



COVERAGE ANALYSIS REPORT

How the 2026 Asos hack was covered

A structural reading of 34 articles, by type of outlet.

PREPARED BY

Frametra Software Inc

PREPARED FOR

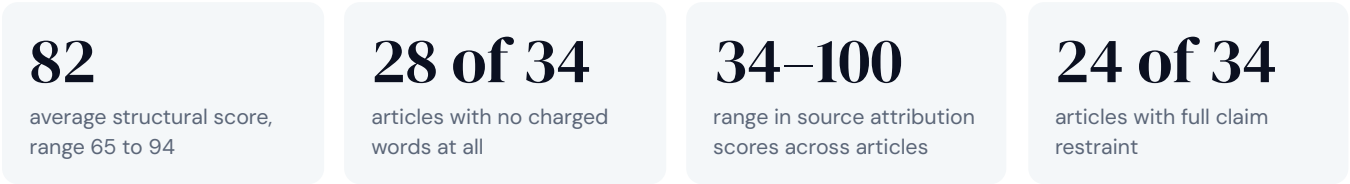
Sample, built on public coverage

SAMPLE REPORT

October 25, 2026. This sample shows what a Coverage Analysis Report looks like. It describes how the articles are written, not the incident itself, and not whether any party or outlet is right or wrong.

At a glance

34 articles from 28 outlets, read by Frametra’s on-device engine across six structural signals.



WHAT THE NUMBERS SHOW

- The tone stayed measured.** Neutral language averaged 99.2 out of 100, and every article scored 95 or above. 28 of the 34 articles used none of the engine’s charged words.
- Security and tech press led on sourcing.** The 14 security and tech articles averaged 75 on sourcing and 7.6 attribution phrases per article. News outlets averaged 58 and 4.5, and business and retail trade 62. This reverses the pattern in our Canvas breach sample, where security press scored lower than news outlets.
- Sourcing varied widely from article to article.** Source attribution ran from 34 to 100. 8 articles scored 80 or above and 6 scored below 50.
- The news group is smaller than it looks.** Five of the 13 news articles share two headlines, which suggests the same agency stories run under different mastheads: one headline appears three times and another twice. Their near-identical scores count more than once in the news average.
- Wording firmed up outside the news group.** All 13 news articles scored 100 on claim restraint, against 78 for business trade and 78 for security and tech. The engine counts words such as “claims” and “reportedly” against this signal, which is usually normal when articles relay what attackers or experts say.
- Security and tech pieces ran longest.** They averaged 508 words, against 428 for news and 380 for business trade. All three groups scored within a few points on overall structure: 83 for news, 78 for business trade and 82 for security and tech.

SOURCING AND LENGTH, BY TYPE OF OUTLET



How to read these scores. They describe how an article is built: its sourcing, wording and evidence. They do not say whether an article is accurate, fair or well-intentioned, and they are not grades.

The six signals, across all 34 articles

Average score for each signal, out of 100. Weights show how much each signal counts toward the structural score.



BY TYPE OF OUTLET

	ARTICLES	AVG WORDS	SCORE	SOURCING	CLAIM RESTRAINT	EVIDENCE	CHARGED WORDS
News outlets	13	428	83	58	100	78	0.0
Business and retail trade	7	380	78	62	78	72	0.1
Security and tech press	14	508	82	75	78	76	0.4

Business and retail trade has seven articles, too few to compare on its own with confidence.

BY ARTICLE LENGTH

	ARTICLES	AVG WORDS	SCORE	SOURCING	CLAIM RESTRAINT	EVIDENCE	CHARGED WORDS
Under 600 words	30	416	82	66	88	76	0.1
600 words or more	4	712	82	69	80	77	0.5

Sourcing = source attribution. Evidence = figures and direct quotations. Charged words = average count per article. Few articles in this sample run past 600 words.

Outlet by outlet

All 34 articles, grouped by type of outlet. Scores out of 100; values below 50 are shown in amber.

