

After the Takedown: Ecosystem Resilience, Affiliate Churn, and the Foundations of Cyber Resilience after Operation Cronos (2024)

Anushka Nehra

ORCID: 0009-0006-0574-9856

Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala, India

Nishu Bansal

ORCID: 0000-0002-2150-9573

Department of Computer Science & Engineering, Chandigarh University, Mohali, India

Correspondence: Nishu Bansal · contact details held in the journal record

Publication history. First published in the offline edition of Cybersecurity Advances, Volume 1, Issue 1 (December 2024). This publisher-authorized digital archival edition was released on 12 October 2026. The scholarly content is reproduced from the supplied offline-edition manuscript; review-stage notices were removed and journal typography, pagination, metadata, and accessibility were normalized.

© 2024 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 verified.

Background: On 19 February 2024, an international law-enforcement operation codenamed Cronos disrupted LockBit — until then the most prolific ransomware-as-a-service (RaaS) brand — seizing infrastructure, source code, and victim data. The following month, the ALPHV/BlackCat cartel imploded in a \$22 million exit scam against a victim (Change Healthcare) whose attack had already caused the most consequential U.S. healthcare disruption of the decade, and new brands such as RansomHub absorbed the displaced affiliate pool. **Objective:** This paper analyzes the 2024 ransomware ecosystem as a *resilient adversarial system* and asks what its post-Cronos behavior teaches about the design of defensive resilience. **Methods:** We conduct a qualitative event-driven analysis of the 2024 disruption sequence from primary and authoritative secondary sources (law-enforcement releases, blockchain analytics, incident-response and industry reports), reconstruct the RaaS value chain and its post-takedown dynamics, and synthesize a resilience-lifecycle framework aligned with NIST CSF 2.0 and the 2024 regulatory instruments (NIS2 transposition deadline, SEC incident-disclosure rule). **Results:** The ecosystem absorbed its largest ever law-enforcement shock within weeks: brands are substitutable but the affiliate economy persists; payment flows, already at a record ~\$1.1 billion in 2023, re-concentrated under successor brands; and the most damaging 2024 incidents (Change Healthcare; the Synnovis/NHS disruption) were produced not by the most sophisticated malware but by systemic vulnerabilities in recovery and sectoral interdependence. Defensive resilience — not attacker attribution — emerges as the decisive variable. **Conclusions:** Ransomware defense should be designed against an ecosystem, not a brand: fund the boring controls (tested immutable backups, segmentation, identity hygiene), prepare for the disclosure era, and treat sector-level interdependence as a resilience parameter.

Keywords: ransomware; ransomware-as-a-service; Operation Cronos; LockBit; cyber resilience; affiliate churn; NIS2; digital trust

Contribution statement. This paper makes four contributions: (1) a source-verified timeline and analysis of the 2024 disruption sequence — Operation Cronos, the ALPHV exit scam, affiliate churn, and successor-brand reconstitution — as a natural experiment in adversarial ecosystem resilience; (2) a structural model of the RaaS value chain that explains why brand takedowns displace rather than dismantle the economy; (3) an analysis of the 2024 flagship incidents (Change Healthcare, Synnovis/NHS) showing that recovery and interdependence, not malware sophistication, determined impact; and (4) a resilience-lifecycle framework aligned with NIST CSF 2.0 and the 2024 regulatory instruments, with stakeholder-differentiated controls.

1. Introduction

For a decade, ransomware has been the defining criminal threat to digital trust: the encryption-plus-extortion business model industrialized into a service economy in which specialized developers rent deployable malware to affiliates, access brokers sell entry into networks, and negotiators monetize victim desperation [16][17][18]. By 2023, on-chain ransomware payments had reached a record of roughly one billion dollars [5], and the largest brands had achieved a market concentration that made their names —

LockBit foremost — synonymous with the threat itself [7][6]. In February 2024, that economy received its largest shock to date, and the response of the ecosystem became, in effect, a public experiment in adversarial resilience.

