claim to the provider's security and privacy contacts through an established channel. Ask for the confirmed scope and customer guidance. Keep internal briefings explicit about which information came from a forum participant.

Bottom line

A request for samples preserves an unresolved evidence gap; it neither confirms nor disproves the offer.

A skeptical reply is evidence of doubt, not a final verdict. Treating a request for samples as disproof would be as unwarranted as treating the quoted allegation as confirmation. Preserve the unresolved question while checking evidence from the responsible organisation.

Evidence card B02 — 10 Mar 2026

john2samira, quoting Niphra | Forum reply quoting an offer | Forum | English

ORIGINAL

Date of breach: January 2026. [...] [telecommunications provider] [...] 6M+ Customer Details [...] please post some rows

Held
A reply preserving an advertised customer-data claim and asking for sample rows.

Not established
An authenticated original seller statement, a verified customer count, file ownership, current access or an incident confirmed by the provider.

Evidence card B03 — 10 Mar 2026

jb75 | Forum discussion | Forum | English

ORIGINAL

Please add a sample. [...] no one can take your word for it if they can't verify the data.

Held
A participant questioned the evidence supporting the telecommunications claim.

Not established
Proof that the claim is false, a technical validation of the purported data, or independent confirmation of the seller.

CASE C

C

Contractor information and physical-security questions

Evidence card B04 | 5 Nov 2026 | Data-sale forum | Business services

Unverified contractor-data offer

CLAIM	A 5 November advertisement described a database from a Swiss business-services provider. It claimed 980,093 structured rows and described facility, collection, logistics and site-handling information. [S1]
CHRONOLOGY	The observed post advertised an exclusive buyer arrangement. It also stated that the advertiser had not verified every row. Neither statement establishes that the advertiser controlled a complete or current dataset.
HELD	The advertisement connects contractor-held business information with several kinds of customer facilities. The post's wording is retained privately. Identifying descriptions, contact details and any purported entry information are omitted from the public card.
ALTERNATIVES	The material could include outdated instructions, duplicate operational records, ordinary delivery information or mischaracterised fields. An authentic administrative export would still require a separate assessment of its current security significance.

LIMITS	The report does not confirm the row total, working entry information, successful entry, a current contractor incident or a sale. Descriptive claims about sensitive customers do not independently establish those customers' involvement.
RESPONSE	Supplier management should establish which handling instructions the contractor holds. Physical security should validate any matched operational detail through its own records. Retire affected instructions when their authenticity and continuing use are established.

Bottom line

Join cyber and physical-security review without assuming that advertised entry information works.

The response should include the owner of the physical process. A cyber team may recognise a customer export while missing that its operational fields are maintained by facilities staff. Equally, a dramatic seller description should not trigger assumptions about successful access to premises.

Evidence card B04 5 Nov 2026

pfavre | Data-sale forum | Forum | English

ORIGINAL

Complete database from a [business-services provider]. [...] 980,093 structured rows [...] we have not manually verified every single row.

Held

An advertisement claiming a contractor dataset with facility-handling information and an asserted row count.

Not established

The data file, current physical access, working entry credentials, the claimed row total or any successful sale.

CASE D

D

Earlier retail material advertised during the window

Evidence card B05 | 11 Oct 2026 | Data-sharing forum | Retail

Earlier material advertised again

CLAIM	An 11 October post advertised information associated with an outdoor retailer. The post itself described a 2025 ransomware event and an earlier estimated incident date. Its historical assertions remain the poster's account. [S1]
CHRONOLOGY	Similar descriptive material appeared in a retained February post under another alias. The October post is therefore a new observation of advertising. It does not establish a new intrusion during October.

HELD	The posts describe similar subject matter and refer to earlier material. Matching descriptions support a relationship between the advertisements' narratives. They do not establish identical files, a transfer between the aliases or a common operator.
ALTERNATIVES	One poster may have copied a description, repackaged older information or obtained material independently. The supplied text cannot resolve these possibilities or authenticate the claimed historical attribution.
LIMITS	The report does not confirm the contents, completeness or historical incident claims. It does not establish that any described credential remains usable. A 2026 post must not become a confirmed 2026 ransomware incident through repetition.
RESPONSE	Compare any matched information with the organisation's previous incident and remediation records. Confirm whether old accounts, secrets, supplier routes or retained exports remain relevant. Reopen a control issue when current evidence justifies it.

Bottom line

A 2026 posting date can describe older material and cannot establish a new intrusion.

Historical information can still create a present protection task. Its defensive value depends on what remains valid, rather than on the date of the latest advertisement. The closure record should distinguish previously remediated material from a newly validated problem.

Evidence card B05 — 11 Oct 2026

updap | Data-sharing forum | Forum | English

ORIGINAL

Today I've uploaded [outdoor retailer] [...] DataCarry attack (2025): [...] The estimated compromise date [...] remains unconfirmed by [outdoor retailer].

Held

A republication that explicitly describes the advertised material as connected to an earlier incident.

Not established

A new 2026 intrusion, the asserted historical attribution, the age or completeness of the files, or unchanged credential validity.

CASE E

E

Hosted-site exports and an asserted common cause

Evidence card B10 | 30 Jan 2026 | Data-sharing forum | Hosted services

Unverified shared-hosting claim

CLAIM	A 30 January post alleged that several Swiss sites shared a database-access configuration. It advertised 92 SQL files and a package described as 45 MB. A separate forum reply repeated the assertion. [S1]
CHRONOLOGY	The retained observations place the offer and its repetition within the reporting window. They do not independently date any underlying intrusion or establish when the files were created.
HELD	The text connects several sites with an asserted common technical explanation. The public card omits the sites, file names and alleged credentials. The claimed file count is not a verified organisation count.
ALTERNATIVES	The advertisement could combine unrelated exports, historical backups or misleading site associations. Shared hosting may explain a relationship without establishing the same fault or the same access across every tenant.
LIMITS	This report does not authenticate the files or the claimed technical cause. It does not confirm that every listed site was affected, that database access remained available or that a common operator produced the material.
RESPONSE	The hosting provider and tenant owners should validate their own access records, administrative interfaces and export history. Keep each tenant's findings separate until the evidence supports a shared cause.

Bottom line

A shared-cause explanation requires provider and tenant evidence rather than matching advertisement text.

A shared-service hypothesis can improve routing without becoming a verified root cause. The provider may own the administrative platform while the customer owns application configuration and data. The investigation needs a named owner on each side and a shared record of established facts.

Evidence card B10 — 30 Jan 2026

hexvior | Data-sharing forum | Forum | English

ORIGINAL

Multiple Swiss Sites [...] Total Package Size: 45 MB [...] 92 .sql files

Held
A claim associating several hosted sites with advertised database exports; a separate reply repeated the claim.

Not established
Successful intrusion, a shared technical cause, file identity, the number of affected organisations or current database access.

4.4 Credentials, contacts and demand

Demand advertisements do not establish successful purchases. A January buyer request sought recent crypto-currency-related databases from Switzerland, Germany and Austria. The post asked for evidence of age and sample lines. It establishes a stated purchasing preference, rather than an identified Swiss exchange incident. [S1]

A separate April advertisement sought Swiss-related mailbox or account material and quoted a payment per validated account. Its Russian and English passages do not describe the requested material in exactly the same way. That inconsistency limits a precise interpretation of the transaction being proposed. No payment or account control was verified. [S1]

Evidence card B06 — 6 Jan 2026

xmrlover76 | Buyer request on a forum | Forum | English

ORIGINAL

interested in purchasing [...] Switzerland Crypto DBs [...] must contain minimum 5k+ lines [...] must be able to provide proof

Held
A demand advertisement naming Switzerland alongside other countries and requesting evidence of data age.

Not established
An offered dataset, a successful purchase, an affected exchange, or a current Swiss intrusion.

Evidence card B11 — 17 Apr 2026

kleinanzeige | Account-buying forum | Forum | Russian and English

ORIGINAL

Почты на других швейцарских доменах и корпы также принимаются ОПЛАТА - 8$ ЗА 1 ВАЛИДНЫЙ АККАУНТ

TRANSLATION

Mailboxes on other Swiss domains and corporate accounts are also accepted. PAYMENT: $8 for one valid account.

Held
A buyer advertisement seeking Swiss-related mailbox or account material and quoting a price.

Not established
A completed transaction, current control of any account, a reliable payout, or agreement between the Russian and English wording in the full post.

Credential-combination posts present another unit problem. A January advertisement labelled a file "Switzerland" and claimed more than 24 thousand email and password lines. Lines can contain duplicates, inactive accounts, reused passwords or incorrect country associations. The seller's freshness label supplies no independent account-validation result. [S1]

The defensive sequence should begin inside the organisation's authorised identity process. Establish whether an account exists, whether previous remediation covered the material and whether there is a current sign-in concern. A disruptive response should follow validated risk rather than an advertised file size.

Evidence card B07 — 27 Jan 2026

thejackal101 | Credential-sharing forum | Forum | English

ORIGINAL

Database: Switzerland [...] Email : Password [...] [24 K++]
Line Status: FRESH | HQ

Held
A Swiss-labelled credential advertisement with a claimed line total and a seller freshness label.

Not established
Unique accounts, usable passwords, Swiss residence, a theft date or a newly affected organisation.

Evidence card B09 — 18 Jan 2026

Cod3xx | Data-sharing forum | Forum | English

ORIGINAL

Country : Switzerland Format : csv [...]

Held
A post advertising a Swiss-labelled contact export and describing its structure.

Not established
How the information was obtained, private-system intrusion, complete records, current access or an affected-person count.

Phone and directory material can support persuasive impersonation without establishing internal network access. A 7 November advertisement labelled one segment "Switzerland-600k" while describing material spanning 2024–2026 and many countries. The same claim appeared under different aliases. Matching wording does not establish file identity or a common operator. [S1]

A person who knows a contact's employer, role or contract details can sound credible. Customer-service and finance teams should still use an independent verification route for account changes, payments and document requests. The existence of an advertised contact list does not confirm that those details were used in a fraud.

Evidence card B08 — 7 Nov 2026

RummRif | Data-sale forum | Forum | English

ORIGINAL

Year: 2024-2026 Country: [...] *Switzerland-600k [...] & from more 70+ Country.

Held
A multi-country phone-data advertisement that labels one segment as Swiss and dates the material across several years.

Not established
Unique Swiss people, reliable attribution of every number, consent status, a 2026 theft date or completed fraud.

4.5 Recent activity: 9–22 November

The recent-activity window is an observation of posts. It is not a separate count of newly affected organisations. Earlier material that reappears during these dates remains earlier material unless new evidence establishes a different incident.

An announced release is not a completed data leak. A 19 November post claimed that a former employee would release bank-related information on 30 November. That promised date falls after the report cutoff. The post does not establish employment, possession of a file or current access. [S1]

The claimed insider story and proposed contents remain the poster's assertions. This report does not authenticate them or identify the bank. The announcement must not become a confirmed incident or a completed publication in the executive summary, timeline or banking totals.

The proportionate response is to preserve the announcement and route it through the organisation's established security process. Compare any independently obtained evidence with authorised access and offboarding records. Decide whether escalation is justified by current evidence, while protecting the confidentiality of the review.

Evidence card B12 — 19 Nov 2026

Jlkrumholz01 | Forum announcement | Forum | English

ORIGINAL

On November 30th I will release a PDF list containing all this information. [...] Wait until November 30th. [...] Account Holder Info.

Held
A 19 November post announced a future bank-related data release scheduled after the report cutoff.

Not established
The poster's claimed employment, possession of a file, current access, data authenticity, affected people or any completed release.

A separate 19 November service advertisement named Switzerland among its voice and messaging destinations. It claimed minimal identity checks and preservation of caller identity information. Related wording appeared in subsequent posts. The advertisement does not verify those capabilities or demonstrate delivery into a Swiss network. [S1]

This service advertisement can inform a defensive exercise without becoming a verified Swiss incident. Ask whether staff rely on the displayed caller number when authorising sensitive requests. Test an independent callback route using already trusted contact information.

The 5 November contractor offer and 7 November phone-data advertisement provide nearby context, but sit outside the recent-activity dates. They must not be shifted into the recent window for emphasis. Their separate validation questions remain relevant after their original posting dates.

4.6 Connect the evidence to an accountable decision

Security operations should maintain an internal record of the source proposition and the validation result. A post can justify an investigation without justifying a public incident statement. Record which current account, system, supplier dataset or process would be affected if the allegation were authentic.

Privacy teams should separate file rows from unique people and organisational responsibility from data possession. A contractor may hold information about a customer without having access to the customer's production systems. Establish the controller and processor roles from the actual relationship.

Supplier managers should preserve the inventory of information shared with each provider. That inventory should include operational instructions and support data alongside obvious customer records. During a claim investigation, it allows the owner to compare the advertised fields with authorised business flows.

Communications teams should retain the distinction between an actor's allegation, the organisation's own finding and the unresolved questions. Repeat only the detail needed for a protective action. Reproducing sensitive field descriptions or dramatic claims can enlarge uncertainty without helping the reader act.

KEY TAKEAWAYS

01

Treat an offer, a reply, a buyer request and a confirmed incident as separate evidence types

02

Validate the age, ownership and current relevance of advertised information before disruptive action

03

Include physical-security and supplier owners when operational handling information may be involved

CHAPTER 05

Targeting examples by sector

05

THIS CHAPTER ANSWERS

How do confirmed incidents change the control priorities for different sectors?

97,000

Permit records, not a count of people

5.1 Read the cases through their evidence boundaries 39

5.2 Campaigns connect otherwise separate sectors 48

5.3 Recent activity: 9–22 November 49

5.4 Additional public reports and narrower dispositions 50

5.5 Additional cantonal incidents and fraud campaigns 51

CHAPTER 05

Targeting examples by sector

IN SHORT

Switzerland's confirmed cases connect information theft, service disruption and subsequent fraud. A cantonal permit database, a pension software supplier and a utility contractor illustrate different dependency risks. Healthcare and media cases show why the affected data and operational consequences need separate descriptions. Recent warnings also extend the discussion to refrigeration controls. Assign each response to the service owner, then verify the affected systems, data and recovery evidence.

5.1 Read the cases through their evidence boundaries

A supplier incident and a customer system intrusion are different events. An organisation may hold affected records at a contractor while its own production systems continue operating. Equally, an organisation can restore service while the consequences of stolen information remain unresolved. These distinctions determine the owners, messages and completion criteria in an incident plan.

The cases below are selected for their decision value. They are not a ranking of sector risk or an inventory of every Swiss intrusion. Dates identify the incident or public update as labelled. Record totals remain attached to their original population. Public announcements do not provide victim-side forensic access to this report.

The following table separates the principal control questions before the case cards supply detail.

Sector	Observed account	Evidence boundary	First decision
Cantonal services	Permit database data theft	Records can repeat a person	Protect applicants and employer contacts
Healthcare	Ransomware interrupted access to imaging information	Medical-data theft remains unresolved	Test clinical workarounds and retrieval
Pensions	Supplier data theft triggered investigations	A supplier event does not establish production-system intrusion	Establish the transferred data inventory
Media	Historical staff contact data affected	No reported evidence of source or research-data exposure	Support staff and review retention
Energy	Contractor-held address and meter information stolen	Utility systems and supply were not affected, according to the utility	Reconcile contractor datasets
Retail and facilities	Refrigeration settings manipulated	The public account does not establish a named actor	Verify temperature and independent alarms

CASE F

F

Cantonal permit records and follow-on identity risk (O01)

Public administration

Official disclosure: records are not people

ACCOUNT	Basel-Landschaft confirmed data theft involving its cross-border worker permit database on 20 November 2026. Its announcement identified 97,000 records, including personal information and employer contact details. [S17]
CHRONOLOGY	An 18 November update described effects on around 20 applications. The 20 November statement confirmed data theft. The permit system had operated since 28 November 2016. [S47][S17]
ESTABLISHED	The canton identified information including names, addresses, birth dates, occupation details and migration-system identifiers. The affected online platform was taken offline. Applications could still be submitted through alternative arrangements. [S16][S17]
LIMITS	The canton explicitly distinguishes records from people. Renewals, changes of address and employment changes can generate repeated records. The FAQ does not confirm theft of uploaded identity documents or employment contracts. [S16]
ALTERNATIVES	Historical entries can explain part of the record volume. The total cannot be converted into current permit holders, unique individuals or confirmed identity-fraud victims. [S16]
RESPONSE	Public-service and employer HR teams should identify affected workflows, preserve the official warning and require independent verification of unusual requests. Correct personal details must not substitute for authentication.

