

After the Successors: Affiliate Collapse, Social-Engineering Mega-Hits, and Resilience Lessons from the 2025 Ransomware Ecosystem

Rodrigo Sanches Miani

ORCID: 0000-0002-8176-8040

Faculty of Computing, Federal University of Uberlândia, Uberlândia, Brazil

Monica T. Whitty

ORCID: 0000-0001-8143-289X

Software Systems and Cyber Security, Monash University, Melbourne, Australia

Kyounggon Kim

ORCID: 0000-0002-5675-4253

Center of Excellence in Cybercrimes and Digital Forensics, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia

Correspondence: Rodrigo Sanches Miani · contact details held in the journal record

Publication history. Assigned by the publisher to Cybersecurity Advances, Volume 2, Issue 1 (2025). This publisher-authorized digital edition was released on 29 October 2026 from the supplied final 2025 manuscript. Review-stage notices were removed and journal typography, pagination, metadata, and accessibility were normalized; substantive scholarly content was preserved.

© 2025 the author(s). Published by AlphaTech Scholarly Press under the Creative Commons Attribution 4.0 International License (CC BY 4.0). No DOI is displayed unless and until registration is independently verified.

Background: The 2025 ransomware year put to its first test the ecosystem-churn model that the 2024 disruption record — Operation Cronos, the ALPHV exit scam, and the documented rise of successor brands — had suggested [3]. RansomHub — the successor brand that had absorbed LockBit's displaced affiliates — went dark on 1 April 2025, with its affiliate pool publicly claimed by the DragonForce "cartel" model within a day. The year's most consequential incidents were not encryption feats but social-engineering campaigns: the April 2025 attacks on Marks & Spencer (reported ~£300 million in lost profits; online orders halted for weeks) and the Co-operative Group (£206 million in lost first-half revenue, £80 million in operating-profit impact), both attributed to the Scattered Spider collective using help-desk and identity social engineering on the DragonForce platform. Meanwhile, on-chain ransomware payments *fell* roughly 35% year-over-year to approximately \$813.55 million in 2024 (Chainalysis), even as single-incident impact reached record levels.

Objective: We analyze the 2025 record as a test of the displacement-versus-dismantlement thesis and extract the resilience lessons that follow. **Methods:** Event-driven qualitative analysis of the 2025 record from primary disclosures, corporate statements, and law-enforcement reporting; payment-flow analysis from blockchain analytics; and a stage-versus-control coverage assessment. **Results:** The churn model performed: brand-level collapse produced affiliate migration, not dismantlement. Impact decoupled from payment volume: the signature 2025 incidents were human-vector attacks whose costs were driven by operational halt, third-party access compromise, and recovery duration — not by encryption sophistication. Disclosure worked: the year's impact figures became public within months, in the disclosure era the field entered in 2024. **Conclusions:** Resilience investment belongs at the identity and help-desk boundary, in third-party access governance, and in tested recovery — with disclosure-era accountability as the forcing function.

Keywords: ransomware; RansomHub; DragonForce; Scattered Spider; social engineering; cyber resilience; disclosure; digital trust

Contribution statement. This paper makes four contributions: (1) a source-verified 2025 event record centered on the RansomHub collapse and the M&S/Co-op campaigns; (2) payment-flow analysis showing the continued decoupling of ransom volumes from realized impact; (3) a stage-versus-control coverage assessment for human-vector ransomware in the retail sector; and (4) an updated resilience-investment ordering reflecting the 2025 evidence.

1. Introduction

In 2024, the Operation Cronos disruption of LockBit and its aftermath functioned as a natural experiment in adversarial ecosystem resilience: brand-level takedowns *displaced* rather than dismantled the ransomware economy — the displaced affiliate labor re-

bundled under successor brands within weeks [3] — and realized impact appeared determined by victim-side recovery capability rather than malware sophistication. The 2025 record tests both observations with unusual clarity — and both held.

The displacement claim was tested by RansomHub itself. The brand that absorbed LockBit's displaced operators through 2024, and that blockchain analytics had identified as the year's most prolific RaaS operation, went dark on 1 April 2025: affiliate chat portals disappeared, and within a day the competing DragonForce operation publicly claimed that RansomHub's affiliates had "decided to move to their infrastructure" under "a new option from The DragonForce Ransomware Cartel" [1][2]. The economy's productive labor — the affiliate pool — migrated again, exactly as the displacement model predicts. No dismantlement occurred; a re-bundling did.