Operation Cronos, announced on 19 February 2024 by the UK National Crime Agency with the FBI, Europol, and international partners, seized LockBit's infrastructure and administration environment, obtained the LockBit source code and keys, and compromised the group's operational security to an extent that law enforcement could publish victim data the cartel had itself collected [1][2][3]. Two days later in the same fortnight, the healthcare payment processor Change Healthcare was attacked by the ALPHV/BlackCat operation — an attack that halted claims processing across much of the U.S. health system, for which a \$22 million ransom was reportedly paid, and whose aftermath included the cartel's *exit scam*: ALPHV's operators took the payment and vanished, leaving affiliates unpaid and a second extortion actor (RansomHub) to re-victimize the same target [13]. Within weeks, LockBit had relaunched on new infrastructure; within months, the brand had been effectively orphaned — its administrator identified and a \$10 million U.S. reward posted for him [4] — while the affiliate pool migrated to successor brands such as RansomHub, which rose to prominence over the following months [6][7]. The payment economy, undeterred, continued to function.

The pattern is theoretically significant. The disruption did not *dismantle* the ransomware economy; it *selected against a brand* while the underlying production function — the affiliate labor market, access-broker supply, laundering infrastructure — persisted and re-bundled. The 2024 flagship incidents reinforce the same lesson from the victim side: the Change Healthcare and Synnovis/NHS disruptions [13][14] were caused by attackers of ordinary technical reputation but extraordinary *consequential* impact, because the victims' recovery capability and sectoral interdependence — not malware sophistication — determined the damage. Together, these observations reframe ransomware defense: the decisive variable in 2024 was not the attacker's code but the defender's resilience, and resilience is measurable, designable, and regulable.

1.1 Research questions

RQ1: What was the verified sequence of 2024 disruptions (Operation Cronos and associated events), and what does each demonstrate about the ecosystem's response repertoire? **RQ2:** What is the structure of the RaaS value chain, and why does brand-level disruption displace rather than dismantle it? **RQ3:** What did the 2024 flagship incidents reveal about the determinants of realized impact? **RQ4:** What resilience-lifecycle controls and 2024 regulatory instruments follow, for defenders and policymakers?

1.2 Contributions

We contribute: (1) a source-verified 2024 disruption timeline with event-level analysis (Section 3, Figure 1, Table 1) (RQ1); (2) a structural model of the RaaS value chain and its churn dynamics (Section 4, Figure 2) (RQ2); (3) incident-based analysis of impact determinants (Section 5) (RQ3); and (4) a resilience-lifecycle framework aligned with NIST CSF 2.0 and mapped to the 2024 regulatory corpus (Section 6, Figure 4, Table 3) (RQ4).

2. Background and Related Work

2.1 Ransomware as an economy

The ransomware literature has evolved from malware-centric analysis — cryptographic detection of encryption behavior [17] — toward characterization of the *social* and *economic* organization of attacks: Conti et al.'s large-scale analysis of ransomware support infrastructures documented the professionalization of the victim-facing side of the economy [16], and the economics literature models ransomware as a market with attacker reputation, victim heterogeneity, and insurance-mediated willingness to pay [18]. The RaaS model divides labor: developers, affiliates, initial access brokers, and money-laundering services, each monetizing a stage of the attack. The policy literature responded with joint defender guidance [9] and, from 2024, with regulatory instruments that convert incident response into disclosure obligations [11][12].

2.2 Measurement from the money side

Blockchain analytics provide the ecosystem's most direct longitudinal measurement: Chainalysis's 2024 Crypto Crime Report estimates on-chain ransomware payments at approximately \$1.1 billion in 2023 — a record, and a reversal of the apparent 2022 decline that analysts attribute to improved tracing of previously unidentified flows and to the resilience of the affiliate economy [5]. Incident-response telemetry adds the victim-side view: Verizon's 2024 DBIR finds ransomware or extortion present in roughly a third of analyzed breaches, with the median time from access to encryption now measured in days [6]; Sophos's 2024 survey documents the cost asymmetry that drives the economy — recovery costs routinely exceeding ransom demands, and backup strategies failing at a non-trivial rate precisely when needed [8]. Microsoft's Digital Defense Report (October 2024) documents the post-Cronos churn we analyze here [7].

2.3 Enforcement against RaaS

Operation Cronos was not the first disruption of a ransomware brand, but its design differed in instructive ways: alongside infrastructure seizure, authorities obtained the builder and source code, penetrated the group's own communications, and ran a sustained counter-operation that published the cartel's internal data [1][2][3]. Subsequent 2024 actions — including Europol's "Endgame" operation against multiple malware families (May 2024) [15] and the identification and reward targeting of LockBit's administrator [4] — extended the pressure from infrastructure to *identity and trust within the criminal ecosystem*, an evolution with implications we return to in Section 6.