Bottom line

Validate applicant and employer workflows, then use trusted contact routes.

The defensible finding is a confirmed database-related data theft with unresolved individual scope. It is not a count of 97,000 people. The immediate protection task includes employers because their administrative contacts also appear in the affected information. [S16]

CASE G

G Radiology continuity and separate questions about stolen data (O02)

Healthcare

Ransomware reported; medical theft unresolved

ACCOUNT	Groupe 3R states that a ransomware attack occurred on 30 April 2026. It reports encryption and theft of administrative information, including information about current and former employees. [S18]
CHRONOLOGY	Patient care was particularly affected on 1 and 2 May. The operator says the centres had a rebuilt infrastructure from 26 June. Its public information page carries a 22 September situation update. [S18]
ESTABLISHED	Medical examination results were encrypted, affecting their availability. The operator says centres remained open, although some examinations were delayed, rescheduled or redirected. Major systems and teleradiology were subsequently restored. [S18]
LIMITS	The operator could not establish with certainty whether patient medical information was also stolen. The absence of a confirmed publication of those files does not resolve that question. [S18][S19]
ALTERNATIVES	Service restoration and data confidentiality require separate closure decisions. The operator describes the 2026 event as unrelated to its 2025 incident. The earlier attack cannot be counted again as a new 2026 case. [S18]
RESPONSE	Clinical operations should test access to examination results, referral alternatives and appointment confirmation. Security and privacy teams should maintain a separate assessment of data theft and any subsequent patient-directed fraud.

Bottom line

Test the clinical workflow and assess confidentiality separately from restoration.

ICTjournal reports that the operator attributed the attack to Akira, citing the findings of its specialist partners. That is the operator's attribution as reported by the publication. This report has no independent technical evidence connecting an actor to the incident. [S19]

For healthcare leaders, a successful restore test should include the full clinical workflow. Restoring a server does not demonstrate that clinicians can retrieve images, interpret examinations and communicate with referring practices.

CASE H

H ■ Pension supplier data and the scope of the investigation (O03)

Pensions

Supplier incident: investigation continuing

ACCOUNT	Publica confirmed a data leak following an attack identified by an external software supplier at the end of September. The supplier informed Publica, other customers and the relevant federal authorities. [S21]
CHRONOLOGY	Publica sent an initial member communication on 8 October. FDPIC received the supplier's notification that day, began preliminary enquiries concerning Publica on 14 October and opened a supplier investigation on 22 October. [S21][S15]
ESTABLISHED	FDPIC says data from several pension institutions was taken. Its investigation seeks to establish the personal information supplied, the legal arrangements for those transfers and the extent of the information lost. [S15]
LIMITS	A confirmed supplier data leak does not identify every affected person, every field or the operational state of every customer system. The investigation remained pending in the cited announcement. [S15]
ALTERNATIVES	A supplier-held working dataset and a production pension database have different roles. The public record must not be expanded into an unsupported assertion about access to the latter.
RESPONSE	Pension administrators should reconcile the supplier's retained datasets with contractual purposes and retention requirements. Member-service teams should verify identity through an independent process when a caller already knows personal or financial details.

Bottom line

Reconcile supplier-held information with contractual purposes and member protection.

The case creates two separate workstreams. The first establishes what information the supplier held and what was taken. The second protects members from convincing approaches that reuse that information. The relationship between those workstreams should be explicit in customer communications.

Cybercrimepolice also warns about investment approaches following a pension-service-provider data leak. Its discussion includes possible misuse of salary and pension information. The warning supports fraud preparedness; it is not a verified list of every field taken from this supplier. [S45]

On 19 November, Publica announced an external review covering procurement, personal-data handling, security controls and governance. It identified the supplier's test environment as the concern and stated that Publica's production systems were unaffected. Technical enquiries into the affected individuals and data remained unfinished. [S55]

CASE I

Historical media staff data and the limits of a broader narrative (O04)

Media

Historical staff information reported

ACCOUNT	SRG reported a cyber incident on 28 September involving contact and organisational information from 2020 concerning around 340 current and former SRF employees. [S20]
CHRONOLOGY	SRG says it disabled the affected access, added security measures, notified authorities and informed affected individuals. The investigation was ongoing when the announcement was issued. [S20]
ESTABLISHED	The identified information included names, roles and business contact details, with some private contact information. SRG described the affected population and supported the people concerned. [S20]
LIMITS	SRG reported no indications that passwords, financial information, journalistic sources, research material or communication contents were affected. It also reported no indications of publication or misuse at that time. [S20]
ALTERNATIVES	Historical employee information can retain social-engineering value. Its presence does not establish interference with reporting, editorial decisions or broadcast operations.
RESPONSE	Security and HR should review why historical contact datasets remain accessible. Staff support should cover impersonation attempts and suspicious approaches without presenting unverified consequences as established harm.

Bottom line

Review retention and access while supporting staff against impersonation.

The control lesson concerns retained information and access governance. A media organisation's role does not justify attributing a political motive. The cited account supplies no basis for that conclusion. The report therefore keeps the affected data category and the unresolved cause separate. [S20]

CASE J

J

Utility contractor records without an energy-supply incident (O05)

Energy and utilities

Contractor data; utility systems unaffected as reported

ACCOUNT	IWB announced on 15 July that attackers had stolen around 40,000 address records held by a service provider. The information included technical details about energy meters. [S40]
CHRONOLOGY	The provider informed IWB after detecting the attack. IWB checked access, limited exchanges with that provider and sent letters to affected customers. [S40]
ESTABLISHED	The utility identified names, addresses, meter numbers and installation characteristics. It stated that its systems and the security of energy supply were unaffected. [S40]
LIMITS	IWB said email addresses, telephone numbers, consumption information and bank or payment data were absent from the stolen dataset. It reported no indications of misuse at the time. [S40]
ALTERNATIVES	A utility-associated dataset is not evidence that attackers reached operational controls. Address and meter information should not be described as a complete customer financial profile.
RESPONSE	Supplier managers should validate the inventory shared with contractors. Customer-service teams should prepare for approaches that reference a real address or meter while demanding urgent payment or additional information.

Bottom line

Reconcile contractor information and prepare customer support for convincing requests.

IWB reported that the cantonal data-protection authority assessed the misuse risk as low. That assessment belongs to the described information and circumstances. It should not become a general statement that contractor data theft is harmless. [S40]

CASE K

K ■ Refrigeration control and independent verification of the physical process (O06)

Retail and facilities

Official warning: actor unassigned

ACCOUNT	BACS warned on 10 November that refrigeration-control attacks had affected Switzerland. A 12 November police notice describes a Swiss business where manipulated refrigeration settings produced substantial temperature deviations and temporary closure of a branch. [S53][S41]
CHRONOLOGY	These notices belong to the recent-activity window. They address attacks known in the preceding weeks. They do not supply a verified first-access date for the individual business. [S53][S41]
ESTABLISHED	The police notice describes the ability to alter temperatures, defrost cycles and alarm settings through inadequately protected management interfaces. It recommends checking actual temperatures with an independent instrument. [S41]
LIMITS	The available accounts do not establish a named actor or a political motive. The technical warning covers several product families and cannot identify which system a particular victim operated. [S53]
ALTERNATIVES	A quiet alarm panel does not establish a healthy physical process if alarm settings can be changed. Equipment failure and unauthorised changes require different investigations, but both require independent safety checks.
RESPONSE	Facilities, the refrigeration contractor and IT should jointly inspect remote access, supported software and alarm delivery. Protect necessary remote maintenance and confirm actual temperatures before restoring normal operation.

Bottom line

Check the physical temperature independently and review remote management access.

This case also limits the interpretation of older national assessments. BACS reported no known targeted Swiss cybersabotage in its first-half overview. A later operational-technology incident must be considered on its own facts, without relabelling it as state sabotage. [S5][S41]

CASE L

L

Federal collaboration access and affected accounts (O07)

Public administration

Official account: around 200 accounts

ACCOUNT	The federal IT office announced on 4 August that around 200 user and technical accounts were affected by an attack against its SharePoint servers. [S54]
CHRONOLOGY	Specialists detected unusual activity on 28 July. Analysis identified affected account credentials on 31 July. The office reset passwords, blocked external internet access and began rebuilding the servers. [S54]
ESTABLISHED	The office's account distinguishes affected credentials from other information. It reported no indications of additional data theft in the analysis available at publication. Internal users retained document access and alternative sharing arrangements. [S54]
LIMITS	The stated absence of indications is not a completed forensic determination. The notice names no actor. It does not provide a basis for attributing a motive or extending the affected population beyond the described accounts. [S54]
RESPONSE	Collaboration-service owners should test credential revocation and alternative document exchange. Separate the authority to reopen external access from the evidence required to close the data-theft investigation.

Bottom line

Validate account scope and affected services without inferring a wider population.

CASE M

M

Education support tickets and targeted helpdesk impersonation (O08)

Education

Official disclosure: school contact information

ACCOUNT	Vaud reported unauthorised copying of names and school email addresses concerning around 3,500 teachers and 38,000 students. Support-request contents were also copied. [S59]
CHRONOLOGY	The canton detected the unauthorised access on 26 October. It disconnected the support platform, secured it with its security operations centre and directly informed users. [S59]

ESTABLISHED	The affected service handled IT support requests for post-compulsory education. The canton stated that account passwords were not stored there and that school records such as grades and student files were not affected. [S59]
LIMITS	A ticket's text and an education-record database are different populations. The case does not establish that attackers obtained every account password or every school record. [S59]
RESPONSE	Education IT should warn users about messages impersonating their school or helpdesk. Require verified support requests and inspect whether attachments or free-text tickets retain information beyond the service's operational need.

Bottom line

Protect affected educational identities and verify unusual contact through trusted routes.

N

CASE N

Adult education and a changing assessment of affected data (O09)

Education

Official incident: scope later revised

ACCOUNT	Ifage states that an attack on 11–12 April led to data theft. Detection followed on 13 April. Its later notice explains that publication on 23 July established that learner and customer information was also involved. [S58]
ESTABLISHED	The institution identifies course-administration information, contact details and examination-related documents. Some files included identity documents, application material or absence justifications. It states that operational continuity was maintained. [S58]
LIMITS	The notice supplies no verified total of affected people. A later clarification expands the known scope of one incident; it does not create a second intrusion. [S58]
ALTERNATIVES	An initial announcement can accurately reflect an incomplete investigation. Readers should distinguish that changing knowledge from a new attack or verified ongoing access.
RESPONSE	Education and privacy teams should maintain a versioned data-impact register. Update direct communications when new categories become established, while retaining the date and basis for the earlier assessment.

Bottom line

Keep the revised data assessment distinct from the earlier service recovery.

CASE O

University online forms in the recent-activity window (O10)

Education

Official disclosure: online form information

ACCOUNT	USI announced on 19 November that unauthorised parties accessed information through a vulnerable online-forms system between 9 and 17 November. [S80]
ESTABLISHED	The application supported some job applications, scholarship requests and surveys. Form answers and attachments were present on the affected server. The university secured it and informed authorities and potentially affected individuals. [S80]
LIMITS	USI said it was still establishing the scope, sensitivity and risks of the affected information. Its announcement did not give a verified count of affected people or establish that every attachment was copied. [S80]
ALTERNATIVES	Different forms collect different information. A job applicant, scholarship applicant and survey respondent should not be treated as one uniform data-risk population.
RESPONSE	Application owners should identify affected form purposes and retention periods. Ask recipients to verify unexpected document, banking and payment requests through an established university channel.

Bottom line

Identify affected forms, preserve the notice and verify subsequent requests independently.

5.2 Campaigns connect otherwise separate sectors

Several official warnings describe a shared mechanism rather than a named victim. They matter because a supplier's customer, an employee and a household can face connected fraud stages. The sequence does not establish that every stage belongs to one operator.

The following campaign table preserves the source's unit and identifies a proportionate control response.

Notice date	Campaign account	What remains uncertain	Defender decision
2026-02-03	Genuine SharePoint sharing led to a later real-time phishing step [S24]	The notice does not count all affected organisations	Review the full link journey and session exposure
2026-02-10	Subscription bombing obscured important account messages [S25]	A noisy inbox alone does not establish a fraudulent payment	Search for account, order and payment changes

Notice date	Campaign account	What remains uncertain	Defender decision
2026-02-24	ClickFix lures encouraged users to run harmful commands [S26]	User action does not reveal the entire intrusion path	Route fake fixes to the help-desk and inspect endpoint evidence
2026-04-14	False bank staff requested remote-maintenance software [S27]	A bank brand in the script does not establish bank intrusion	Verify calls independently and restrict unsolicited remote support
2026-05-05	Parcel phishing was followed by a false-bank phone call [S28]	Campaign scale and operator identity are not established	Tell customers what a payment confirmation actually authorises
2026-06-09	Jobseekers faced interview phishing, payment demands and malware lures [S30]	The notice describes different schemes	Separate recruitment and payment workflows
2026-09-01	A food-delivery website was used for attempted payment-data theft [S32]	The source does not identify every affected transaction	Monitor payment-page changes and third-party content
2026-10-20	Hotel-booking lures expanded toward mobile-payment and banking access [S34]	Detailed booking knowledge does not establish every upstream cause	Confirm unusual requests through the booked provider

5.3 Recent activity: 9–22 November

Accurate personal details no longer establish a trustworthy request. The 17 November BACS notice links an earlier household-service-provider data leak with subsequent targeted phishing. Messages reused names, addresses and social-insurance numbers. The notice also describes phishing built around a PHP security-update pretext. [S14]

The same week's police notice describes holiday-booking messages containing real accommodation details and booking references. The attackers requested a supposed reservation confirmation and then payment-card information. This report retains the service-provider role because naming eligibility has not been fully established. [S43]

The 18 November police warning adds an offline payment stage. Callers impersonated bank staff and used a forged central-bank letter to solicit cash for a supposed safeguarding account. The claimed authority is part of the fraud narrative, not evidence of central-bank involvement. [S44]

The 20 November Basel-Landschaft update makes the data-to-fraud link an immediate operational question. HR departments should expect approaches that reference genuine employment or permit details. The official statement supports heightened vigilance; it does not establish that every affected person has already received a fraudulent message. [S16][S17]

USI's 19 November notice adds online forms and attachments to the immediate response agenda. Publica's update that day concerns an external governance review of its existing supplier incident. These are different developments: a newly disclosed university incident and a later response to an earlier pension-data event. [S80] [S55]

These updates support a practical November exercise. Give customer support and the helpdesk an unexpected request containing correct personal details. Require independent verification, preserve the message and record the decision. Measure whether the team follows the trusted process despite the convincing information.

5.4 Additional public reports and narrower dispositions

The following items add sector coverage without adopting an unverified actor narrative. Where a direct public confirmation was not retained, the organisation remains described by role. The linked publication is the source of the reported organisational account.