The victim-side claim was tested by two of the most economically consequential incidents in ransomware history. In late April 2025, Marks & Spencer suffered a ransomware attack — attributed to threat actors linked to the Scattered Spider collective and executed on the DragonForce platform — that halted online ordering for weeks, disrupted click-and-collect and contactless payment, and by the company's own May statement cost approximately £300 million in lost operating profit [4][5]. The intrusion reportedly succeeded through social engineering of a third-party supplier's service desk. Days later, the Co-operative Group detected an attempted intrusion and proactively shut down parts of its IT estate; DragonForce-affiliated actors claimed the attack, data theft was confirmed for a significant number of current and former members and customers, and by September 2025 the Co-op disclosed £206 million in lost first-half revenue and an £80 million operating-profit hit, with a £120 million full-year estimate [6][7][8]. In July 2025, UK authorities arrested three teenagers in connection with the campaigns [5]. The through-line is not cryptography: both intrusions reportedly began with *people* — service desks persuaded to reset credentials — and both impacts were driven by *operational halt and recovery duration*, not by the malware.

Meanwhile the payment economy's own numbers moved the other way: on-chain ransomware payments fell roughly 35% year-over-year to approximately \$813.55 million in 2024, per Chainalysis's February 2025 analysis — which also documented RansomHub's absorption of displaced LockBit operators [3]. Falling payments coexisting with rising single-incident impact is the year's central economic fact, and it sharpens the 2024 argument: the victim-side variables are where the money and the damage part ways.

1.1 Research questions

RQ1: What is the verified 2025 event record — the RansomHub collapse, the affiliate migration, and the M&S/Co-op campaigns? **RQ2:** What do payment flows show about the relationship between ecosystem churn, payment volume, and realized impact? **RQ3:** Which resilience controls map onto the 2025 impact stages, and where do gaps remain? **RQ4:** What should retail-sector and high-interdependence organizations prioritize in 2026?

1.2 Contributions

(1) The verified 2025 event record (Section 3, Figure 1, Table 1) (RQ1). (2) Payment-flow analysis across 2021–2024 (Section 3.3, Figure 2, Table 2) (RQ2). (3) A stage-versus-control coverage assessment for the 2025 human-vector campaign profile (Section 4, Figure 3, Table 3) (RQ3). (4) Prioritized resilience guidance (Section 5) (RQ4).

2. Background

2.1 From brand-centered to affiliate-centered analysis

Analyst and blockchain-analytics reporting through 2024–2025 established that RaaS economies re-bundle after brand disruption because affiliates — the labor — are brand-agnostic; RansomHub's own rise was built on absorbing operators displaced from LockBit [3]. The 2025 record supplies the natural follow-on: RansomHub's collapse showed that even the *successor* brand is substitutable, and DragonForce's "cartel" model — branding itself as a platform hosting affiliate "white-label" operations rather than a single gang — is the churn model's logical next step. Analyst reporting through 2025 documented affiliates distributing across Qilin, DragonForce, and other platforms after the April collapse [1][2].

2.2 The social-engineering pivot

The 2025 flagship campaigns belong to a distinct operational lineage — the Scattered Spider collective's playbook: telephone-based social engineering of IT help desks and third-party service providers, credential reset, deep reconnaissance, and delayed encryption for maximum leverage [7][9]. This vector had already hit casinos, hospitality, and transportation in 2023–2024; retail's 2025 campaigns demonstrated the playbook at national-retail scale. The NCA publicly identified Scattered Spider as the investigation focus in May 2025 [9], and the July arrests marked the enforcement system's first material traction against the human layer [5]. The

defensive implication is uncomfortable: the year's most expensive incidents were defeated or enabled at the *identity* boundary, not the network boundary.

2.3 The disclosure era matures

The Co-op's September 2025 interim-results disclosure — quantifying cyber-incident impact in its financial statements to the pound — is the disclosure era functioning as designed: incident costs entering public accounting within months, in audited form [7][8]. This is the accountability environment 2024's regulation created, and it changes victim behavior measurably: impact statements are now recovery-credibility statements.

3. The 2025 Record (RQ1)

3.1 Methodology

Events were compiled from primary disclosures where available: the analyst reports that documented RansomHub's collapse in real time [1][2], Chainalysis's payment analytics [3], corporate statements and financial disclosures for M&S and the Co-op [4][6][7][8] [10], and law-enforcement reporting for the enforcement events [5][9]. Contested attribution (e.g., Scattered Spider's precise membership) is reported as attributed, not asserted. The coverage assessment is a qualitative author analysis, with subjectivity stated in Section 6.