2.4 Resilience and regulation

The 2024 regulatory environment operationalized the resilience lesson. NIS2's transposition deadline (17 October 2024) hardened management accountability and 24-hour early-warning incident reporting for essential entities across the EU [11]; the U.S. SEC's cybersecurity disclosure rule (effective September 2023, with the four-business-day Form 8-K material-incident disclosure requirement operative for most registrants from December 18, 2023) requires material-incident disclosure within four business days [12]; NIST CSF 2.0 (February 2024) elevated Governance and sharpened the Recover function's emphasis on tested restoration [10]; and the CISA/NSA/FBI StopRansomware guide consolidated the defensive baseline [9]. These instruments share a premise this paper makes explicit: ransomware is no longer treated as a security failure but as an *organizational resilience failure* — and resilience is auditable.

3. Methodology

The study applies a qualitative event-driven case design in three components.

Disruption-sequence analysis (RQ1). We compiled the 2024 disruption timeline (February–October) from primary and authoritative secondary sources: the law-enforcement announcements of Operation Cronos [1][2][3], the identification and reward announcement for LockBit's administrator [4], Europol's Endgame operation [15], victim-side incident documentation for Change Healthcare [13] and the Synnovis/NHS event [14], and ecosystem assessments from blockchain analytics and industry telemetry [5] [6][7][8]. Each event is recorded with its date, actor class, and documented consequence (Table 1). Where public reporting is contested (e.g., exact affiliate counts), we report ranges as reported and mark uncertainty.

Value-chain structural analysis (RQ2). The RaaS economy was modeled as a four-role production chain — developers, affiliates, access brokers, monetization services — using the attack-economy literature [16][18] and the 2024 telemetry of brand churn [6][7]. The model's purpose is explanatory: to identify which roles the Cronos operation actually degraded and which were untouched.

Resilience synthesis (RQ4). Defensive implications were synthesized into a lifecycle framework aligned with NIST CSF 2.0 functions [10] and mapped to the 2024 regulatory instruments [11][12] and joint guidance [9]. The synthesis is analytical; no new empirical dataset is introduced, and all quantitative claims are attributed to their published sources.

4. The 2024 Disruption Sequence and Ecosystem Response (RQ1, RQ2)

4.1 The verified timeline

Figure 1 presents the sequence; Table 1 records the events with sources. The density of the February–June window is the study's first finding: within roughly ninety days, the field's dominant brand was seized, the second-most significant cartel self-destructed in the largest ransom of the period, a successor brand was born, and a sector-defining incident demonstrated the stakes. The 2024 ransomware "year" was, in effect, decided in a single quarter.