Date	Role	Reported account	Disposition
2026-01-23	Radio and events operator	External event database affected; passwords and payment data excluded from the reported scope [S56]	Supplier-data exposure example
2026-03-04	Business software provider	Company acknowledged an incident with limited operational effects; a separate advertised data volume remains a claim [S50]	Claim and impact kept separate
2026-03-25	Engineering services provider	February incident followed by precautionary disconnection and reported restoration [S48]	Verify unexpected supplier invoices
2026-04-14	Medical-products manufacturer	Legacy internal system and older internal documents were identified in the reported company account [S49]	Legacy-system retention example
2026-08-26	Business school	External provider incident affected student and alumni information; local operations continued, according to the school [S57]	Supplier and local systems distinguished
2026-07-09	Residential care provider	Ransomware disrupted systems; an October update described partial rebuilding and continuing care [S81]	Test prolonged communications and care workarounds
2026-03-14	Municipal administration	Partial encryption followed by restoration; the municipality reported no indications of data theft [S86]	Keep restoration and data-theft findings distinct
2026-07	Industrial manufacturer	A cantonal review described access to a supplier-sharing platform and a separate extortion demand [S84]	Confirm the scope of shared platforms

Date	Role	Reported account	Disposition
2026-07	Fiduciary services	The cantonal review described published client files after an incident [S84]	Inventory tax and client documents held by advisers
2026-09	Hospital laboratory partner	A cantonal review described patient information affected at an external laboratory [S85]	Reconcile laboratory transfers and patient contacts
2026-10-26	Sports administration platform	The federation confirmed unauthorised account access and a subsequent forum sale offer; passwords were not affected [S88]	Review account permissions and warn participants
2026-10-31	Sports licensing platform	The federation confirmed a personal-data incident but had not established its complete scope [S87]	Avoid treating advertised row totals as people
2026-11-16	Streaming website	A security researcher reported malicious third-party website scripts affecting a Swiss streaming service [S89]	Review browser-side dependencies and supplier notices

The care provider's October update still assumed a data leak but did not establish its extent. It stated that basic care, medical support and residents' safety remained assured. Its expectation of normal operation by late November was a forecast, not a confirmed recovery date. [S81]

Official notices also distinguish defensive action from an intrusion. A public authority reported temporarily restricting some services while addressing PHP vulnerabilities in October, with no related attack observed. FDPIC's April warning concerned impersonation of the regulator, not access to its systems. [S83][S82]

These examples should not be added to the case-card totals as new evidence cards. They are incident mentions. The difference is a presentation choice, not a claim that mentioned incidents have a lower business impact.

5.5 Additional cantonal incidents and fraud campaigns

Separate unauthorised access from precautionary service restrictions. A cantonal authority reported a SharePoint incident on 5 August. Its preliminary analysis found no indications of affected accounts or data theft. An evening security update would temporarily interrupt the public website. Other applications remained available. The announcement describes a distinct incident from the federal collaboration case. [S90]

Public information can still support convincing fraud. A 28 August joint notice described automated collection of publicly accessible vehicle-holder information across five cantons. Protected entries were not affected. The notice also described extortion attempts and warned about payment demands that could reuse the information. This is not evidence that protected vehicle records were stolen. [S91]

The police notices below add local evidence to the year's broader impersonation pattern. They concern different periods and populations. Their counts should not be summed into a national incident or loss total.

Notice	Police account	Scope boundary	Action
2026-01	Vaud recorded 24 false-bank or false-police cases during the week of 12 January, including 12 attempts [S92]	A single cantonal week	Train customer-facing staff to recognise urgent cash demands
2026-02-10	St.Gallen described remote-access fraud causing an individual loss above CHF 500,000 in late January [S93]	One reported person's loss	Verify unsolicited support calls before allowing remote access
2026-04-24	Ticino described an attempted family-emergency fraud interrupted following a prompt report [S94]	A police-reported attempt, not a completed loss	Establish a trusted family verification route
2026-06-10	Bern warned about remote-access fraud involving substantial losses [S95]	Its loss period began in November 2025 and extended to April 2026	Avoid assigning the complete amount to 2026
2026-09-24	Two suspected couriers reported accepting online job offers [S96]	Their account does not identify a whole network	Scrutinise paid envelope collections
2026-10-13	Messages led to calls and collection of cards with intact chips [S97]	Several investigations and observations	Escalate card-collection requests
2026-10-29	Neuchâtel reported 160 established cases during 2026 to that date, with estimated losses around CHF 950,000 [S98]	Cantonal reporting to the notice date	Preserve the reporting period in leadership briefings
2026-11-10	Valais described around 40 reports since mid-October, including attempts and completed fraud [S99]	Reported attempts are not completed-loss incidents	Record the outcome as well as the approach
2026-11-19	Zug described two courier investigations and an intervention prompted by bank staff [S100]	Two independent cases; investigations remained ongoing	Maintain an escalation route for unusual cash withdrawals

These notices support a control that spans banking, customer service and family support. A persuasive caller may combine a familiar institution, genuine personal details and an urgent request. A subsequent courier gives the fraud an offline completion stage. Verify the request through a known channel before transferring money, releasing a card or permitting remote access. [S92][S93][S97][S100]

The Schaffhausen account also connects job-offer scrutiny with fraud prevention. It does not establish that every courier understands the purpose of a collection. Employers, platforms and applicants should examine unusually easy paid tasks involving cash or sealed envelopes without assuming that all such adverts belong to one actor. [S96]

The November notices strengthen the recent-activity assessment without establishing national growth. Local case counts depend on their stated periods and reporting populations. A warning or arrest is useful evidence of an active mechanism; it does not provide a national prevalence measure. [S99][S100]

KEY TAKEAWAYS

01

Keep service restoration and data-theft assessment as separate decisions

02

Treat records, people and organisations as different populations

03

Verify unexpected requests even when the sender knows genuine personal details

CHAPTER 06

Hacktivism and DDoS

06

THIS CHAPTER ANSWERS

What can availability incidents establish about impact, attribution and motive?

40 minutes

Reported Salt internet outage

6.1 The 2026 official account 55

6.2 Claim versus reporting 55

6.3 A dated historical comparison: the 2024 summit 56

6.4 Timeline and response decisions 56

6.5 Messaging availability and an independent status channel 57

CHAPTER 06

Hacktivism and DDoS

IN SHORT

Availability attacks require an impact record separate from any actor's publicity. BACS describes limited Swiss DDoS disruption in the first half of 2026, while identifying a noticeable telecom outage. Historical summit-related attacks remain useful preparation examples, but belong to 2024. Neither country-themed rhetoric nor a successful website interruption establishes access to internal data. Record the service affected, customer impact, source attribution and recovery evidence before deciding on escalation.

6.1 The 2026 official account

Availability impact and publicity are different measures. In its first-half report, BACS states that DDoS activity remained within manageable limits for Swiss organisations. It says there were virtually no hacktivist attacks against major events such as the WEF or the Winter Olympics. It also describes attempts affecting DNS infrastructure and individual banking services without significant outages. [S5]

Those statements concern the reporting period and the authority's visibility. They do not establish that no attempts occurred, that every organisation reported an attempt or that the same pattern continued through November. A later actor announcement must therefore be evaluated as new evidence.

The report identifies a Salt incident as the period's widely noticeable DDoS impact. Netzwoche reports that fixed-network customers lost internet access for around 40 minutes on 15 May. It distinguishes that disruption from the mobile network, which continued working. The publication says the actor, motive and any ransom demand remained unclear. [S5][S22]

Do not convert a telecom-service interruption into an unsupported claim about stolen customer data. Likewise, an interrupted public website does not establish interference with an organisation's internal network. The response needs separate owners for availability, intrusion analysis and customer communications.

6.2 Claim versus reporting

The panel below deliberately separates the measures. It includes an unresolved actor account rather than filling that gap with a plausible name.

Point	Actor claim	Official account	Public reporting
2026 telecom impact	No authenticated actor statement establishes responsibility here	BACS identifies a noticeable Salt DDoS outage in its first-half report [S5]	Around 40 minutes of fixed-network internet disruption on 15 May [S22]
Network scope	No verified claim establishes broader access	The authority's account concerns availability [S5]	The mobile network continued operating, according to the cited report [S22]
Motive	No independently supported motive	The cited national account does not assign a political purpose to this incident [S5]	Actor identity and motive were unclear in the publication [S22]
Internal data	A service interruption supplies no evidence of data theft	No such finding is established by the cited availability account [S5]	The reporting describes outage effects rather than a confirmed internal-data incident [S22]

The panel is a response discipline. A loud claim can coexist with limited disruption, while an unnamed attack can produce substantial customer impact. Neither relationship supports a numerical claim-to-impact ratio unless both measurements describe the same event and unit.

6.3 A dated historical comparison: the 2024 summit

The Summit on Peace in Ukraine took place on 15–16 June 2024. In its 20 June review, the NCSC attributed related DDoS attacks to NoName057(16). The authority described minor disruption and stated that summit IT systems and data were not threatened. Those findings are the NCSC's account. [S42]

The same review distinguishes other incidents from the DDoS activity. It describes intrusion attempts against cantonal systems and phishing directed at emergency-call-centre employees. It also states that live-broadcast technical problems and a regional power outage were not cyber incidents. Those distinctions prevent unrelated disruption from being absorbed into an attack narrative. [S42]

This historical comparison is not a 2026 incident count. It does not establish responsibility for the 2026 telecom attack or a current campaign against every organisation involved in international events. The report takes no position on the summit, sanctions, EU relations or government policy.

The transferable lesson concerns preparation. The NCSC describes a public-private situation network, early preparation and coordinated response. Event organisers can use that example to assign communication contacts, protect public services and confirm how disruption will be measured. [S42]

6.4 Timeline and response decisions

The timeline distinguishes historical background, a 2026 incident date and later publication dates.

20 Jun 2024 **NCSC**

Historical review attributed summit-related DDoS to NoName057(16), with minor disruption [S42]

15 May 2026	**Public reporting** Salt fixed-network outage later described as a DDoS incident [S22]
24 Aug 2026	**BACS** First-half report described manageable DDoS impact and the telecom outage [S5]
18 Nov 2026	**Cantonal administration** Basel-Landschaft said emergency and rescue systems remained operational during its separate IT incident [S47]

The November cantonal update belongs here as a communication lesson, not a DDoS attribution. An early warning about possible disruption must not be reported as an observed emergency-service failure. The canton stated that the relevant emergency and rescue IT systems were never affected. [S47]

For security operations, escalation should depend on observed service degradation and a documented business consequence. Preserve the start and recovery times, the affected function and the organisation's own service measurements. A third-party screenshot provides a lead rather than a complete impact record.

For communications teams, distinguish the public site, customer authentication, communications network and internal systems. Issue updates around the function customers can use and the alternative route available. Avoid repeating actor slogans or treating an asserted political motive as established fact.

For service owners, rehearse the point at which protective action reduces functionality. Agree who authorises that action, who explains it and how restoration is validated. The record should make preventive containment distinguishable from damage caused by an attacker.

6.5 Messaging availability and an independent status channel

Threema's 14 August 2026 account describes DDoS disruption during 11–12 August. The company reported unavailability between 19:30 and 23:30 CEST on Tuesday, followed by intermittent interruptions on Wednesday morning. It reported normal operation restored at 12:23 on Wednesday. The event belongs to the second half of 2026. [S101]

The company described attacks affecting its service and a colocation partner. It could not establish whether Threema was the primary target or one of several targets. Customers running Threema OnPrem on their own infrastructure were unaffected, according to the company. The availability account supplies no basis for assigning a state actor or inferring access to internal messages. [S101][S102]

An unrelated technical issue initially prevented the status page from updating. Threema temporarily took that page offline. Its 14 August update states that additional DDoS protection had been activated. It also planned an incident history and an independent notification feed. Those are the company's dated response statements, rather than an assessment of present control effectiveness. [S101]

For service owners, the case supports testing an alternative communication route alongside availability mitigation. Confirm that customers can distinguish an unavailable service from an unavailable status page. Preserve each function's interruption and recovery times separately.

KEY TAKEAWAYS

01

Attribute actor responsibility only to the source that establishes it

02

Keep the 2024 summit outside the 2026 incident totals

03

Measure the affected service and recovery before amplifying an actor's narrative

CHAPTER 07

Threat actors and supported relationships

07

THIS CHAPTER ANSWERS

Which actor descriptions help defenders without overstating attribution?

41

group labels in the Swiss ransomware listing snapshot

7.1 Ransomware brands describe listings, not complete intrusion histories 60
7.2 Regional context without a country ranking 63
7.3 Personas and relationships in the retained posts 63
7.4 State-linked activity as assessed by the FIS 65
7.5 Technique matrix for control planning 66
7.6 Patch readiness: the October PHP warning 67
7.7 Politically framed actors 67
7.8 What would strengthen an actor assessment 68
7.9 Brief update tampering and retrospective evidence 68

CHAPTER 07

Threat actors and supported relationships

IN SHORT

The evidence supports several separate actor views: ransomware listing brands, personas advertising material, politically framed availability claims and official assessments of espionage. They do not form one proven network. AKIRA has the largest Swiss listing count in this snapshot, while other brands account for most listings. National and state-linked attributions remain those of the cited authority. Use actor information to choose investigation questions and recovery scenarios.

7.1 Ransomware brands describe listings, not complete intrusion histories

Ransompedia records 122 Swiss listings across 41 group labels in the reporting window. AKIRA contributes 13 listings, and The Gentlemen (listed as Thegentlemen in the raw snapshot) and Qilin each contribute 9. Together these three labels account for 31 listings, or 25.4% of the Swiss total. The remaining 91 listings account for 74.6% [S2].

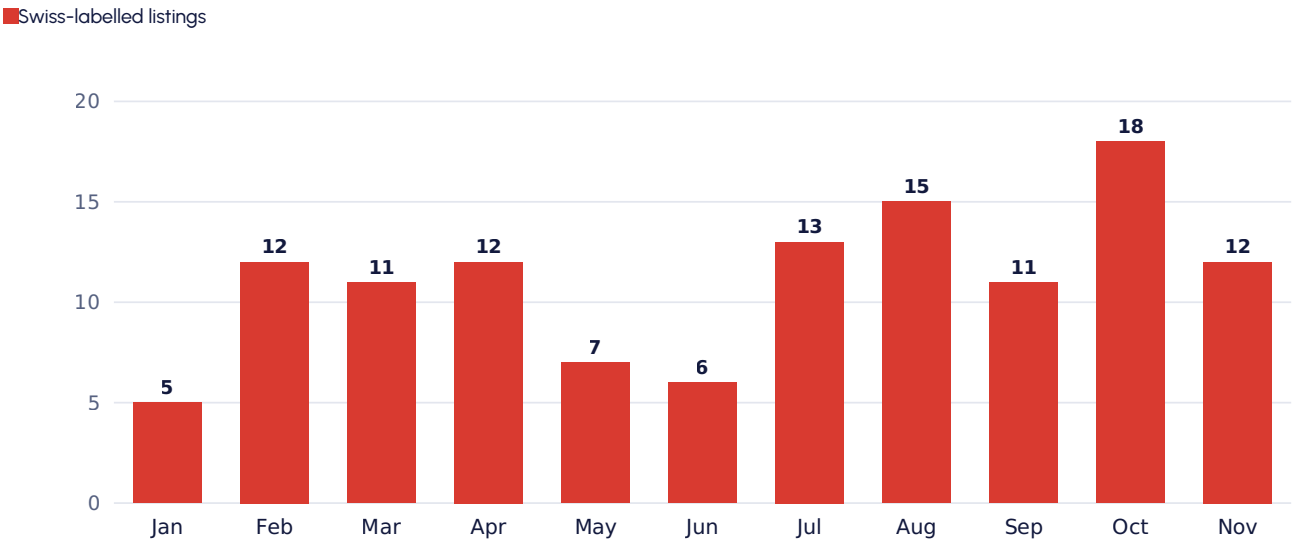
This distribution argues against designing continuity around a single brand. Listing labels can change, organisations can appear more than once, and a public extortion claim does not establish which software ran. Recovery planning should remain useful when the specific operator or entry route is unresolved.

The table preserves the unit of measurement. It is a count of listings in the snapshot, rather than a count of independently verified incidents.