3.2 The event record

Figure 1 and Table 1 present the verified sequence. Three observations. First, the churn signature: RansomHub's collapse on 1 April was followed within a day by a rival's public affiliate-recruitment claim — the ecosystem's re-bundling now happens publicly and competitively. Second, the impact signature: within the same three weeks, the UK retail sector absorbed two of the costliest ransomware incidents on record, both human-vector, both executed on the same affiliate platform. Third, the accountability signature: by September, incident costs were in audited financial disclosures, and by July the enforcement system had made arrests.

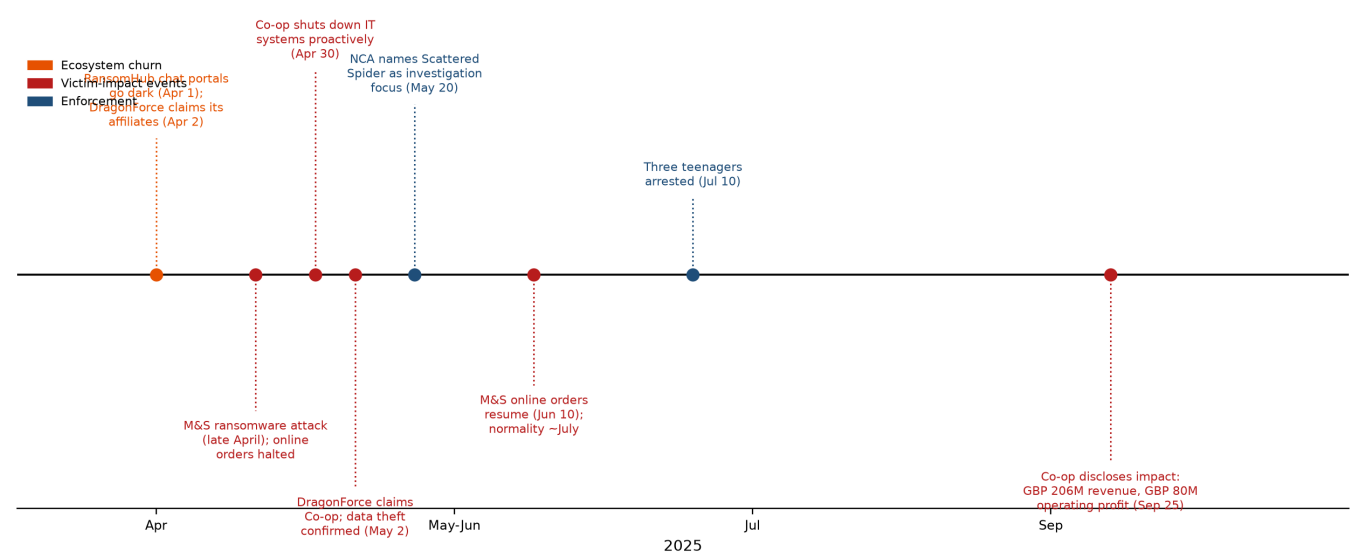


Figure 1. The 2025 ransomware event record: ecosystem churn, victim-impact events, and enforcement milestones (sources per Table 1).

Event	Date (2025)	Class	Documented consequence	Source
RansomHub chat portals go dark; DragonForce publicly claims RansomHub's affiliates have "moved to their infrastructure"	Apr 1-2	Ecosystem churn	The year's most prolific RaaS brand collapses; affiliate pool publicly re-bundles	[1][2]
M&S ransomware attack	Late Apr	Victim impact	Online ordering, click-and-collect and contactless payment halted for weeks; ~GBP 300M lost operating profit disclosed in May; entry reportedly via third-party supplier social engineering	[4][5]
Co-op proactively shuts down parts of its IT estate	Apr 30	Victim impact	Back-office and call-center disruption; later confirmed data theft for significant numbers of members/customers	[6][7]

DragonForce claims the Co-op attack	May 2	Ecosystem churn	Same affiliate platform as M&S; tactics "similar" per analyst reporting	[6]
NCA names Scattered Spider as investigation focus	May 20	Enforcement	Collective linked to human-vector help-desk social engineering on the DragonForce platform	[9]
M&S online ordering resumes	Jun 10	Victim impact	Full recovery into July; H1 pre-tax profit falls from GBP 391.9M to GBP 3.4M	[4][10]
Three teenagers arrested over the retail campaigns	Jul 10	Enforcement	First material enforcement traction against the human layer	[5]
Co-op quantifies impact	Sep 25	Victim impact	GBP 206M lost first-half revenue; GBP 80M operating-profit hit; GBP 120M full-year estimate	[7][8]

Table 1. The 2025 ransomware event record (sources per row).