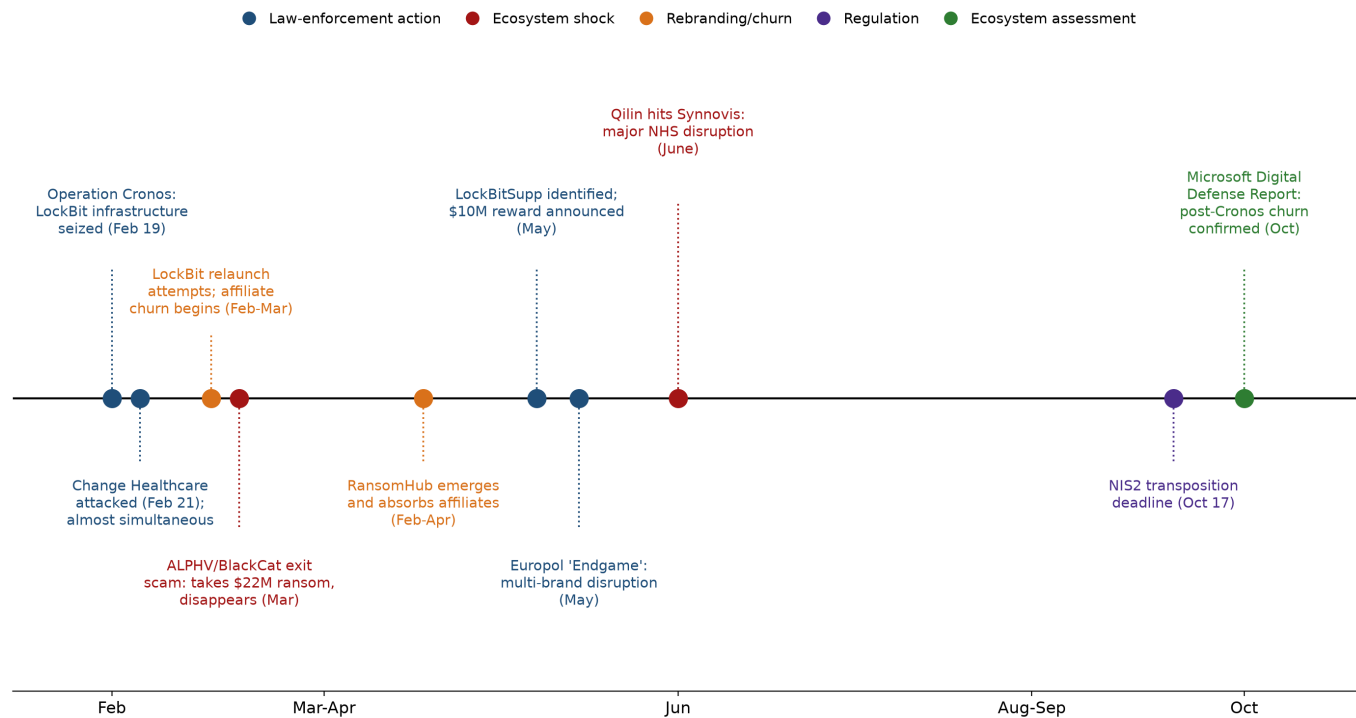


Figure 1. The 2024 ransomware disruption sequence: law-enforcement action, ecosystem shocks, churn, and regulation (sources per Table 1).

4.2 Operation Cronos: what was actually disrupted

The Cronos operation degraded LockBit at three layers simultaneously. *Infrastructure*: servers and leak sites were seized, and takedown notices replaced victim pages. *Product*: authorities obtained the LockBit builder, source code, and decryption keys — enabling not only victim remediation but the publication of decryption resources and the exposure of unpatched flaws in the malware itself [1][3]. *Trust and identity*: the sustained counter-operation culminated in the identification of the administrator and the posting of a \$10 million reward [4], converting the brand's internal anonymity — the asset that lets an RaaS operator retain affiliates — into a liability. The operation also revealed the cartel's own operational dependence on trust: law enforcement's ability to publish LockBit's victim data demonstrated that the group's assurance to affiliates and victims alike had been compromised.

4.3 The response repertoire: displacement, not dismantlement

The ecosystem's reaction followed a documented script (Figure 2). **Relaunch**: LockBit announced continued operations on new infrastructure within days — plausible, given that the developer core and affiliate relationships survived the infrastructure seizure [6] [7]. **Churn**: the affiliate pool — the economy's actual productive labor — migrated among successor brands; RansomHub, founded in early 2024, rose through the spring partly by absorbing displaced LockBit affiliates [6][7]. **Diversification**: access brokers, negotiators, and laundering services continued operating largely brand-agnostically, since their services are substitutable across brands. The outcome is visible in the payment data (Figure 3): 2023's record flows [5] were not interrupted by the 2024 enforcement wave; industry telemetry recorded continued — and in some windows increased — ransomware activity under reconstituted brands [6][7][8]. Table 2 records the post-Cronos status of each value-chain role.