Group label	Listings	Share	Evidence boundary
AKIRA	13	10.7%	Listing label; individual outcomes require corroboration
The Gentlemen	9	7.4%	Listed as Thegentlemen in the snapshot; no shared operator inferred with other brands
Qilin	9	7.4%	Listing label; count does not establish initial access
Bravox	8	6.6%	Listing label; claims remain claims
Safepay	7	5.7%	Listing label; payment and data scope unresolved
Other labels	76	62.3%	Remaining labels combined; no alliance implied
Total	122	100.0%	Separate from the authority's ransomware population

Rounding the displayed group shares produces a small difference from the total. The total uses the underlying listing counts.

Swiss extortion listings occur throughout the reporting window



Source: retained Ransompedia country-labelled listings, collected 22 November 2026. Listing dates are not incident dates [S2].

AKIRA

Ransomware listing brand | Extortion claims; individual operator identity unresolved

EVIDENCE HELD

1 January–22 November

13 Swiss listings in the retained snapshot [S2]

LISTING SCOPE

Organisation labels in the Swiss listing snapshot

SEEN IN PUBLIC REPORTING

[S2] 13 of 122 Swiss listings; a listing is a criminal claim.

OUR ASSESSMENT

The listing count supports continuity planning. It does not establish encryption, data theft, payment or an entry route for each organisation.

CONFIDENCE

High for the retained listing count; individual incident outcomes require corroboration.

Qilin

Ransomware listing brand | Extortion claims; individual operator identity unresolved

EVIDENCE HELD

1 January–22 November

9 Swiss listings in the retained snapshot [S2]

LISTING SCOPE

Organisation labels in the Swiss listing snapshot

SEEN IN PUBLIC REPORTING

[S2] 9 of 122 Swiss listings; a listing is a criminal claim.

OUR ASSESSMENT

The listing count supports continuity planning. It does not establish encryption, data theft, payment or an entry route for each organisation.

CONFIDENCE

High for the retained listing count; individual incident outcomes require corroboration.

The Gentlemen

Thegentlemen (listing label)

Ransomware listing brand | Extortion claims; individual operator identity unresolved

EVIDENCE HELD

1 January–22 November

9 Swiss listings in the retained snapshot [S2]

LISTING SCOPE

Organisation labels in the Swiss listing snapshot

SEEN IN PUBLIC REPORTING

[S2] 9 of 122 Swiss listings; a listing is a criminal claim.

OUR ASSESSMENT

The listing count supports continuity planning. It does not establish encryption, data theft, payment or an entry route for each organisation.

CONFIDENCE

High for the retained listing count; individual incident outcomes require corroboration.

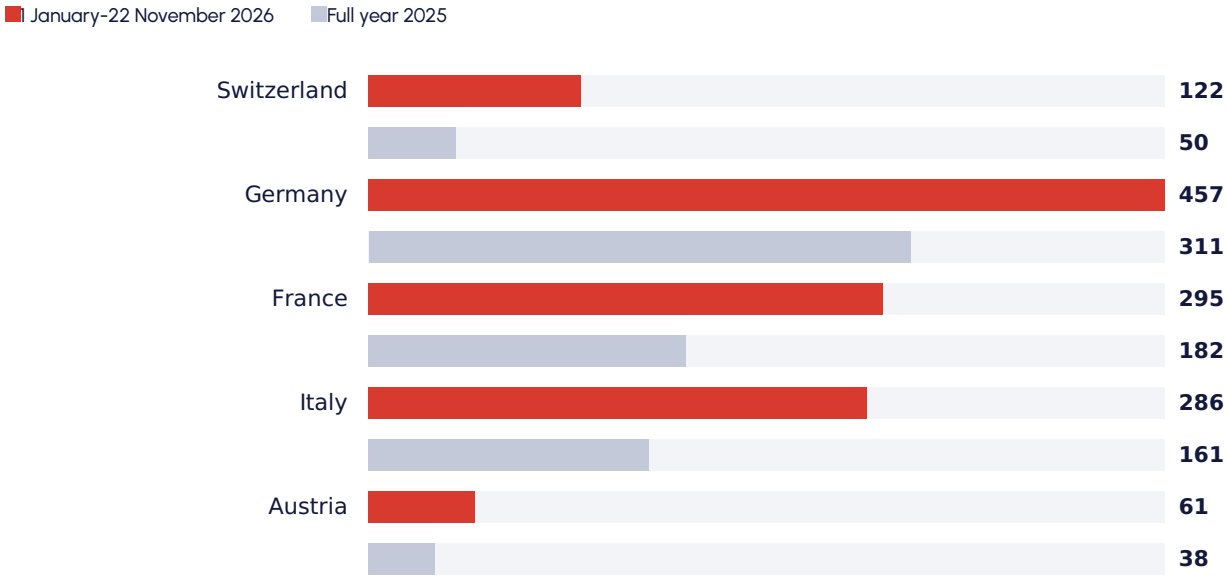
7.2 Regional context without a country ranking

The regional peers share borders or language and business connections with Switzerland. Their listing totals are Germany 457, France 295, Italy 286 and Austria 61. The same snapshot holds full-year 2025 totals of 311, 182, 161 and 38 respectively. Switzerland's full-year 2025 total is 50 [S2].

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

Every selected peer's partial-year 2026 count exceeds its full-year 2025 count in this snapshot. That is a descriptive listing comparison. Different time periods, observation coverage, disclosure and country assignment prevent a direct attack-rate conclusion. It does not establish that a resident or business is safer in one country.

Every selected peer has more listings than its full-year prior-period total



Unmatched periods; not a national risk ranking. Source: retained Ransompedia country-labelled listings, collected 22 November 2026. Listing dates are not incident dates [S2].

For a multinational business, the practical use is to test a common recovery scenario across regional operations. A shared service or supplier can create a cross-border dependency even when the public listing names only one local entity. The incident owner must establish the actual scope rather than inheriting the listing's country label.

7.3 Personas and relationships in the retained posts

A persona is the alias attached to a post. It is not a verified person, company, nationality or stable operator. The evidence cards preserve only the information needed to understand the claim. Contacts, victim identifiers and personal information are withheld [S1].

A repeated alias can support a relationship between advertisements. It does not independently establish that the same human wrote both posts, that the advertised files are identical, or that any sale occurred. Similar titles or record counts can also arise from copied advertising.

The relationship view therefore keeps advertisements, personas and listing brands as separate nodes. A source-backed edge states what connects two nodes; the displayed graph contains only two observed persona-to-post edges (NormalLeVrai to B01 and pfavre to B04), while the three listing brands remain unconnected. The table below summarises possible evidence relationships across the report.



Unconnected nodes have no established relationship. No common operator or alliance is inferred.

Possible evidence relationship	What supports it	What it does not establish
Persona to post	Alias attached to retained material [S1]	Legal identity, nationality or control of every account using that alias
Post to claimed dataset	The offer's description [S1]	File authenticity, origin, age or number of unique people
Brand to listing	The retained listing record [S2]	Encryption, theft, an affiliate's identity or completed payment
Authority to attribution	The authority's published assessment [S9][S42]	Independent attribution of an unrelated Swiss advertisement

NormalLeVrai

Forum persona | Advertising role observed; legal identity unresolved

EVIDENCE AND PUBLIC CORROBORATION

2026-05-04
Advertisement shown in B01 [S1]

CLAIMED SUBJECT

Insurance-labelled information

SEEN IN PUBLIC REPORTING

[S1] The retained post establishes the advertisement. Independent confirmation of the underlying claim is not established here.

OUR ASSESSMENT

An alias attached to an offer does not establish a verified person, nationality, current access or a completed transaction.

CONFIDENCE
High that the material was observed; the advertised information remains unverified.

pfavre

Forum persona | Advertising role observed; legal identity unresolved

EVIDENCE AND PUBLIC CORROBORATION

2026-11-05
Advertisement shown in B04 [S1]

CLAIMED SUBJECT

Business-services information

SEEN IN PUBLIC REPORTING

[S1] The retained post establishes the advertisement. Independent confirmation of the underlying claim is not established here.

OUR ASSESSMENT

An alias attached to an offer does not establish a verified person, nationality, current access or a completed transaction.

CONFIDENCE
High that the material was observed; the advertised information remains unverified.

A progression from identity information to impersonation, account abuse and extortion can be useful as an **analytical model**. It is a planning sequence, not a finding that the personas and brands in this report cooperate.

7.4 State-linked activity as assessed by the FIS

The FIS 2026 report and federal summary identify Russian and Chinese services as the principal espionage threat in Switzerland, alongside state cyber threats from Russia, China, Iran and North Korea [S9][S110]. The official assessment distinguishes political, diplomatic and critical-infrastructure targeting from collection against research institutions, universities and advanced technology companies [S9][S110]. Those attributions belong to the Swiss authorities; this report does not attribute an unnamed seller or unverified listing to a state.

The FIS describes phishing, exploitation of known vulnerabilities in network equipment, and access through IT or telecommunications providers. These are strategic patterns in an official assessment. They do not determine the entry route in the specific health, supplier or administrative incidents discussed in Chapter 5.

Use this assessment to identify sensitive information and persistent access paths. A research institution may need to review external collaboration accounts. An international business may need to examine remote access to commercially sensitive material. A supplier may need to establish which customer environments its support identities can reach.

Source-attributed focus	Official assessment [S9][S110]	CISO decision priority
Principal espionage priority	FIS identifies Russian and Chinese intelligence services as the main espionage threat in Switzerland	Review persistent access, diplomatic or policy workspaces, and external collaboration accounts
Advanced technology and research	FIS highlights collection against universities, research institutes and technology businesses	Audit project-repository permissions, offboarding of visiting researchers, and partner data sharing
Critical infrastructure and suppliers	FIS identifies state cyber activity against critical infrastructure, IT providers and telecommunications	Validate internet-facing network equipment, patching of known vulnerabilities, and supplier support paths

7.5 Technique matrix for control planning

The matrix maps source-described behaviour to standard ATT&CK terms. The mapping is an analyst interpretation for planning. It does not assert a complete attack chain or confirm execution in every Swiss case [S9].

Source behaviour	ATT&CK term	Planning question	Boundary
Tailored phishing	T1566, Phishing [S70]	Can users verify the sender through a trusted route?	FIS describes the pattern; individual case delivery remains separate
Exploitation of exposed equipment	T1190, Exploit Public-Facing Application [S71]	Is the service owned, supported and remediated?	A vulnerable product does not establish exploitation
Use of an obtained account	T1078, Valid Accounts [S72]	Are sessions, privileges and recovery settings reviewed?	Account possession and use require their own evidence

ANALYST MAPPING FOR CONTROL PLANNING

T1566
Phishing

FIS source-described pattern; planning interpretation [S9] [S70]

T1190
Exploit Public-Facing Application

FIS source-described pattern; planning interpretation [S9] [S71]

T1078
Valid Accounts

Planning interpretation requiring case-specific evidence [S72]

These terms help organise evidence requests. They should not become a decorative checklist of techniques that the report never observed. An incident team should mark a technique as established only when its own evidence or the cited case source supports it.

7.6 Patch readiness: the October PHP warning

BACS issued an urgent PHP warning on 21 October 2026 for CVE-2026-109618 and CVE-2026-109619. The warning is evidence of an official remediation campaign. It does not establish exploitation at a Swiss organisation [S62].

NVD records describe memory-corruption and request-state weaknesses. They carry the PHP Group's CVSS 4.0 score of 9.2, rather than an independent NVD assessment. The vendor advisories identify the affected and corrected branch versions [S63][S64][S65][S66].

PHP branch	Affected branch versions	Corrected version
8.2	Before 8.2.35	8.2.35
8.3	Before 8.3.36	8.3.36
8.4	Before 8.4.27	8.4.27
8.5	Before 8.5.12	8.5.12

The table lists four branches from the cited release announcement. It does not establish that older releases are unaffected.

The vendor published these security releases on 21 October. Service owners should inventory embedded and hosted installations, then verify the running component after restart or redeployment. A supplier's documented backport can require separate package validation [S67].

Obtain updates through the vendor's established release channel, independently of an unsolicited message.

A version finding should lead to a remediation decision, not a conclusion that data was taken. If exploitation is suspected, preserve the relevant evidence and investigate the affected service. Protective filtering can support a response, but it should not replace validation of the corrected software.

7.7 Politically framed actors

Historical DDoS reporting is useful for availability exercises, while remaining outside this report's 2026 incident total. The NCSC's review of the June 2024 summit attributed DDoS activity to NoName057(16). Its account described limited disruption and separated unrelated technical problems from cyber incidents [S42].

A group's political description is not evidence of state direction. An announcement timed around sanctions, an international meeting or a policy decision does not independently establish why an incident occurred. The operational response should rely on service evidence and established incident responsibilities.

7.8 What would strengthen an actor assessment

For an advertisement, stronger evidence would connect an authentic sample to a relevant system and period. For an access claim, it would establish that an account existed, what privileges it held, and whether unauthorised activity occurred. For a listing, it would include the organisation's own account of service and data consequences.

For an attribution, stronger evidence would connect infrastructure, accounts, tools or operations to a named operator through an accountable source. Shared language or geography is insufficient. Each new fact should strengthen a specific proposition rather than turning an entire persona into a blanket confidence rating.

7.9 Brief update tampering and retrospective evidence

P

CASE P

Backup-software update campaign with reported Swiss impact (R01)

Software supply chain

Vendor-confirmed incident; Swiss victims unnamed

ACCOUNT	Google Threat Intelligence Group and Mandiant report a campaign affecting AOMEI Technology's update infrastructure between April and July 2026. Their account includes Switzerland among countries with affected organisations. AOMEI acknowledges the update-server incident in its own statement. [S103] [S105]
CHRONOLOGY	The vendor's statement was published on 19 October and updated on 30 October 2026. It describes server hardening by 29 July, migration on 5 August and release of Backupper 8.5.1 on 19 October. These are the vendor's dated response statements. [S105]
ESTABLISHED	The researchers describe configuration changes lasting five to ten minutes before legitimate contents returned. They track the activity as UNC7017 and describe CROSSROAD and SHINYROAD malware. The account supports a supplier-update investigation, without establishing a relationship to this report's advertising personas or ransomware brands. [S103]
LIMITS	Swiss organisations are not named. The campaign-wide sector list cannot identify which sectors were affected within Switzerland. This report has no victim-side access or evidence connecting the campaign to its organisation sample. Neither the research nor the vendor statement establishes a state sponsor. [S103][S105]

ALTERNATIVES	The researchers describe opportunistic delivery during short tampering windows. The country list does not establish Switzerland-specific targeting. A legitimate update response observed later cannot resolve what an endpoint received earlier. AOMEI says its assessment of potentially affected users continues. [S103][S105]
RESPONSE	Software and endpoint owners should establish whether the product was used, preserve historical update and endpoint records, and assess the source-described period. Follow the vendor's current incident guidance. Updating the product alone does not replace investigation of possible earlier exposure. [S105]

Bottom line

Assess historical delivery and endpoint activity separately from the supplier's current update response.

The control implication is to preserve evidence across supplier and customer systems. AOMEI's statement explicitly distinguishes updating Backupper from checking whether a device was affected. Closure should therefore address historical delivery, endpoint activity and relevant account exposure separately. No number of Swiss victims can be inferred from these sources. [S105]

KEY TAKEAWAYS

01

Treat ransomware brands, personas and official attributions as different evidence populations.

02

Use technique mappings to request evidence and test controls, without inventing an attack chain.

03

Keep unsupported actor relationships unconnected and political attributions tied to their sources.

CHAPTER 08

The fraud economy: identity, trust and payment

THIS CHAPTER ANSWERS

How can exposed information make a later fraudulent request more convincing?