3.3 Payment flows versus realized impact (RQ2)

Figure 2 and Table 2 assemble the payment record: \$987M (2021), \$567M (2022), a revised \$1.25B (2023), and \$813.55M (2024) — a 35% decline, attributed by analysts to enforcement pressure, improved tracing, and payment abstention [3]. Against this, the 2025 flagship incidents' disclosed impacts — roughly £300M for a single retailer [5][10] — exceed entire brand-year payment totals of earlier eras. The inference is structural: on-chain payments measure only the ransom leg of the economy, and they have decoupled from realized impact, which is driven by downtime, recovery duration, and interdependency. A year in which payments fell 35% while single-incident losses reached record levels is a year in which the victim-side variables did the damage — which is precisely where defenders hold leverage.

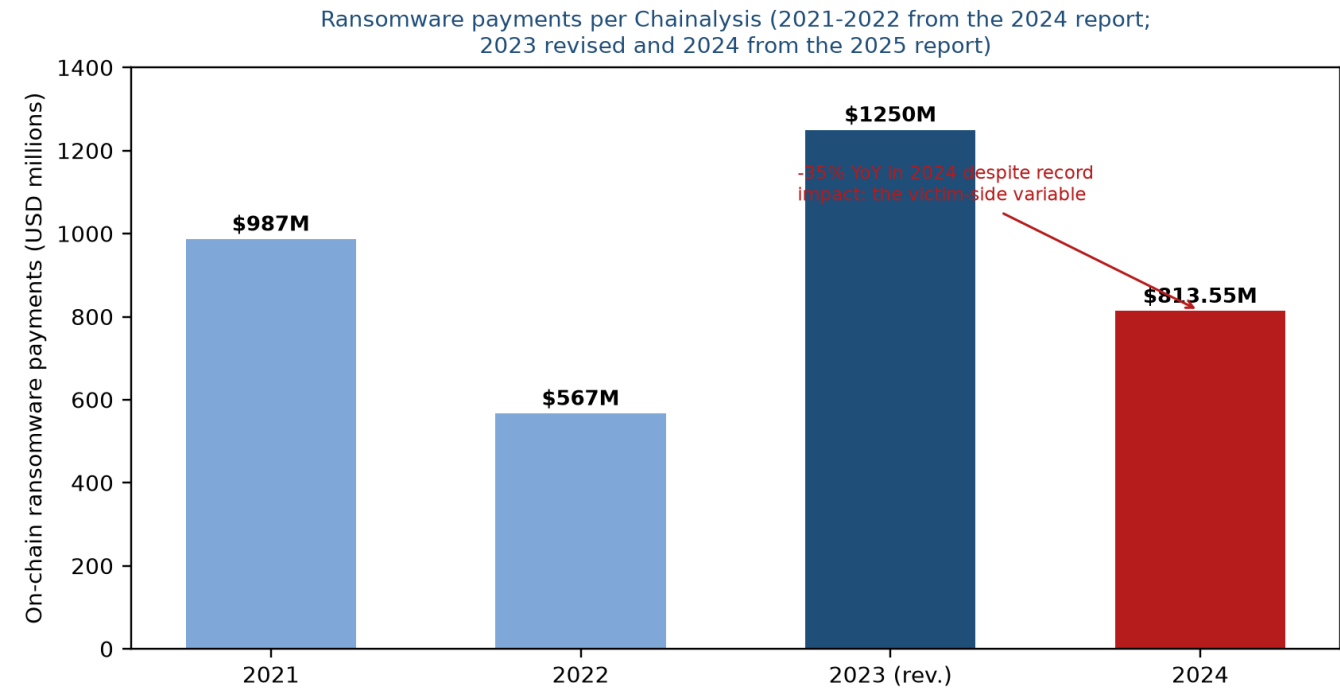


Figure 2. On-chain ransomware payment flows as reported by Chainalysis [3][11]: 2023 revised upward, 2024 down 35% — while single-incident disclosed impacts reached record levels.

Year	On-chain payments (USD M)	Source basis
2021	987	2024 report [11]
2022	567	2024 report [11]
2023	1,250 (revised)	2025 report [3]
2024	813.55 (-35% YoY)	2025 report [3]

Table 2. Ransomware payment flows as reported by Chainalysis [3][11].