The ransomware-as-a-service value chain after Operation Cronos

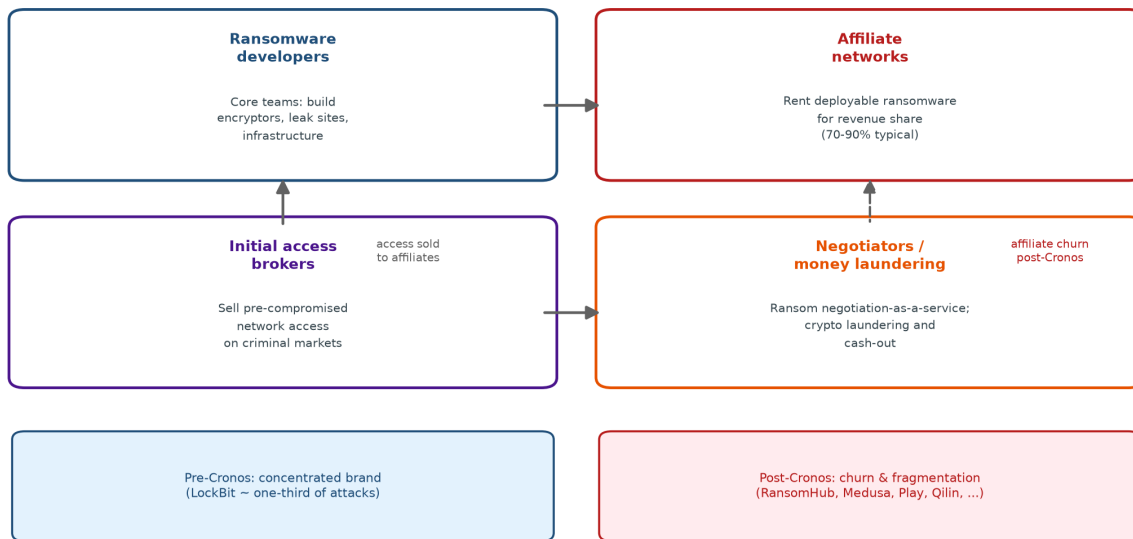


Figure 2. The RaaS value chain and its post-Cronos dynamics: affiliate churn re-bundles production under successor brands while specialized services persist.

Ransomware payment flows as reported by Chainalysis (2024 Crypto Crime Report)

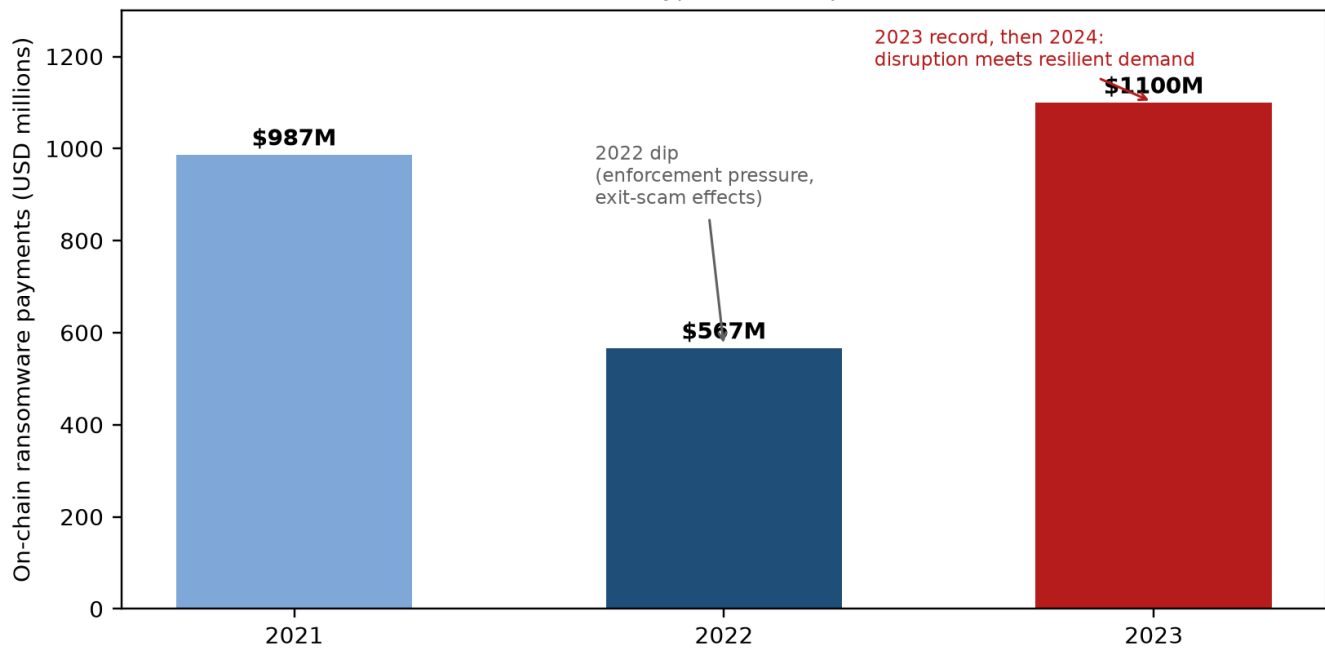


Figure 3. On-chain ransomware payment flows as reported by Chainalysis [5]: the 2023 record preceded, and was not interrupted by, the 2024 enforcement wave.