3

separate decisions: identity, authority and payment

8.1 Personal information is context, not authority 71

8.2 Booking and delivery pretexts turn context into urgency 71

8.3 False bank authority and the offline payment stage 72

8.4 What underground offers establish 72

8.5 Payment-card material in narrow scope 73

8.6 Interrupt the progression at more than one point 74

CHAPTER 08

The fraud economy: identity, trust and payment

IN SHORT

Official warnings show how real personal or booking details can strengthen a false request. The attacker still needs the recipient to trust a message, change access or authorise payment. Underground offers describe potential inputs to that process, rather than completed fraud. Keep payment-card observations narrow and separate from loss figures. Require an independent verification route when an unexpected request contains accurate information.

8.1 Personal information is context, not authority

The 17 November BACS notice describes targeted phishing after a service-provider data leak. The messages reused genuine personal details, including social-insurance identifiers. Their accuracy made the approach more convincing, without establishing that the sender was authorised [S14].

This changes the support-team question. Asking a caller to repeat an address or another exposed detail may confirm that the caller has the information. It does not establish that the caller is the person concerned. A stronger workflow verifies the request through an existing trusted channel and treats changes to that channel as a separate sensitive action.

There are three propositions to preserve. The data may be authentic. The sender may still be fraudulent. The requested action may create a new loss even when the original incident has already been contained. Combining these into a single conclusion can lead an organisation to underestimate follow-on risk.

The pension supplier case adds a service-specific example. An official police warning discusses investment approaches after a pension-service-provider leak. Its mention of salary and pension information supports preparedness for tailored approaches. It does not establish the exact fields taken from every customer of the supplier [S45].

The appropriate response is to prepare member-service teams for convincing information. Give them a safe way to verify a genuine case and a clear route for preserving a fraudulent approach. Avoid making affected individuals repeat sensitive information into a conversation that began through an unexpected channel.

8.2 Booking and delivery pretexts turn context into urgency

The November police warning describes messages that knew accommodation details and booking references. The message asked the recipient to confirm a reservation and then sought payment-card information. Knowledge of a real reservation did not establish that the request came from the booked provider [S43].

The same distinction matters when an apparent delivery message reaches a customer expecting a parcel. A familiar timing pattern can supply a persuasive pretext. BACS's 10 November update discusses fraudulent shops and parcel-themed phishing. The notice supports verification of the seller and the message, rather than a presumption that every delayed delivery is malicious [S13].

For travel, hospitality and retail organisations, the operational question is how a customer can check an unexpected request without using its link or telephone number. The answer should be visible before an incident. A consistent portal, booking record and support route can help customers resolve uncertainty safely.

A provider should also protect the accounts used to send genuine messages. A convincing request might originate from a fraudulent domain, an abused account or another communication path. The message alone does not establish the upstream cause. Preserve that distinction while the investigation proceeds.

8.3 False bank authority and the offline payment stage

The 18 November police warning describes callers impersonating bank staff and using a forged central-bank letter. The fraud sought cash for a supposed safeguarding account. The central bank's claimed involvement was part of the deception, not an established relationship [S44].

This example shows why fraud response must extend beyond the online sign-in. A customer may be persuaded to withdraw cash, move assets or install software. Technical controls on a website do not replace the need for trusted customer verification and an escalation route when a request is unusual.

The source also limits the conclusion. A warning establishes the described method and the authority's concern. It does not provide a national loss estimate or show that every recipient followed the instruction. This report does not infer either from the warning's publication.

Banks and other organisations should give support teams language that is clear enough to interrupt the story. A customer can be asked to end an unexpected conversation and contact the organisation using its established route. Staff should avoid confirming the fraudster's claimed authority through details supplied in the suspicious message.

8.4 What underground offers establish

The retained post material includes advertisements whose language concerns accounts, identities, access and data. Those advertisements can indicate a criminal interest in a product. They do not establish a completed transaction, a verified Swiss issuer, or how a buyer would use the material [S1].

The account-buying advertisement in B11 quoted $8 for one account described by the advertiser as valid. This is a proposed payment, not an observed transaction or a market average [S1].

Example	Advertised amount	Unit	Boundary
Account-buying request, B11	$8	One account described as valid	Payment and account control not verified
Insurance-labelled offer, B01	Not stated in the selected excerpt	Files and contract-related rows	No comparable transaction price established
Contractor offer, B04	Not stated in the selected excerpt	Claimed dataset	Exclusivity claim does not establish a completed sale

An asking price is an advertising term. It can vary with age, scope, claimed exclusivity, verification and seller reputation. A quoted amount should not become a loss estimate or a market average without evidence about completed transactions and comparable products.

The same applies to account and identity descriptions. A seller can describe a fully verified account, a document set or a recovery service. The wording establishes what is offered. It does not establish that the account exists, that verification was lawful, or that the buyer obtained control.

For defenders, the first decision is whether the claim concerns an account, customer or service they own. The next is whether there is corroborating activity. Only then can the organisation decide whether account intervention, fraud controls, customer support or a wider incident response is proportionate.

8.5 Payment-card material in narrow scope

SCOPE OF THE CARD FIGURES

These observations cover only payment cards that appeared in clear text in the dark-web posts retained for this report. Brandefense detects stolen cards through other methods that are outside this section. These observations do not measure card theft, active cards, fraud loss or total Brandefense coverage.

The retained population contains 164 distinct Swiss-associated cards visible in clear text, across 165 posts. This is the narrow population described above [S4].

A post may label a card as working or show an apparent checker response. Such text remains the poster's representation. It is not an issuer-authorised test and does not establish a completed charge. The report does not publish personal details, card numbers or actionable card material.

An issuer receiving a relevant external signal should validate it through its established internal process. The decision to contact a customer, restrict an account or replace a card depends on issuer evidence. A small retained post population cannot establish that cards are either a major or minor source of national financial loss.

8.6 Interrupt the progression at more than one point

The progression below is an **analytical model** for control planning. It does not establish a common operator behind the cited warnings or the retained advertisements.

Stage	Possible abuse	Decision point	Owner
Information	Real personal or booking details appear in a message	Verify the sender's authority separately	Customer support
Persuasion	Urgency or a trusted institutional role is asserted	End the unexpected contact and use the established route	Recipient and support
Identity	A caller requests a reset or change of recovery details	Require independent verification of the sensitive change	Identity operations
Payment	A new payee, cash withdrawal or card action is requested	Apply the institution's transaction and fraud review	Fraud operations
Aftercare	The recipient reports an attempted or completed fraud	Preserve the evidence and assess further exposure	Incident and customer teams

The model creates several opportunities to act. A person might already have disclosed information but still be able to stop a payment. A service provider might have restored systems but still need to prepare customers for tailored messages. An institution should therefore avoid treating the initial incident's technical closure as the end of fraud support.

KEY TAKEAWAYS

01

Verify authority separately from the accuracy of personal or booking details.

02

Treat advertised prices and checker labels as claims, without inferring sales or losses.

03

Give customers and support staff a trusted route that does not depend on the suspicious message.

CHAPTER 09

Banking deep dive

09

THIS CHAPTER ANSWERS

Which banking decisions connect identity, fraud, suppliers and supervision?

40

banking and finance candidates in the selected universe

9.1 Measured banking and issuer populations 76

9.2 Banking secrecy is not a cyber-risk inference 77

9.3 Connect identity and fraud evidence without collapsing the cases 77

9.4 Supplier detection can start the supervisory assessment 77

9.5 A banking exercise grounded in the cited warnings 78

CHAPTER 09

Banking deep dive

IN SHORT

The 40 selected banking and finance organisations record at least 16,082 device associations and 1,055,051 historical credential associations. Credentials associated with 7 were listed for sale when checked. These are observations, not affected customer totals or confirmed bank intrusions. The issuer-matched subset and narrow card population answer separate questions. Assign identity, endpoint and fraud teams to validate each relevant signal through authorised records.

9.1 Measured banking and issuer populations

The selected universe includes 40 banking and finance candidates. This is a purposive cell, rather than a complete list of licensed banks or a representative sample. Principal domains do not define every subsidiary, customer portal or outsourced function [S3].

Observation	Count
Banking and finance organisations assessed	40
Organisations with current listings	7
Device associations, at least	16,082
Employee-classified device associations	236
Historical credential associations	1,055,051

The issuer-matched subset contains 6 organisations from that banking cell. It records 4 with current credential listings, 5 with employee-classified device associations and 6 with associations outside that classification [S3][S4].

Across that subset, the snapshot contains 208 employee-classified and 12,924 other device associations. The retained post population attributes 7 distinct clear-text card observations to these issuers. These are overlapping populations with different meanings, not affected customer or fraud-loss totals.

A card observation does not establish an intrusion into its issuer. A device association does not establish ownership, current infection or whether a banking account remains active. Validate each signal through the issuer's authorised identity, endpoint and fraud processes.

Official fraud notices remain source-specific examples [S14][S44][S45]. Use them to test trusted verification and transaction escalation. Keep passive configuration checks separate from the national Atlas headline and account investigations.

9.2 Banking secrecy is not a cyber-risk inference

This report takes no position on banking secrecy or government policy. It does not infer a bank's security posture, attacker interest or incident cause from a legal or political description of the financial sector. The evidence concerns specific claims, official warnings and selected control observations.

For a bank, the operational question is which information can authorise access or a transaction. A caller's knowledge of a customer's address, pension history or another private detail should not automatically establish authority. The cited warnings show why accurate context and a fraudulent instruction can appear together [S14] [S44][S45].

Staff need a usable route for checking authority without relying on information provided by the caller. The process should cover a customer requesting an urgent action, an apparent manager asking for an exception, and a purported supplier reporting an incident. Each requires a different confirmation path and accountable owner.

9.3 Connect identity and fraud evidence without collapsing the cases

An identity alert can establish a suspicious sign-in without establishing a fraudulent transfer. A payment alert can establish an unusual transaction without showing that the customer's online account was used. An information leak can make a call more persuasive without providing access to the bank's systems.

A shared incident record should preserve those distinctions. Identity operations can record sessions, recovery changes and application access. Fraud operations can record the requested beneficiary, approval path and transaction state. Customer support can preserve the communication and explain how the customer was approached.

This shared view helps teams choose a proportionate response. Revoking sessions addresses one access path. Reviewing a new beneficiary addresses another. Helping the customer verify a message addresses a third. No single action establishes that the entire problem has been resolved.

9.4 Supplier detection can start the supervisory assessment

FINMA's guidance makes outsourced functions part of the institution's incident responsibility. For the described reporting obligation, the relevant timing can begin when the institution or its service provider identifies the attack. The institution cannot assume that its own later management meeting starts the clock [S8].

FINMA's 2025 Risk Monitor states that reports concerning attacks on third parties covered around 47% of cyber incidents reported to FINMA in its stated period [S109]. That supervisory benchmark explains why outsourcing exercises matter across the financial sector, without implying a supplier-incident rate for the 40 selected banking and finance candidates [S3][S109].

Test the first supplier message as a practical exercise. It should identify the affected function, discovery time, known effects, uncertainty and a contact able to provide updates. The institution's compliance and incident teams should be able to assess reportability while technical investigation continues.

The institution should also keep its supervisory notification distinct from other duties. A personal-data risk assessment and a critical-infrastructure assessment have their own triggers. A form forwarded through one channel does not automatically complete every required notification. Chapter 10 sets out the relevant differences [S6][S7][S8].

9.5 A banking exercise grounded in the cited warnings

Use a scenario in which a customer receives a call referencing a real service-provider incident and accurate personal details. The caller asks for an urgent protective transfer or cash movement. The exercise should test support, fraud and identity teams together [S14][S44][S45].

The customer-support completion evidence is an independently verified contact route. The fraud-team evidence is a recorded decision about the requested transaction. The identity-team evidence is an assessment of account access and recovery changes. The communications evidence is a clear message explaining what the institution knows.

A second scenario can start with an outsourcing provider's cyber alert. Require the service owner to identify the affected banking function and the continuity arrangement. Require compliance to record which reporting obligations apply. Require infrastructure to demonstrate restoration independently of the affected provider's production access.

The result should be a set of demonstrated decisions, not a declaration that the bank is secure. An exercise can reveal a missing contact, an unclear trigger or an unavailable recovery account. Those are actionable findings with owners and closure evidence.

KEY TAKEAWAYS

01

Keep identity, transaction and data-exposure findings distinct within a shared case record.

02

Test the first supplier alert against the institution's own reporting responsibilities.

03

Use trusted verification and independent recovery as demonstrable banking controls.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which Swiss reporting duties apply, when do their clocks start, and what should an organisation prepare?

24 h

initial critical-infrastructure report after discovery, where the duty applies

10.1 Three duties that can apply to one incident 80
10.2 Critical infrastructure: establish scope before the incident 81
10.3 Personal data: assess harm to people 81
10.4 Financial institutions: keep supplier discovery in the clock 82
10.5 A proposed Cybersecurity Act is not an enacted duty 83
10.6 Prepare one evidence record and several decisions 83

CHAPTER 10

Regulatory and national response

IN SHORT

Switzerland has separate reporting duties for critical infrastructure, personal data and supervised financial institutions. Their scope, clocks and completion requirements differ. The critical-infrastructure duty is already in force. The proposed Cybersecurity Act is future legislation, with a consultation draft requested for June 2027. Build one incident record that supports each applicable duty, and assign someone to submit timely initial reports while facts remain incomplete.

10.1 Three duties that can apply to one incident

One technical incident can require several legal assessments. The Information Security Act concerns cyberattacks on covered critical infrastructure. Article 24 of the Federal Act on Data Protection concerns data security breaches and risks to people. FINMA's guidance concerns material cyber incidents at supervised institutions [S6] [S7][S8].

These duties have different triggers. They should share an incident record without being treated as interchangeable. The legal owner must document why a duty applies, why it does not apply, or which facts are still needed. This chapter summarises the cited official guidance and is not legal advice.

The table separates the decision that starts each workstream from its principal reporting requirement.

Regime	Applicability decision	Initial requirement	Further requirement
Information Security Act and Cybersecurity Ordinance	Covered critical infrastructure and a reportable cyberattack	Report to NCSC within 24 hours of discovery [S6]	Complete the report within 14 days; these are calendar days [S12]
Federal Act on Data Protection, Article 24	First establish applicable law and supervisory authority [S106]. Under FDPIC jurisdiction, assess a data security breach likely to result in high risk to affected people's personality or fundamental rights	Controller notifies FDPIC as soon as possible [S7]	Inform affected people when necessary for their protection or when FDPIC requires it [S7]
FINMA Guidance 05/2020, clarified by 03/2024	Supervised institution and incident meeting the reporting criteria	Initial notice within 24 hours [S8]	Full notification within 72 hours through FINMA's reporting platform, subject to the guidance's clock rules [S8]

The financial-sector clock needs particular care. FINMA counts the 24-hour and 72-hour periods on official bank working days. Attacks classified as severe are an exception: the initial report is required within 24 hours even outside bank working days [S8]. A single simplified deadline in an incident playbook would miss this distinction.

10.2 Critical infrastructure: establish scope before the incident

The NCSC identifies the Information Security Act and Cybersecurity Ordinance as the legal basis for the reporting obligation [S6]. Its scope includes covered authorities and organisations, with examples such as energy, drinking water, transport, and cantonal or communal administrations. The ordinance contains exceptions [S6]. Do not assume that sector membership alone resolves every organisation's status.

The NCSC says it can determine whether an interested authority or organisation is subject to the duty. The organisation can request a decision where its position is unclear [S12]. That is a concrete preparation task for the legal and continuity owners. Record the answer, the services considered and the contact responsible for reassessment.

The reportable event also needs assessment. Official guidance includes attacks that threaten critical-infrastructure functioning, manipulate or disclose information, remain undetected for a longer period, or involve blackmail, threats or coercion [S12]. An attack on information technology is not excluded simply because operational technology continues functioning.

Conversely, the NCSC says a DDoS attack against a noncritical application does not automatically create a reporting duty. The decisive question is whether critical-infrastructure operability is jeopardised [S12]. The response record should therefore state the business function affected, rather than only listing technical symptoms.