4. Impact Stages and Resilience Coverage (RQ3)

Figure 3 maps the five impact stages of the 2025 human-vector campaign profile against five resilience-control classes aligned with the functions of NIST CSF 2.0 [12]; Table 3 records the reasoning.

S1 — Help-desk and identity social engineering. The initial access of both flagship campaigns: attackers impersonating employees to service desks, inducing credential resets [7][9]. The strong control is phishing-resistant authentication plus *process* hardening of the reset path — out-of-band verification, callback-to-known-number policies, and help-desk-specific abuse training. This is the control the 2025 record says to fund first.

S2 — Third-party supplier access. M&S's intrusion reportedly entered through a third-party supplier's compromised credentials [4]. Third-party access governance — scoped identities, short-lived credentials, and monitored delegation — scores partial: necessary, but the 2025 record shows the trusted-supplier premise itself must be treated as attackable.

S3 — Retail operations disruption. The M&S impact (weeks without online ordering, click-and-collect, contactless payment) is a continuity failure, not a data failure. Segmentation, rapid isolation, and *tested* recovery — the StopRansomware baseline [13] — score strong where they existed and are the defining gap where they did not.

S4 — Data theft and double extortion. The Co-op confirmed exfiltration of significant customer and colleague data [6]. Data minimization and egress detection score partial: the exfiltration in both campaigns proceeded over legitimately authenticated channels, which is the hard case.

S5 — Disclosure and regulatory follow-through. Both organizations disclosed; the Co-op quantified impact in its audited results [7][8]. Disclosure readiness scores strong as a control — it functioned as designed — and as a forcing function for the others.

2025 ransomware impact stages vs. resilience controls (author assessment)					
	Phishing-resistant MFA & help-desk verification	Third-party access governance	Segmentation, isolation & tested recovery	Data minimization & exfiltration detection	Disclosure readiness & sector coordination
S1 Help-desk / identity social engineering	+	~	-	~	~
S2 Third-party supplier access	~	+	~	~	~
S3 Retail operations disruption	~	-	+	-	~
S4 Data theft & double extortion	-	~	~	+	~
S5 Disclosure & regulatory follow-through	-	-	~	~	+

Figure 3. The 2025 impact stages versus resilience-control classes (author assessment; reasoning in Table 3).

Impact stage	Description (2025 record)	Primary control class	Coverage note
S1 Help-desk / identity social engineering	Employee impersonation to reset credentials at M&S and Co-op supplier desks	Phishing-resistant MFA + hardened reset verification	Strong where deployed; the decisive control in the 2025 record
S2 Third-party supplier access	Intrusion via a compromised third party's credentials	Third-party access governance	Partial: the trusted-supplier premise is itself attackable
S3 Retail operations disruption	Weeks without online ordering, click-and-collect, contactless payment	Segmentation, rapid isolation, tested recovery	Strong driver of the GBP impact figures
S4 Data theft & double extortion	Confirmed exfiltration of member/customer data (Co-op)	Data minimization & egress detection	Partial: exfiltration over legitimate authenticated channels

S5 Disclosure & regulatory follow-through	Impact quantified in audited financial disclosures within months	Disclosure readiness & sector coordination	Strong: functioned as designed in 2025
---	--	--	--

Table 3. Impact stages mapped to resilience controls for retail-sector victims [4][6][7].

5. Priorities for 2026 (RQ4)

The 2025 evidence reorders the resilience investment list. **First, the identity boundary:** phishing-resistant MFA and a hardened, socially engineered-resistant reset process — the cheapest control per unit of realized-impact reduction in the 2025 record. **Second, third-party access governance:** the trusted-supplier premise is now demonstrably part of the attack surface. **Third, tested recovery:** the difference between the two flagship campaigns' trajectories was containment and restoration speed. **Fourth, disclosure competence:** the September 2025 financial disclosures show that recovery credibility is now a public, priced attribute. Enforcement against the human layer (the July arrests [5]) is welcome, but the Scattered Spider playbook's dependence on *legitimate credentials* means the identity boundary remains the decisive terrain.

6. Limitations and Threats to Validity

Construct validity. The five-stage impact cut is analytical; other decompositions are possible. **Internal validity.** Attribution to Scattered Spider is law-enforcement and press attribution, not adjudicated fact; the analysis treats it as attributed. Corporate impact figures are company-disclosed and subject to revision. **External validity.** Retail-sector findings may not transfer to sectors with different operational coupling; the sample is two flagship campaigns plus one brand collapse — a small, informative record, not a population. **Reliability.** Event dating relies on press and analyst reporting; the analysis privileges primary statements where they exist. **Temporal scope.** Frozen at the end of 2025; the prosecution record and DragonForce's subsequent evolution are out of scope.