Value-chain role	Function in the economy	Post-Cronos status (2024)
Developers / brands	Build encryptors, leak sites, negotiation infrastructure	Brand-level displacement (LockBit orphaned; ALPHV exit scam); successor brands emerged
Affiliates	Execute attacks in exchange for revenue share	Persisted; migrated to successor brands (e.g., RansomHub) [6][7]

Initial access brokers	Sell pre-compromised network access	Persisted; largely brand-agnostic
Negotiation & laundering services	Monetize and settle payments	Persisted; substitutable across brands

Table 2. Value-chain roles and their post-Cronos status.

The structural reading is direct. A brand-level takedown attacks the *most visible* layer of the value chain (the developer/brand) while leaving the *labor market* (affiliates) and the *commodity inputs* (access, laundering) intact. Because the affiliate's binding constraint is a working deployable product and a launderable payment channel — both available from multiple brands — displacement is the equilibrium outcome. This is the ransomware economy's resilience: the same property defenders cultivate in their own systems, present at scale in the adversary's.

Event	Date (2024)	Actor class	Documented consequence	Source
Operation Cronos announced	Feb 19	Law enforcement	LockBit infrastructure seized; builder, source code, and keys obtained; per the NCA/ Europol releases: 34 servers, 14,000+ rogue accounts identified for removal, 200+ cryptocurrency accounts frozen, 1,000+ decryption keys obtained, and a network of 194 affiliates identified	[1][2][3]
Change Healthcare attack	Feb 21	Ecosystem shock	U.S. healthcare claims/eligibility processing disrupted at national scale	[13]
ALPHV/BlackCat exit scam	Mar	Ecosystem shock	Reported \$22M ransom taken; cartel disappears; affiliates left unpaid	[13]
LockBit relaunch attempts	Feb-Mar	Rebranding/ churn	Continued operations claimed on new infrastructure; brand credibility degraded	[6][7]
RansomHub emergence	Feb-Apr	Rebranding/ churn	Successor brand rises, absorbing displaced LockBit affiliates	[6][7]
LockBit administrator identified; \$10M reward	May	Law enforcement	"LockBitSupp" named; internal trust of the cartel degraded	[4]
Operation Endgame	May	Law enforcement	Multi-brand disruption of malware dropper infrastructure	[15]
Synnovis/NHS disruption	Jun	Ecosystem shock	Pathology services for London NHS trusts disrupted; thousands of appointments postponed	[14]
NIS2 transposition deadline	Oct 17	Regulation	Management accountability; 24h early warning / 72h notification for essential entities	[11]
Microsoft Digital Defense Report	Oct	Assessment	Documents post-Cronos affiliate churn and successor-brand reconstitution	[7]

Table 1. The 2024 disruption sequence: events, dates, actor classes, and documented consequences.

5. Impact Determinants: The 2024 Flagship Incidents (RQ3)

5.1 Change Healthcare: single points of systemic failure

The Change Healthcare attack (February 2024) halted claims and eligibility processing across a substantial share of the U.S. healthcare system, and its aftermath became a public case study in ecosystem mechanics: the reported \$22 million ransom paid to ALPHV [13], the cartel's exit scam leaving the payment effectively worthless in trust terms, and the second extortion of the same victim by a successor group over stolen data [13]. The incident's impact determinant was not malware sophistication — it was *concentration*: one intermediary processing a critical national workflow, with recovery that measured in weeks against a sector's real-time dependencies. Congressional testimony and regulatory follow-up focused, tellingly, on resumption of service and modernization of the payments architecture — resilience variables, not cryptographic ones [13].

5.2 Synnovis/NHS: interdependence as an attack surface

In June 2024, the Qilin group's attack on the Synnovis pathology partnership disrupted laboratory services for London NHS trusts, postponing thousands of appointments and forcing the sector into mutual-aid operations for weeks [14]. The malware was unremarkable; the impact flowed through *interdependence* — laboratory data services embedded in clinical pathways. The episode illustrates that in interdependent sectors, the marginal resilience of any single organization is capped by the weakest partner in its service chain, and that sector-level coordination (mutual aid, shared recovery priorities) is a control in its own right.