OUTLET	HEADLINE	WORDS	SCORE	SRC	LANG	CLM	HDG	EVD	ACT
News outlets (13 articles)									
itv.com	Asos investigating suspected hack that saw shoppers sent threat...	587	80	41	100	100	94	77	96
itv.com	Asos says 'unauthorised party' gained access but payment inform...	424	84	63	100	100	71	71	96
expressandstar.com	Asos customers told online retailer 'hacked' in phone alert	356	76	34	100	100	75	69	96
expressandstar.com	Asos says customer data may have been accessed after 'unauthori.	419	84	63	100	100	71	74	96
expressandstar.com	Asos apologises to customers after 'unauthorised activity'	474	84	59	100	100	81	74	96
yorkshirepost.co.uk	Asos says customer data may have been accessed after 'unauthori.	280	79	67	100	100	61	74	98
irishnews.com	Asos apologises to customers after 'unauthorised activity'	474	82	53	100	100	81	74	96
irishnews.com	Asos says customer data may have been accessed after 'unauthori.	419	82	56	100	100	71	74	96
lbc.co.uk	Asos warns customers their personal details 'may have been acce...	350	80	43	100	100	87	71	95
canberratimes.com.au	Rogue phone alert sent to fashion giant Asos customers	516	77	47	100	100	49	74	98
malaymail.com	'Asos hacked': Fashion giant probes breach after customers rece...	445	89	79	100	100	55	100	97
kuwaittimes.com	Asos says probing 'unauthorized activity' after phone alerts	439	87	71	100	100	55	98	97
thepinknews.com	ASOS 'hacked' as users get threatening app alert	387	92	84	100	100	84	83	98
Business and retail trade (7 articles)									
cityam.com	Asos shares crater after 'hackers' threaten data leak	572	86	68	100	100	72	83	97
cityam.com	Asos hackers posed as 'trusted contact' to dupe employee	466	88	66	100	100	95	77	99
mediaweek.com.au	ASOS alerts customers to data breach as shares fall by 14%	315	78	63	100	71	65	80	97
fashionunited.uk	Asos confirms cyber attack: What to know	258	68	58	100	50	93	57	94
businessinsurance.com	UK's ASOS says cyber hack accessed customers' personal data	189	79	65	100	100	80	61	100
insideretail.com.au	Hackers breach Asos database	352	83	54	100	100	78	83	97
retailbiz.com.au	Cybersecurity expert says ASOS hack is 'public extortion'	509	65	57	95	28	64	65	96
Security and tech press (14 articles)									
techcrunch.com	Asos confirms breach of customer data after hackers send rogue...	427	86	100	100	50	90	67	98
helpnetsecurity.com	ASOS confirms data breach after "hacked" app alert reaches shop...	509	88	80	100	100	50	86	96
techradar.com	ASOS 'hacked' alert live — all the latest from security experts...	465	91	92	95	100	76	78	95
therecord.media	Shares in British clothing company ASOS dive after hackers appa...	380	66	45	100	40	60	74	96
bleepingcomputer.com	ASOS confirms data breach after "HACKED" in-app notifications	435	76	62	100	56	70	89	97
bleepingcomputer.com	ASOS links data breach to social engineering attack, credential...	376	88	80	100	100	58	83	98
securityweek.com	ASOS Confirms Cyberattack, Data Breach	603	90	78	100	100	82	83	96
malwarebytes.com	ASOS breach update: Hackers stole customer details and shopping.	493	83	75	95	81	90	60	98
computerweekly.com	Scope of Asos data breach wider than first reported	623	84	64	96	100	73	77	97
silicon.co.uk	Asos Acknowledges Theft Of Detailed Customer Data	247	76	92	100	50	60	74	96
cybermagazine.com	The ASOS Data Breach Exposed Millions of Customers' Details	491	94	99	95	100	84	77	98
cybersecurecatalyst.ca	Threatening notification sent to customers' phones following br...	668	87	87	96	73	93	74	98
rescana.com	ASOS Data Breach 2026: Cybersecurity Incident Analysis of Third...	955	66	46	100	49	40	73	99
cyberinsider.com	ASOS credential-stuffing attack exposed data of 138,828 custome...	441	80	54	100	100	69	62	96

Src source attribution · Lang neutral language · Clm claim restraint · Hdg calibrated hedging · Evd evidence signals · Act active voice

What a communications team can take from this

- **Where the tone held.** Neutral language was close to the maximum in every group: 100 for news outlets, 99 for business trade and 98 for security and tech press. The wording was not where the articles differed.
- **Where the articles differed.** Sourcing. Security and tech press carried the most attribution phrases and scored highest on sourcing, while news outlets and business trade scored lower.
- **Where one story repeats.** Several news articles share headlines and appear to be the same agency stories. A count of mentions overstates how many separate accounts exist.
- **Where the language firmed up.** The six lowest claim restraint scores all came from business trade and security pieces, none from the news group. That is usually normal when an article relays what attackers or experts say.

WHAT THIS SAMPLE DOES NOT COVER

This sample uses Frametra's free on-device engine, which reads each article's wording. It cannot say **who was quoted**, how often sources were **anonymous**, whose voices were missing (customers, regulators, the company), or whether a claim is supported. A full Coverage Analysis Report adds a person-checked read of those questions, with the exact sentences behind each finding.

WHAT A FULL REPORT INCLUDES

- Up to 30 or 50 articles about your subject, by outlet, with a written comparison
- Source patterns, anonymity rates and missing voices, with the evidence behind each finding
- Editorial language trends over time
- A check by a person before delivery

METHOD AND LIMITS

Each article was read from the public web page by Frametra's free engine, on the reader's device, and scored on six signals: source attribution (28% of the score), neutral language (25%), claim restraint (20%), calibrated hedging (10%), evidence signals (10%) and active voice (7%). Articles under 300 words carry a small length adjustment. Source attribution reflects the variety of attribution wording and linked citations relative to article length, so longer articles need more to score the same. Claim restraint falls when an article uses words such as "claims", "alleges" or "reportedly". The charged-word list is built for news wording and can flag terms that are descriptive in a cyber-incident story. Of 38 links, three did not return readable text and were left out, and one paywalled page returned only a headline and was removed, leaving 34. The sample is a selection of public articles about the October 2026 incident, not every article published, and it mixes agency copy, trade reports and security analysis, which are built differently. Compare groups of articles rather than single pages.

Frametra reports are an analytical aid. They are not legal, journalistic or professional advice.