7. Conclusion

The 2025 ransomware record is the churn model's confirmation and the resilience thesis's sharpest demonstration to date. The year's most prolific brand vanished in a day and its affiliates re-bundled within 24 hours; the year's costliest incidents were won at the help desk, not in the kernel; and the money contracted while the damage grew. For defenders, the 2025 record is close to a decision procedure: harden the identity boundary that the attackers actually used, govern the third-party access they actually exploited, rehearse the recovery that actually determined the losses, and treat disclosure as the resilience statement it has become. The adversary's 2025 was a study in human engineering; the defender's 2026 must be too.

Declarations

Funding. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

CRedit contribution statement. Rodrigo Sanches Miani: conceptualization, event-record reconstruction, writing – original draft. Monica T. Whitty: validation, social-engineering human-factor analysis, writing – review & editing. Kyounggon Kim: investigation, cybercrime-context analysis, writing – review & editing. (Corresponding author: Rodrigo Sanches Miani.)

Competing interests. The authors declare no competing interests.

Data and code availability. No new datasets were generated; all quantitative claims are attributed to the cited primary disclosures and analytics [1][2][3][7][8][10].

Ethics and dual-use. The paper analyzes publicly reported incidents and contains no attack tooling, negotiation guidance, or victim-identifying detail beyond public reporting.

AI assistance declaration. AI-based tools were used in a limited supporting capacity (literature search, figure preparation, and language editing); all research content, analysis, and conclusions were produced, reviewed, and verified by the authors, who take full responsibility for the work.

References

- [1] Group-IB, "Ransomware debris: an analysis of the RansomHub operation," Apr. 30, 2025. [Online]. Available: <https://www.group-ib.com/blog/ransomware-debris/>
- [2] GuidePoint Security, "RansomSnub: RansomHub's Affiliate Confusion," Apr. 8, 2025. [Online]. Available: <https://www.guidepointsecurity.com/blog/ransomsnub-ransomhubs-affiliate-confusion>
- [3] Chainalysis, "Crypto Ransomware 2025: 35% Year-over-Year Decrease in Ransomware Payments," Feb. 5, 2025. [Online]. Available: <https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/>

- [4] BBC News, "M&S cyber attack: What we know about it and its impact," May-Jun. 2025. [Online]. Available: <https://www.bbc.com/news/articles/c0el31nqnpvo>
- [5] J. Gross, "3 Teenagers Arrested Over Cyberattacks That Cost U.K. Retailers Millions," The New York Times, Jul. 10, 2025. [Online]. Available: <https://www.nytimes.com/2025/07/10/business/cyber-attack-arrests-marks-spencers-harrods-coop.html>
- [6] L. Abrams, "Co-op confirms data theft after DragonForce ransomware claims attack," BleepingComputer, May 2, 2025. [Online]. Available: <https://www.bleepingcomputer.com/news/security/co-op-confirms-data-theft-after-dragonforce-ransomware-claims-attack>
- [7] B. Toulas, "Co-op says it lost \$107 million after Scattered Spider attack," BleepingComputer, Sep. 25, 2025. [Online]. Available: <https://www.bleepingcomputer.com/news/security/co-op-says-it-lost-107-million-after-scattered-spider-attack/>
- [8] Reuters, "Britain's Co-op warns of \$161 million profit hit from cyberattack," Sep. 25, 2025. [Online]. Available: <https://www.reuters.com/world/uk/britains-co-op-says-cyberattack-cost-it-108-million-2025-09-25/>
- [9] BBC News, "M&S and Co-op hacks: Scattered Spider is focus of police investigation," May 2025. [Online]. Available: <https://www.bbc.com/news/articles/ckgnndrgxv3o>
- [10] A. Scroxton, "M&S profits tumble after cyber attack," ComputerWeekly, Nov. 5, 2025. [Online]. Available: <https://www.computerweekly.com/news/366634121/MS-profits-tumble-after-cyber-attack>
- [11] Chainalysis, "The 2024 Crypto Crime Report," Feb. 2024. [Online]. Available: <https://www.chainalysis.com/reports/crypto-crime-2024/>
- [12] NIST, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
- [13] CISA, NSA, and FBI, "StopRansomware Guide," Sep. 2023. [Online]. Available: <https://www.cisa.gov/stopransomware>