5.3 Synthesis: what determines realized impact

Across the 2024 record, three determinants of realized impact recur, in descending order of importance: (1) **recovery capability** — the presence and restorability of immutable, offline-tested backups [8][9]; (2) **containment** — segmentation and identity hygiene that bound the blast radius of initial access [6][9]; and (3) **interdependence management** — the organization's position in sectoral service chains and its preparedness for mutual-aid operation [13][14]. Malware family, encryption speed, and brand affiliation — the variables that dominate threat reporting — barely register as impact determinants. This is the empirical core of the paper's defensive thesis.

6. Resilience Foundations for the Post-Cronos Era (RQ4)

6.1 The resilience lifecycle

Figure 4 presents the framework: four lifecycle phases — *Anticipate* (asset inventory, patching, identity hygiene, threat-informed defense), *Withstand* (segmentation, immutable offline-tested backups, least privilege), *Absorb & Operate* (incident response, containment, sector mutual aid), and *Recover & Learn* (tested restoration, disclosure compliance, threat-intel feedback) — aligned with NIST CSF 2.0 functions [10] and grounded in the impact determinants of Section 5.3. The framework's orientation follows the 2024 evidence: investment priority descends from *Recover* through *Absorb* to *Withstand* and *Anticipate*, inverting the perimeter-centric spending pattern of the pre-ransomware decade [8][9].

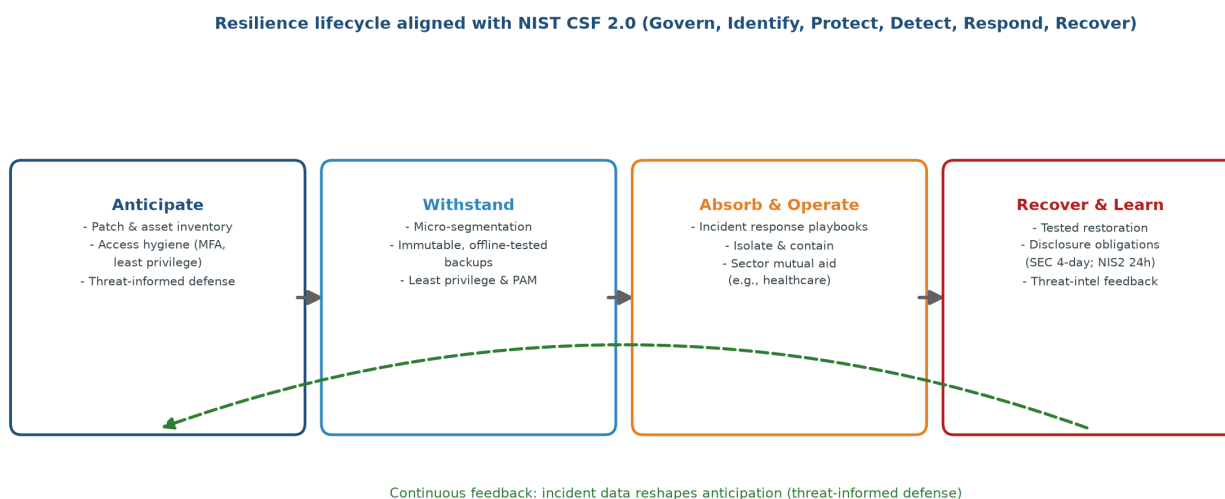


Figure 4. The resilience lifecycle for ransomware defense, aligned with NIST CSF 2.0 [10] and the 2024 regulatory instruments [11][12].

6.2 The 2024 disclosure era

Regulation converted resilience from private virtue into public accounting. The SEC rule requires material-incident disclosure within four business days [12]; NIS2 requires 24-hour early warning and 72-hour notification for essential entities, with management personally accountable [11]. These obligations change defender behavior in two ways that matter for ransomware: they force *early* executive engagement in ransomware incidents (when containment decisions are still open), and they make recovery capability — the decisive variable — visible to boards, regulators, and insurers. Table 3 maps the instruments to lifecycle phases.

6.3 Policy against an ecosystem, not a brand

The Cronos year also teaches policymakers. Because displacement is the equilibrium response to brand takedowns (Section 4.3), enforcement should be evaluated against ecosystem variables rather than brand headlines: affiliate *migration costs* (e.g., continued pressure on hosting and laundering infrastructure), *trust within the criminal economy* (the identification of LockBit's administrator

[4] and the ALPHV exit scam [13] both degrade the trust that RaaS depends on), and the *victim-side economics* that set demand [5] [18]. The 2024 sequence suggests the enforcement frontier is shifting from seizing servers to *raising the cost of re-bundling* — a slower, less visible, and plausibly more durable strategy [1][15].