An incomplete investigation does not suspend the initial deadline. The NCSC requires an initial report within 24 hours even when the full information is unavailable. Additional information can complete the report within 14 calendar days [S12]. Record confirmed facts, uncertainty and the next update owner.

The duty began on 1 April 2025. Sanctions provisions took effect on 1 October 2025, with possible fines up to CHF 100,000 [S60]. This is not an automatic fine for every late report. The official account describes contact with the operator, a subsequent order, and a possible criminal complaint if the operator still does not respond [S60].

10.3 Personal data: assess harm to people

First establish the applicable data-protection law and supervisory authority. FDPIC supervises private parties and federal bodies. Cantonal and municipal authorities should assess their applicable cantonal requirements and supervisory authority [S106].

The FDPIC's guidance defines a data security breach through accidental or unlawful loss, deletion, destruction, modification, disclosure or access to personal data [S7]. A breach need not involve a public leak. Availability and integrity can matter as well as confidentiality.

The controller must notify the FDPIC as soon as possible when the breach is likely to result in high risk to people's personality or fundamental rights [S7]. This is not a universal Swiss 72-hour deadline. The assessment must consider the affected information and its consequences for the people concerned.

The guidance warns against waiting in a situation of doubt where high risk cannot sufficiently be excluded. Planned measures do not remove the reporting question. The controller should document what is known, the basis for the risk assessment and the protective steps already supported by evidence [S7].

Notification to the authority and information to affected people are separate decisions. Article 24 requires information to individuals when necessary for their protection, or when the FDPIC requests it [S7]. A customer message should explain the relevant facts and protective action without reproducing exposed information.

This distinction is useful for a claim involving old customer data. The advertisement's date does not establish when the data was accessed. The organisation should establish whether the records are authentic and what protective action people need. The legal assessment should follow the evidence, rather than the seller's description.

10.4 Financial institutions: keep supplier discovery in the clock

FINMA's guidance expects an initial assessment of criticality within the initial reporting period [S8]. If the institution must choose between completing that assessment and meeting the deadline, it should prioritise the deadline. The initial report can later be withdrawn if investigation shows the reporting criteria were not met.

For outsourced functions, the reporting period begins when either the institution or its provider identifies the cyber incident [S8]. The contract and escalation process must therefore bring the provider's discovery time into the institution's incident record. Waiting for a final supplier report can leave the institution without the information needed for its own duty.

The guidance also addresses providers that are not material outsourcing partners. Institutions must ensure they receive information about relevant provider cyber incidents and assess their own reporting duty [S8]. A supplier register limited to the largest contracts can miss an operational dependency.

Institutions also covered by the Information Security Act can use the NCSC form to forward their initial notification to FINMA, provided timely transmission is assured. The full 72-hour notification must still go through FINMA's survey and application platform [S8]. Keep proof of delivery for each required submission.

The reporting process should be exercised alongside recovery. FINMA's guidance calls for scenario-based cyber exercises and distinguishes the expectations for systemically important and other institutions [S8]. Its February 2026 account also highlights incomplete institution-specific scenarios, unclear responsibilities and insufficiently tested response processes [S61].

For a bank, a useful exercise combines a provider outage, uncertain customer-data access and a weekend discovery. The objective is to produce the required initial decisions without waiting for a complete forensic account. The exercise should also test who can approve customer communications and how critical services continue operating.

10.5 A proposed Cybersecurity Act is not an enacted duty

On 25 September 2026, the Federal Council instructed the DDPS to prepare a consultation draft for a standalone Cybersecurity Act by June 2027 [S11]. The announcement covers proposed requirements for digital products, important digital data, and hosting or cloud services. It also proposes transferring the existing critical-infrastructure reporting duty into the new legislation.

The announcement describes legislation under development. It does not establish that those proposed duties were already in force at this report's cut-off. The source states that existing sector-specific rules remain in force [S11]. Record the proposal as a watch item with a legal owner, rather than an operational deadline that already applies.

The proposal references the EU Cyber Resilience Act as a model for product rules [S11]. This does not make every EU cybersecurity duty a domestic Swiss duty. International groups should assess each legal entity, service and applicable jurisdiction. The report takes no position on the policy choice or Switzerland's relations with the European Union.

10.6 Prepare one evidence record and several decisions

The following preparation tasks turn the separate regimes into a process that can run during uncertainty.

Preparation	Owner	Completion evidence
Resolve critical-infrastructure status and applicable exceptions	Legal and continuity lead	Written applicability record and reassessment date
Record incident discovery at the institution and relevant providers	Incident commander	Time-stamped event record with uncertainty explained
Assess affected people and likely harm	Privacy lead	Documented risk assessment and notification decision
Prepare initial reports with incomplete facts	Legal and security lead	Tested templates and named submitter with a deputy
Confirm reporting channels and delivery evidence	Compliance lead	Exercised access and retained confirmation
Exercise provider failure with business owners	Continuity lead	Tested alternative process, recovery evidence and assigned fixes

The incident commander should keep observations separate from conclusions. An actor claim, a service outage, confirmed unauthorised access and confirmed data disclosure can enter the record at different times. Each can change the legal assessment. The record should show who made the decision and what evidence supported it.

KEY TAKEAWAYS

01

The critical-infrastructure duty is already in force: report within 24 hours where applicable and complete the report within 14 calendar days.

02

FDPIC and FINMA duties have separate triggers and clocks; provider discovery can start the financial-sector reporting period.

03

The proposed Cybersecurity Act remains a legislative watch item; prepare current obligations and monitor the consultation draft.

CHAPTER 11

Outlook

11

THIS CHAPTER ANSWERS

Which evidence should change the next security decision, and what would change this assessment?

5

conditional judgements with explicit limits and response signals

11.1 Key judgements 86
11.2 What would change the assessment 87
11.3 Conditional scenarios 87
11.4 A review rhythm tied to decisions 88

CHAPTER 11

Outlook

IN SHORT

Plan for data extortion, identity abuse, supplier disruption and targeted information collection. The evidence does not provide attack probabilities for an individual Swiss organisation. Official assessments and observed claims serve different purposes. The scenarios below turn them into decisions with owners and evidence that would change the plan. Revisit each judgement when new organisational evidence arrives.

11.1 Key judgements

The judgements concern planning priorities. Confidence describes the stated proposition, rather than an actor's reliability or an organisation's likelihood of being attacked.

Judgement	Confidence	Basis and limit	Decision signal
Extortion warrants tested business recovery	High for the preparation need	The report records ransomware listings, while the FIS identifies ransomware risk to critical infrastructure [S2] [S9]. Listings do not confirm individual incidents	Corroborated access, impaired recovery or a relevant supplier incident
Sensitive research and policy information require persistent-access controls	High for the source assessment	FIS identifies these information targets and describes phishing and network-device exploitation [S9]. No attack probability follows	Unexplained access, external sharing or suspicious contact involving sensitive work
Supplier discovery must reach the incident commander quickly	High for the reporting dependency	FINMA's outsourced-function clock can begin at provider discovery [S8]. Applicability depends on the institution and incident	Provider identifies a cyber incident involving an outsourced function
Public events justify continuity readiness	Moderate for the planning scenario	FIS identifies event-related overload risk, and the 2024 summit provides historical context [S9][S10]. This does not establish a new campaign	Relevant actor claims combined with service anomalies or provider warnings
Reporting readiness can improve before every incident fact is known	High for the preparation need	Official guidance permits initial reports followed by fuller information [S8][S12]. The legal trigger still needs assessment	A potentially reportable incident with incomplete technical facts

The first question is whether the evidence concerns your service. A national warning can justify a readiness check. It cannot establish that a specific account is active, that a data offer is genuine, or that an affected supplier holds your records. Those propositions need organisational evidence.

The priorities also differ by business. A research institution may put external project access first. A payment provider may prioritise customer-account protection and third-party escalation. A public-service operator may need a tested manual process before a highly visible event. The same national context can support those different choices.

11.2 What would change the assessment

The table identifies evidence that warrants a change in response. It also specifies evidence that would narrow the concern, avoiding a permanent emergency posture after an unverified claim.

New evidence	Change in response	Evidence that narrows concern	Owner
A current, valid account appears in relevant exposure evidence	Investigate the account, sessions and access history; contain according to findings	Account already disabled, information obsolete, or no supported link to the organisation	Identity and incident-response teams
A supplier confirms access to a tenant holding organisational information	Establish affected scope, reporting clocks and continuity options	Evidence that the relevant tenant, data and administrative paths were unaffected	Supplier owner and legal lead
A data sample matches controlled internal records	Start a documented investigation and privacy-risk assessment	Evidence of a previously remediated disclosure or public information, with residual risk assessed	Data owner and privacy lead
A relevant public website becomes unavailable during an actor campaign	Confirm service impact and activate provider escalation	Internal and provider evidence identifies an unrelated fault	Service owner and communications lead
Unusual activity reaches a sensitive research or policy workspace	Preserve evidence and examine access persistence and sharing	Authorised activity confirmed by the information owner and supporting records	Information owner and security team

None of these signals requires immediate public attribution. Establish service impact, access and data scope first. Attribution can remain unresolved while the organisation contains harm and meets reporting duties. Communications should retain the same uncertainty as the investigation.

11.3 Conditional scenarios

First conditional scenario: a supplier's service fails during a data-extortion claim. This is a planning assumption. If the supplier supports a critical business process, activate the agreed continuity process while assessing whether organisational information was accessed. Assign a business owner to service restoration and a separate owner to the data question.

The first evidence requirement is the supplier's discovery time and the systems it can confirm are affected. For financial institutions, assess the outsourced-function reporting rule without waiting for the supplier's final investigation [S8]. For other covered critical services, assess operability and the applicable reporting trigger [S12]. The exercise closes when the business process works through its approved alternative and outstanding risks have owners.

Second conditional scenario: an actor cites a political issue and names a public service. The actor's explanation remains its own. If the service experiences anomalies, verify them with the provider and business owner. Preserve the claim as evidence without repeating slurs or adopting its position. Use a statement that reports the organisation's verified service impact.

The historical summit review shows why separate explanations matter: the NCSC distinguished DDoS, intrusion attempts, phishing and unrelated technical problems [S42]. The scenario should test that separation. It closes when the service owner can explain the interruption, record the recovery and state what remains unverified.

Third conditional scenario: a sensitive project receives convincing external contact. The FIS describes tailored messages and messaging-application approaches among espionage techniques [S9]. If a suspicious contact involves an actual research or policy project, verify the sender through an established channel. Review any associated authentication, sharing or software installation evidence.

The information owner should decide which project material needs additional access restrictions. The security team should look for access beyond the initial message. The scenario closes when the contact is resolved and any affected account or sharing route has a documented disposition. A convincing invitation alone does not establish a successful intrusion.

Fourth conditional scenario: an old dataset is advertised as a new incident. Treat the advertisement date and access date as separate. If the material appears relevant, compare it against retained incident information through authorised processes. Explain to customer-facing teams how genuine old details can support convincing fraud.

The action changes if records indicate a new access period or a newly affected system. The privacy lead should reassess risk when new facts emerge. If the offer instead concerns an already remediated disclosure, record that conclusion and the continuing fraud precautions. Do not describe recirculation as proof of a new incident.

11.4 A review rhythm tied to decisions

Assign a review owner for each judgement and include it in the existing risk process. Update the owner when the underlying service or supplier changes. A new count of posts or listings should prompt an evidence review, rather than an automatic escalation in business risk.

The national Atlas headline describes the assessed portfolio, while sector signal counts and passive observations support different validation tasks. Use the documented service, information and supplier dependencies to sequence work. Reassess priorities when account validity, relevant activity or service impact is established [S3].

The most useful sign of progress is completion evidence. A restored service, removed obsolete access, tested reporting channel or resolved supplier dependency changes what the organisation can do during an incident. An expanding list of alerts does not establish that those outcomes improved.

KEY TAKEAWAYS

01

Treat the outlook as conditional planning; the report does not estimate an organisation's attack probability.

02

Change the response when evidence confirms relevant access, affected information or service impact, while keeping attribution separate.

03

Review priorities with accountable owners and completion evidence, especially where recovery depends on a supplier.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

Who acts next, and what evidence demonstrates completion?

3

implementation periods with named owners

12.1 Actions for the next planning cycle 91
12.2 Identity and incident response 93
12.3 Service owners and suppliers 93
12.4 Fraud and banking teams 93
12.5 Legal and communications 94
12.6 How Brandefense can help 94

CHAPTER 12

Action plan

IN SHORT

Turn the report into work that can be demonstrated. Begin with account validation, supplier contacts and the notification decision tree. Then exercise isolation, communications and recovery. Finally, test that the business can operate through an essential service disruption. Each action needs an owner, an activating condition and evidence of completion. Assign responsibility before buying another source of alerts.

12.1 Actions for the next planning cycle

The periods below are planning targets. They do not replace a statutory clock that may already be running during an incident.

30 days

If a new credential or access offer matches an organisation account, validate status and recent activity

OWNER
Identity operations

COMPLETION EVIDENCE
Disposition with account status, relevant sessions, action and unresolved facts

If an essential supplier handles sensitive data, verify its incident contact and initial-notice route

OWNER
Procurement and service owner

COMPLETION EVIDENCE
Contact test and data-to-service dependency record

If an event could affect essential operations, assess critical-infrastructure reporting criteria

OWNER
Incident commander and legal

COMPLETION EVIDENCE
Trigger decision, discovery time and named reporting owner

If personal data may be affected, assess likely risk to individuals independently of service impact

OWNER
Privacy officer

COMPLETION EVIDENCE
Documented risk assessment and notification decision

If a financial institution uses an outsourced function, confirm who starts the supervisory reporting assessment

OWNER
Compliance and outsourcing owner

COMPLETION EVIDENCE
Rehearsed provider-to-institution alert with recorded timing

260 days

If helpdesk staff can reset sensitive access, test a separate-channel verification process

OWNER

Identity and support leads

COMPLETION EVIDENCE

Exercise showing an impersonation attempt was refused or safely escalated

If a customer incident notice could be imitated, prepare a trusted verification route

OWNER

Fraud and communications

COMPLETION EVIDENCE

Published contact route and tested call-centre script

If a public service faces politically framed claims, rehearse service checks and mitigation activation

OWNER

Operations and communications

COMPLETION EVIDENCE

Exercise timeline separating announcement, availability and verified impact

If a processor incident affects several business units, practise a shared evidence and decision record

OWNER

Privacy and service owners

COMPLETION EVIDENCE

Tabletop record with a separate conclusion for each affected data population

390 days

If an essential service cannot operate without its main identity platform, test an independent restoration route

OWNER

Continuity and infrastructure

COMPLETION EVIDENCE

Business-approved restoration with separate recovery credentials

If recovery requires a supplier, test the supplier's role alongside internal restoration

OWNER

Continuity and procurement

COMPLETION EVIDENCE

Joint exercise showing access, data validation and hand-back responsibilities

If external claims recur, review whether closed cases have been reopened consistently

OWNER

Threat intelligence and incident response

COMPLETION EVIDENCE

Sampled decisions showing why repeated offers were closed or escalated

12.2 Identity and incident response

Start with the identities that can change other identities. Helpdesk operators, delegated administrators and recovery accounts can alter the outcome of a phishing event. A strong sign-in process loses value if a persuasive caller can replace its recovery factor.

Test the actual support workflow. Have an authorised exercise request an urgent reset using a plausible manager identity and accurate organisational details. The completion evidence is a safe refusal or escalation through an independently verified contact. A reminder email to staff is not equivalent evidence.

When unauthorised activity is established, preserve the relevant records before access changes erase context. Review sessions, application permissions, mailbox rules and recovery factors as applicable. A password change alone may leave another path available. The incident owner should record which paths were checked and which remained outside visibility.

An intelligence team should also maintain a clear response to weak signals. A dataset title can refer to a historic incident, a public directory or an unrelated organisation with a similar name. Document the alternative, then record what additional evidence would justify reopening the case.

12.3 Service owners and suppliers

Map important business outcomes to the systems, accounts and providers that enable them. For a public application, include alternative submission and verification arrangements. For health services, include clinical access and data validation. For financial services, include payment approval, customer support and reconciliation.

A useful supplier exercise starts with an incomplete notice. The provider knows that access was unauthorised but has not determined whether data left its environment. Ask the service owner to identify affected workflows without filling that uncertainty with an attacker claim.

Then test the next message. Can the provider explain what evidence changed, which customer population it concerns, and whether the data types are confirmed or provisional? The customer's incident team should be able to update its own assessment without silently expanding the supplier's conclusion.

Keep recovery evidence separate from confidentiality evidence. A functioning service does not establish that data remained private. Conversely, an unverified data allegation does not establish that the organisation's operations have stopped. Business and privacy owners need separate facts and separate decisions.

12.4 Fraud and banking teams

Use the official examples of impersonation and follow-on phishing to test customer-facing procedures. A caller who knows a person's address, social-insurance identifier or recent provider incident may still be fraudulent. Accurate personal data should help locate a case, not authorise a payment or an authentication change.

Contact-centre staff need an approved way to move a conversation to a trusted route. A customer should not have to follow a link in an unexpected message to check whether the warning is genuine. The organisation can make this easier through consistent notices and a clear verification page reached independently.

Fraud teams should agree when to pause a transaction and when to involve incident response. Identity abuse, payment fraud and exposure of personal information can coexist, but they remain different findings. The case record should preserve which evidence supports each conclusion.

An issuer should validate any external card signal within its own controlled environment. A post's label or apparent checker response is not a reason to publish account details or announce customer loss. Reissue and customer-contact decisions belong to the issuer's established fraud and incident process.

12.5 Legal and communications

Prepare a decision tree that records the trigger for each reporting duty. Include who first discovered the incident, what essential operations were affected, what personal-data risks are likely, and which supervisory requirements may apply. Preserve the basis for deciding that a duty does or does not apply.

Give communications the same evidence boundaries as the incident team. A useful holding statement can identify a service issue, an investigation and alternative customer arrangements without repeating an unverified actor volume. Later statements should say what has changed and which facts remain uncertain.

Political wording should receive the same discipline. Describe a group's stated motive only when it helps the reader understand the claim. Attribute it to the group or the cited authority. Avoid reproducing slogans or treating the timing of a government decision as proof of sponsorship.

12.6 How Brandefense can help

Brandefense brings Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management into the same platform [S73]. For the decisions in this report, the useful connection is between an external signal, the organisation's assets and an accountable validation step.

Use threat intelligence to preserve and assess claims. Use digital-risk work to understand abuse of brands and trusted communications. Use external asset visibility to identify who owns a service and where a configuration finding should be checked. None replaces internal incident evidence or the organisation's reporting assessment.

Ask for a Brandefense demonstration using an operational question from this report: how a new claim reaches the right owner and receives a recorded disposition. Product scope and service arrangements should be confirmed in that discussion.

KEY TAKEAWAYS

01

Give every action an owner, activating condition and demonstrable completion evidence.

02

Exercise suppliers, identity recovery and business restoration together.

03

Keep legal deadlines and public statements tied to their own triggers and facts.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

How should the evidence be interpreted and traced to its source?

4

appendices for scope, evidence, sources and terms

Appendix A. Scope, sources and confidence 97
Appendix B. Evidence register 99
Appendix C. Sources 101
Appendix D. Glossary 106

Appendix A. Scope, sources and confidence

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

A.1 Window and timestamp meaning

The report window is 1 January–22 November 2026. Underground material is dated by the time of the post, rather than the time a reader encountered it. The recent-activity section covers 9–22 November. An older incident discussed in a new post remains an older incident unless evidence establishes a new event.

The data and source readings reflect what was available at collection. The cut-off day was still in progress during preparation. Later material published on that date may require an update. The report does not infer an absence of activity from a missing observation.

Passive observations have their own collection-time meaning. They do not establish that the same configuration existed throughout the reporting window. Ransomware listing dates likewise do not establish an intrusion date. Official notices can describe an earlier event or revise an initial estimate.

Post figures include material dated through 07:20 UTC on 22 November 2026. The requested cut-off day remains open.

A.2 Source populations

The report uses retained dark-web posts collected by Odin by Brandefense, public ransomware listings, passive DNS and TLS observations, web-security observations, and public reporting. Each contributes a different kind of evidence [S1][S2][S3].

A post records an advertisement, request, announcement or discussion. It does not establish the authenticity of a dataset, current account access or completion of a transaction. Repeated offers can describe the same alleged material. Advertised lines, records, accounts and people are different units.

A ransomware listing records a criminal claim associated with an organisation and group label. It does not independently confirm encryption, data removal, payment or a unique victim. The authority's ransomware cases are a separate population, with its own reporting and observation basis [S2][S5].

Official reporting establishes what the named organisation or authority disclosed. It does not give this report access to internal forensic evidence. Where a source says a question remains unresolved, the case card and takeaway preserve that uncertainty.

A.3 Organisation selection and missing measures

The selected universe contains 250 organisation candidates across thirteen sector cells. It is purposive and includes some related corporate entities and public bodies sharing a parent domain. It is not a national ranking or a statistically independent sample [S3].

Passive checks cover 246 of the 250 selected candidates (omitting four candidates across banking and finance, public administration, education and research, and healthcare) and keep inconclusive observations separate from failures.

Exposure observations have separate coverage across 247 of the 250 selected candidates, omitting three candidates across energy and utilities, transport and logistics, and business and consumer services. The four passive omissions and three exposure omissions do not overlap, leaving 243 candidates in both populations. The national Atlas headline is 48 out of 100 for the assessed portfolio. Only the national Atlas figure is published. Device and credential associations can overlap across organisations and dates; they do not count unique people or confirmed incidents [S3].

A.4 Card scope

Payment-card observations cover only material that appeared in clear text in retained dark-web posts. Brandefense detects stolen cards through other methods outside this section. These observations do not measure card theft, active cards, fraud losses or total Brandefense coverage [S4].

The card population must not be added to credential, device or person counts. A poster's apparent checker result remains a claim. Any account intervention requires validation through the issuer's established process.

A.5 Confidence and alternative explanations

Confidence attaches to a proposition. The report can be confident that an advertisement was observed while remaining unable to establish its authenticity. It can be confident that an organisation disclosed an incident while the final population and data scope remain unresolved.

An actor alias is not a verified person. Shared language, hosting country, a similar title or political rhetoric does not establish common control. A relationship is stated only at the level its evidence supports. A planning sequence without an established operational link is labelled an analytical model.

Conditional scenarios in Chapter 11 are planning assumptions. They identify the evidence that would strengthen or weaken the judgement. They are not quantified probabilities of an attack or promises about control effectiveness.

A.6 Public naming and neutrality

Organisations are named in incident accounts only where official confirmation and wider reporting support the case. Other targets and third parties use broad role labels. Where a third-party article link would disclose a withheld organisation, the public source entry uses the publisher's site root and withholds the article URL. Where the publisher itself is the withheld organisation or authority, the entry identifies the publisher by role and omits the URL.

The report takes no position on government decisions, banking secrecy, sanctions, EU relations or international meetings. State and actor attributions remain those of their cited sources. Actor slogans and loaded descriptions are omitted.

Appendix B. Evidence register

The register points to the evidence shown in the chapters. Card IDs remain the same in every edition. A card's presence establishes the retained material, rather than the truth of its claim.

Card	Date	Venue	Alias	Language	Chapter
B01	2026-05-04	Data-sharing forum	NormalLeVrai	English	4
B02	2026-03-10	Forum reply quoting an offer	john2samira, quoting Niphra	English	4
B03	2026-03-10	Forum discussion	jb75	English	4
B04	2026-11-05	Data-sale forum	pfavre	English	4
B05	2026-10-11	Data-sharing forum	updap	English	4
B06	2026-01-06	Buyer request on a forum	xmrlover76	English	4
B07	2026-01-27	Credential-sharing forum	thejackal101	English	4
B08	2026-11-07	Data-sale forum	RummRif	English	4
B09	2026-01-18	Data-sharing forum	Cod3xx	English	4
B10	2026-01-30	Data-sharing forum	hexvior	English	4
B11	2026-04-17	Account-buying forum	kleinanzeige	Russian and English	4
B12	2026-11-19	Forum announcement	Jlkrumholz01	English	4

The following register records official case cards separately from underground post cards. Official disclosures and criminal advertisements must not be merged into one incident count.

Card	Date	Subject	Evidence	Chapter
O01 / Case F	2026-11-20	Cantonal permit records	Official account; limits in case card	5
O02 / Case G	2026-04-30	Radiology continuity	Official account; limits in case card	5
O03 / Case H	2026-10-23	Pension software supplier	Official account; limits in case card	5

Card	Date	Subject	Evidence	Chapter
O04 / Case I	2026-09-28	Historical media staff information	Official account; limits in case card	5
O05 / Case J	2026-07-15	Utility contractor records	Official account; limits in case card	5
O06 / Case K	2026-11-12	Refrigeration controls	Official account; limits in case card	5
O07 / Case L	2026-08-04	Federal collaboration accounts	Official account; limits in case card	5
O08 / Case M	2026-10-26	Education IT support platform	Official account; limits in case card	5
O09 / Case N	2026-04-11	Adult education data scope	Official account; limits in case card	5
O10 / Case O	2026-11-19	University online forms	Official account; limits in case card	5
R01 / Case P	2026-10-19	Backup-software update campaign	Vendor statement and primary research; Swiss victims unnamed	7

Appendix C. Sources

Source numbers that do not appear were retired during review and are not cited. External source pages and the supporting passages were read during preparation. Verification dates describe that reading, not a guarantee that a page will remain unchanged. Own-source entries identify the population used by this edition.

S1: Odin by Brandefense. Odin by Brandefense retained Switzerland-related post material, post window 1 January–22 November 2026 through 07:20 UTC. Own-source population. Verified on 22 November 2026.

S2: Brandefense. Ransompedia listing snapshot for Switzerland and regional peers, collected 22 November 2026. Own-source population. Verified on 22 November 2026.

S3: Odin by Brandefense. Selected organisation universe, Atlas exposure observations read 21–22 November 2026, and passive DNS, TLS and web-security observations collected 22 November 2026. Own-source population. Verified on 22 November 2026.

S4: Brandefense. Clear-text payment-card aggregates from the retained post population. Own-source population. Verified on 22 November 2026.

S5: Federal Office for Cyber Security. First semi-annual cyber report 2026. https://www.bacs.admin.ch/en/hjb-26-1-en. Verified on 22 November 2026.

S6: Federal Office for Cyber Security. Reporting obligation for cyberattacks on critical infrastructure. https://www.bacs.admin.ch/en/reporting-obligation. Verified on 22 November 2026.

S7: FDPIC. Guidelines on reporting data security breaches and informing affected persons under Article 24 FADP. https://www.edoeb.admin.ch/dam/en/sd-web/T64CAUyvAMcF/1_2%20Leitfaden%20des%20ED%C3%96B%20betreffend%20der%20Meldung%20von%20Datensicherheitsverletzungen%20und%20Information%20der%20Betroffenen%20nach%20Art.%2024%20DSG_EN.pdf. Verified on 22 November 2026.

S8: FINMA. FINMA Guidance 03/2024: Cyber risks. https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20160707-finma-aufsichtsmitteilung-03-2024.pdf?sc_lang=en&hash=A1A633E2246BE27B2020897E1A389049. Verified on 22 November 2026.

S9: Federal Intelligence Service. Switzerland's Security 2026. https://www.vbs.admin.ch/dam/en/sd-web/tfhqKbM8ZL5k/VBS-DDPS-NDB-Sicherheit-Schweiz-2026-en.pdf. Verified on 22 November 2026.

S10: Swiss Confederation. First report on the Cyber Situation Network for the Summit on Peace in Ukraine. https://www.europa.eda.admin.ch/en/nsb?id=101528. Verified on 22 November 2026.

S11: Swiss Confederation. Federal Council plans to introduce new Cybersecurity Act. https://www.emek.admin.ch/en/newnsb/zX9oNK8tuI-Z. Verified on 22 November 2026.

S12: Federal Office for Cyber Security. FAQ on the reporting obligation. https://www.bacs.admin.ch/en/faq-reporting-obligation. Verified on 22 November 2026.

S13: Federal Office for Cyber Security. Woche 45: Black Friday wirft seine Schatten voraus – KI-Fakeshops und Paket-Phishing. https://www.bacs.admin.ch/de/26w45-de. Verified on 22 November 2026.

S14: Federal Office for Cyber Security. Woche 46: Personalisiertes Phishing aufgrund von abgeflossenen Daten. https://www.bacs.admin.ch/de/26w46-de. Verified on 22 November 2026.

S15: FDPIC. EDÖB leitete nach Cyberangriff auf Softwarelieferant Abklärungen ein. https://www.edoeb.admin.ch/de/edoeb-leitete-nach-cyberangriff-auf-softwarelieferant-abklaerungen-ein. Verified on 22 November 2026.

S16: Canton of Basel-Landschaft. FAQ-Data - Kanton Basel-Landschaft. https://www.baselland.ch/politik-und-behorden/direktionen/sicherheitsdirektion/amt_fuer_migration/bewilligungen/faq-data/. Verified on 22 November 2026.

S17: Canton of Basel-Landschaft. Cyberangriff auf die IT-Infrastruktur der kantonalen Verwaltung führte zu Datenabfluss - Kanton Basel-Landschaft. https://www.baselland.ch/politik-und-behorden/besondere-behoerden/landeskanzlei/medienmitteilungen/cyberangriff-auf-die-it-infrastruktur-der-kantonalen-verwaltung-fuehrte-zu-datenabfluss. Verified on 22 November 2026.

S18: Groupe 3R. Informations sur la cyberattaque d'avril 2026 - 3R - Réseau Radiologique Romand. https://www.groupe3r.ch/fr/informations-importantes/infos-cyberattaque-avril-2026-7268/. Verified on 22 November 2026.

S19: ICTjournal. Données volées, systèmes rétablis: le Groupe 3R fait le point après la cyberattaque (update) | ICTjournal. https://www.ictjournal.ch/news/2026-07-06/donnees-volees-systemes-retablis-le-groupe-3r-fait-le-point-apres-la-cyberattaque. Verified on 22 November 2026.

S20: SRG. SRG von Cybervorfall betroffen | SRG SSR. https://www.srgssr.ch/de/news-medien/news/srg-von-cybervorfall-betroffen. Verified on 22 November 2026.

S21: Publica. Cyber attack on Publica software supplier: data leak confirmed | PUBLICA. https://www.publica.ch/en/about-us/news/cyber-attack-publica-software-supplier-data-leak-confirmed. Verified on 22 November 2026.

S22: Netzwoche. Salt bestätigt Netzwerkausfall durch Cyberangriff | Netzwoche. https://www.netzwoche.ch/news/2026-05-18/salt-bestaetigt-netzwerkausfall-durch-cyberangriff. Verified on 22 November 2026.

S24: Federal Office for Cyber Security. Woche 5: Weltweite «SharePoint»-Phishing-Welle – auch die Schweiz ist betroffen. https://www.bacs.admin.ch/de/26w5-de. Verified on 22 November 2026.

S25: Federal Office for Cyber Security. Woche 6: «Subscription Bombing» – Wenn das E-Mail-Postfach unter Beschuss steht. https://www.bacs.admin.ch/de/26w6-de. Verified on 22 November 2026.

S26: Federal Office for Cyber Security. Woche 8: «ClickFix» – Wenn eine vermeintliche Fehlerbehebung oder Verifikation eine Malware installiert. https://www.bacs.admin.ch/de/26w8-de. Verified on 22 November 2026.

S27: Federal Office for Cyber Security. Woche 15: Falsche Bankmitarbeiter fordern Installation von Fernwartungssoftware. https://www.bacs.admin.ch/de/26w15-de. Verified on 22 November 2026.

S28: Federal Office for Cyber Security. Woche 18: Paket-Phishing mit perfider Fortsetzung – Die Masche des «Double Phishing». https://www.bacs.admin.ch/de/26w18-de. Verified on 22 November 2026.

S30: Federal Office for Cyber Security. Woche 23: Stellensuchende im Visier – Phishing, Betrug und Schadsoftware im Bewerbungsprozess. https://www.bacs.admin.ch/de/26w23-de. Verified on 22 November 2026.

S32: Federal Office for Cyber Security. Woche 35: Skimming bei Essenslieferdienst - Statt einem vollen Magen eine leere Kreditkarte. https://www.bacs.admin.ch/de/26w35-de. Verified on 22 November 2026.

S34: Federal Office for Cyber Security. Woche 42: Neue Variante von Phishing in Zusammenhang mit Hotelbuchungen zielt auf TWINT-Konten. https://www.bacs.admin.ch/de/26w42-de. Verified on 22 November 2026.

S40: IWB. Adressdaten bei Dienstleister von IWB entwendet (15 July 2026). https://www.iwb.ch/ueber-uns/newsroom/medienmitteilungen/artikel~_adressdaten-bei-dienstleister-von-iwb-entwendet~. Verified on 22 November 2026.

S41: Swiss police cybercrime portal. cybercrimepolice.ch | Cyberangriffe auf Kühlanlagen zeigen die…. https://cybercrimepolice.ch/de/faelle/cyberangriffe-auf-kuehlanlagen-zeigen-die-risiken-vernetzter-geraete. Verified on 22 November 2026.

S42: Federal Office for Cyber Security. Summit on Peace in Ukraine: first NCSC report on Cyber Situation Network. https://www.bacs.admin.ch/en/24-kfu-2-en. Verified on 22 November 2026.

S43: Official public source. Official incident or campaign account concerning a withheld organisation. https://cybercrimepolice.ch/ (article URL withheld). Verified on 22 November 2026.

S44: Swiss police cybercrime portal. cybercrimepolice.ch | Falsches Bankpersonal fordert Bargeld für…. https://cybercrimepolice.ch/de/faelle/falsches-bankpersonal-fordert-bargeld-fuer-angebliches-snb-sicherungskonto. Verified on 22 November 2026.

S45: Swiss police cybercrime portal. cybercrimepolice.ch | Betrügerische Investitionsanrufe nach…. https://cybercrimepolice.ch/de/faelle/betrugerische-investitionsanrufe-nach-datenabfluss-bei-pensionskassendienstleister. Verified on 22 November 2026.

S47: Canton of Basel-Landschaft. Update zum Cyberangriff auf die IT-Infrastruktur der kantonalen Verwaltung Basel-Landschaft - Kanton Basel-Landschaft. https://www.baselland.ch/politik-und-behorden/besondere-behoerden/landeskanzlei/medienmitteilungen/update-zum-cyberangriff-auf-die-it-infrastruktur-der-kantonalen-verwaltung-basel-landschaft. Verified on 22 November 2026.

S48: Netzwoche. Public reporting on an incident concerning a withheld organisation. https://www.netzwoche.ch/ (article URL withheld). Verified on 22 November 2026.

S49: Netzwoche. Public reporting on an incident concerning a withheld organisation. https://www.netzwoche.ch/ (article URL withheld). Verified on 22 November 2026.

S50: Netzwoche. Public reporting on an incident concerning a withheld organisation. https://www.netzwoche.ch/ (article URL withheld). Verified on 22 November 2026.

S53: Federal Office for Cyber Security. Kühl- und Kältesteuerungen: Systeme identifizieren, aktualisieren und schützen. https://www.bacs.admin.ch/de/warnung-kuehlanlagen-de. Verified on 22 November 2026.

S54: Swiss Confederation. Cyberangriff auf SharePoint-Server. https://www.admin.ch/de/newnsb/1CjmpBBHQaMV82PjKEpcL. Verified on 22 November 2026.

S55: Swiss Confederation. Cyberangriff auf Softwarelieferanten: Publica lässt Umgang mit Personendaten und Sicherheitskontrollen extern untersuchen. https://www.admin.ch/de/newnsb/A40p0VPerHSv. Verified on 22 November 2026.

S56: IT-Markt. Public reporting on an incident concerning a withheld organisation. https://www.it-markt.ch/ (article URL withheld). Verified on 22 November 2026.

S57: Netzwoche. Public reporting on an incident concerning a withheld organisation. https://www.netzwoche.ch/ (article URL withheld). Verified on 22 November 2026.

S58: Ifage. Information relative à un incident de sécurité impliquant des données personnelles | ifage. https://www.ifage.ch/news/2026/information-relative-a-un-incident-de-securite-impliquant-des-donnees-personnelles/. Verified on 22 November 2026.

S59: Canton of Vaud. La plateforme de support informatique des Gymnases et des Ecoles professionnelles du Canton victime d'un vol de données | État de Vaud. https://www.vd.ch/actualites/communiques-de-presse-de-letat-de-vaud/detail/communique/la-plateforme-de-support-informatique-des-gymnases-et-des-ecoles-professionnelles-du-canton-victime-dun-vol-de-donnees. Verified on 22 November 2026.

S60: Swiss government / NCSC. Six-month reporting obligation for cyberattacks on critical infrastructures. https://www.admin.ch/en/newnsb/gezctyF6KYR7UkCjXBC5s. Verified on 22 November 2026.

S61: FINMA. How FINMA is getting to the bottom of cyber risks in the financial sector. https://www.finma.ch/en/finma-public/article-series,-c-,-finma-at-work/artikelserie/cyberrisiken/. Verified on 22 November 2026.

S62: BACS warning. Kritische Schwachstellen in PHP: Sicherheitsupdates sofort einspielen. https://www.bacs.admin.ch/de/warnung-php-de. Verified on 22 November 2026.

S63: NVD record. NVD CVE-2026-109618. https://nvd.nist.gov/vuln/detail/CVE-2026-109618. Verified on 22 November 2026.

S64: NVD record. NVD CVE-2026-109619. https://nvd.nist.gov/vuln/detail/CVE-2026-109619. Verified on 22 November 2026.

S65: PHP vendor advisory. PHP security advisory: RCE via OOM corruption. https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w. Verified on 22 November 2026.

S66: PHP vendor advisory. PHP security advisory: RCE via stale global state. https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp. Verified on 22 November 2026.

S67: PHP release announcement. PHP security releases of 21 October 2026. https://www.php.net/archive/2026.php#2026-10-21-5. Verified on 22 November 2026.

S70: MITRE ATT&CK. Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1566/. Verified on 22 November 2026.

S71: MITRE ATT&CK. Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1190/. Verified on 22 November 2026.

S72: MITRE ATT&CK. Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1078/. Verified on 22 November 2026.

S73: Brandefense. Request a Demo | See AI-Driven Threat Intelligence in Action. https://brandefense.io/request-a-demo/. Verified on 22 November 2026.

S80: Università della Svizzera italiana. Incidente di sicurezza informatica – Informazioni e aggiornamenti | USI. https://www.usi.ch/it/data-breach. Verified on 22 November 2026.

S81: Withheld residential care provider. Public incident notices on the July 2026 ransomware disruption and October 2026 recovery update. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S82: FDPIC. Warnung vor betrügerischen E-Mails im Namen des EDÖB. https://www.edoeb.admin.ch/de/warnung-vor-betruegerischen-e-mails-im-namen-des-edoeb. Verified on 22 November 2026.

S83: Withheld Swiss public authority. Public notice on temporary service restrictions during October 2026 PHP vulnerability remediation. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S84: Canton of Vaud. Revue des cybermenaces : Juillet 2026 | État de Vaud. https://www.vd.ch/actualites/actualite/news/26508-revue-des-cybermenaces-juillet-2026. Verified on 22 November 2026.

S85: Canton of Vaud. Revue des cybermenaces : Septembre 2026 | État de Vaud. https://www.vd.ch/actualites/actualite/news/26702-revue-des-cybermenaces-septembre-2026. Verified on 22 November 2026.

S86: Withheld Swiss municipal administration. Public notice of 14 March 2026 on partial encryption and service restoration. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S87: Withheld Swiss sports federation. Public notice of 31 October 2026 on a personal-data incident affecting a licensing platform. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S88: Withheld Swiss sports federation. Public notice of 26 October 2026 on unauthorised account access affecting an administration platform. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S89: Report URI. Vendor research on an incident concerning a withheld organisation. https://blog.report-uri.com/ (article URL withheld). Verified on 22 November 2026.

S90: Withheld cantonal authority. Public notice of 5 August 2026 on a SharePoint incident and precautionary website update. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S91: Withheld cantonal authorities. Joint public notice of 28 August 2026 on automated collection of public vehicle-holder information across five cantons. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S92: Canton of Vaud. Vaud false-bank and false-police fraud update. https://www.vd.ch/actualites/actualite/news/25944-escroquerie-aux-faux-banquiers-policiers-le-nombre-de-cas-repart-a-la-hausse. Verified on 22 November 2026.

S93: Official or public reporting. St.Gallen remote-access fraud warning. https://www.sg.ch/news/sgch_kantonspolizei/2026/02/kanton-st-gallen--betrugsmasche-richtet-grossen-schaden-an.html. Verified on 22 November 2026.

S94: Official or public reporting. Ticino attempted family-emergency fraud. https://www4.ti.ch/di/pol-new/comunicazioni/comunicati-stampa-1/dettaglio/?user_polizia_pi1%5BnewsId%5D=259127. Verified on 22 November 2026.

S95: Official or public reporting. Bern remote-access fraud warning. https://www.police.be.ch/de/start/themen/news/medienmitteilungen.html?newsID=5cd77d2d-9a47-459f-b91d-60e5b6d54a5b. Verified on 22 November 2026.

S96: Official or public reporting. Schaffhausen suspected courier recruitment. https://www.shpol.ch/CMS/Webseite/Schaffhauser-Polizei-23813465-DE.html. Verified on 22 November 2026.

S97: Official or public reporting. Fribourg false-bank messages and card collection. https://www.fr.ch/dsjs/pol/actualites/escroqueries-aux-faux-banquiers-trois-auteurs-presumes-mis-en-cause. Verified on 22 November 2026.

S98: Official or public reporting. Neuchatel false-police and false-bank prevention. https://www.ne.ch/communiques-de-presse/escroquerie-au-faux-policier-et-faux-banquier-la-police-neuchateloise-la-rencontre-de-la-population-du-2-au-7-novembre-2026. Verified on 22 November 2026.

S99: Official or public reporting. Valais false-police and false-bank fraud. https://www.policevalais.ch/communiques-pour-les-medias/arnaque-aux-faux-policiers-pres-de-deux-tiers-des-escroqueries-dejouees/. Verified on 22 November 2026.

S100: Official or public reporting. Zug two courier investigations. https://zg.ch/de/zuger-polizei-news/2026/November/137-kanton-zug-telefonbetrug-zwei-geldkuriere-festgenommen. Verified on 22 November 2026.

S101: Threema. DDoS Attacks on Threema. https://threema.com/en/blog/outage-august-2026. Verified on 22 November 2026.

S102: SC Media. Encrypted messaging provider Threema hit by large-scale DDoS attacks. https://www.scworld.com/brief/encrypted-messaging-provider-threema-hit-by-large-scale-ddos-attacks. Verified on 22 November 2026.

S103: Google Threat Intelligence Group and Mandiant. Investigating Ephemeral Supply Chain Tampering. https://cloud.google.com/blog/topics/threat-intelligence/investigating-ephemeral-supply-chain-tampering. Verified on 22 November 2026.

S105: AOMEI. Statement on Ephemeral Tampering with the AOMEI Backupper Update Server. https://www.aomeitech.com/company/investigating-ephemeral-tampering.html. Verified on 22 November 2026.

S106: FDPIC. Tasks: data protection. https://www.edoeb.admin.ch/en/tasks-data-protection. Verified on 22 November 2026.

S107: Federal Office for Cyber Security. Semi-Annual Report 2025/2 (30 March 2026). https://www.bacs.admin.ch/en/hjb-25-2-en. Verified on 23 November 2026.

S108: Federal Office for Cyber Security. Semi-Annual Report 2025/1 (18 November 2025). https://www.bacs.admin.ch/en/hjb-25-1-en. Verified on 23 November 2026.

S109: FINMA. FINMA Risk Monitor 2025 (17 November 2025). https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/risikomonitor/20251117-finma-risikomonitor-2025.pdf?hash=6CB0C57B5333208BA29F26542B3B76B8&sc_lang=en. Verified on 23 November 2026.

S110: Swiss Confederation. «Sicherheit Schweiz 2026»: Keine Entwarnung für die Schweiz (25 June 2026). https://www.wbf.admin.ch/de/newnsb/jyRmuld1hBVy. Verified on 23 November 2026.

Appendix D. Glossary

- **BACS / NCSC:** the Federal Office for Cyber Security; BACS is the German abbreviation and NCSC is used in English-language material [S6].
- **FDPIC / EDÖB:** the Federal Data Protection and Information Commissioner; the abbreviations refer to the same federal authority in English and German [S7].
- **FINMA:** the Swiss Financial Market Supervisory Authority, with separate supervisory cyber-reporting requirements for the institutions covered by its guidance [S8].
- **FADP:** the Federal Act on Data Protection, whose data-security-breach duties depend on the conditions in the statute [S7].
- **ISA:** the Information Security Act, which establishes the critical-infrastructure cyber reporting obligation discussed in this report [S6].
- **CySA:** the proposed Cybersecurity Act described in the Federal Council's 2026 drafting decision; it is not treated here as enacted legislation [S11].
- **MFA:** multi-factor authentication, a sign-in process requiring more than one type of proof.
- **Phishing-resistant authentication:** authentication tied to the intended service, reducing the usefulness of a lookalike sign-in page.
- **DDoS:** distributed denial of service, traffic intended to prevent legitimate users from reaching a service.
- **DMARC:** an email-authentication policy that helps receiving systems handle messages that fail the relevant alignment checks.
- **SPF / DKIM:** email-authentication mechanisms concerning authorised sending and a message's cryptographic signature.
- **DNSSEC:** signatures that help validating resolvers check the authenticity of DNS information.
- **TLS:** transport encryption used by services such as HTTPS; a certificate check does not audit the application.
- **HSTS:** a website policy telling supporting browsers to use HTTPS for the specified host.
- **Credential record:** a recorded account-related item, which can be historical and does not establish a usable current password.
- **Device association:** an association between a device-related record and a service; it does not independently establish ownership or current infection.
- **Initial-access offer:** an advertisement claiming a route into an organisation's environment, which requires validation.
- **Stealer:** malware designed to collect information such as credentials or session material from a device.
- **Ransomware listing:** a public extortion claim associated with a group label and organisation.
- **Post card:** a redacted reproduction of retained underground material, with its date and explicit evidence boundaries.
- **Supplier incident:** an incident affecting a provider whose information or services may support another organisation.

- **Record versus person:** a record is an entry; one person may appear in several entries.
- **TLP:CLEAR:** a sharing designation allowing unrestricted distribution, subject to other applicable obligations.

About this report

Prepared by Odin by Brandefense for the Brandefense Country Report series. The English master and the German and French editions share the same source IDs, card IDs, figures and numerical findings. Translations carry a visible AI notice, and the English edition prevails where meanings differ.

This source package supports security decisions and subsequent editorial verification. It is not a complete census of Swiss incidents or a certification of any organisation. Recommendations describe work that defenders can perform; they do not assert that a named organisation has or has not performed it.

© 2026 Brandefense. All rights reserved.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

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

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

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

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

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

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

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

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

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

TÜRKIYE

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

BRANDEFENSE.IO