Lifecycle phase	Representative controls	2024 instrument alignment
Anticipate	Asset inventory; patching; phishing-resistant MFA; threat-informed defense	CSF 2.0 Govern/Identify [10]; StopRansomware guide [9]
Withstand	Micro-segmentation; immutable, offline-tested backups; least privilege; PAM	CSF 2.0 Protect [10]; [9]
Absorb & Operate	Incident-response playbooks; containment; sector mutual aid	NIS2 24h early warning [11]; healthcare mutual aid practice [14]
Recover & Learn	Tested restoration; disclosure (SEC: 4 business days; NIS2: 72h); threat-intel feedback	SEC rule [12]; NIS2 [11]; CSF 2.0 Recover [10]

Table 3. Resilience lifecycle controls mapped to the 2024 regulatory instruments [9][10][11][12].

7. Discussion

7.1 Adversarial resilience as a design mirror

The ecosystem's post-Cronos behavior — redundancy, rapid reconstitution, churn under pressure — is a textbook resilient-systems design, executed by the adversary. Defenders can read it as a mirror: the properties that made the ransomware economy survive its worst month (no single point of failure, substitutable components, tested reconstitution) are precisely the properties the resilience lifecycle asks of victims. Digital trust in this domain is thus a *symmetric* engineering discipline: whichever side builds better redundancy and faster reconstitution wins the exchange.

7.2 The disclosure dividend

The 2024 disclosure obligations, often framed as compliance burdens, function analytically as ecosystem instrumentation: mandatory early reporting and sector sharing turn individual incidents into the population-level telemetry (sectoral patterns, initial-access trends, affiliate behavior) that both defenders and enforcers need [6][11][12]. The paper's recommendation is therefore to treat disclosure data as a resilience input — closing the loop of the lifecycle's Learn phase — rather than as a legal endpoint.

7.3 Honest limits of the defensive thesis

Two cautions temper the resilience-first thesis. First, prevention is not worthless: every avoided incident saves the full disruption cost, and identity hygiene (phishing-resistant MFA, least privilege) remains the cheapest control per unit of risk reduction [9]. Second, resilience has distributional limits: small organizations and under-resourced sectors (municipalities, hospitals in low-margin systems) cannot buy their way to the recovery posture of large enterprises — which is why sector-level mutual aid and national coordination appear in the framework as first-class controls, not afterthoughts [13][14].

8. Limitations and Threats to Validity

Construct validity. The value-chain model is a simplification; real ecosystems include overlapping roles (affiliate-developers, access-broker-affiliates) and the model should be read as an analytical scaffold, not an organizational chart. **Internal validity.** Event dating and consequence attribution rely on law-enforcement and industry reporting, which have institutional incentives; contested figures are reported as attributed ranges. **External validity.** The 2024 sequence is one natural experiment in one year; generalization to other years and ecosystems (e.g., non-Russian-language operations) is plausible but not demonstrated. The synthetic-free analysis introduces no new quantitative data, so statistical threats do not arise; interpretive threats do. **Reliability.** Leak-site and telemetry sources fluctuate; we privileged primary law-enforcement documents, victim testimony, and established annual reports [1][2][3][4] [13][14][5][6][7][8]. **Temporal scope.** The analysis closes at the fourth quarter of 2024; the ecosystem's subsequent evolution and the enforcement effects of 2024 operations are outside scope.

9. Conclusion

Operation Cronos and the 2024 disruption sequence constitute the clearest demonstration to date that the ransomware economy is an *ecosystem* — resilient, re-bundling, and indifferent to the fate of individual brands. The affiliates displaced by Cronos were not dismantled; they were re-hired. The record payment year preceded the record enforcement year, and the year's most damaging incidents were produced by unremarkable malware meeting unrecoverable architectures and fragile interdependencies. The defensive consequence is equally clear. Impact in the 2024 record was determined by recovery capability, containment, and interdependence management — all designable, all regulable, all testable. Organizations should build against the ecosystem they actually face: fund tested immutable restoration, harden identity and segmentation, rehearse sector-level mutual aid, and meet the disclosure era as an accountability instrument rather than a legal hazard. Policymakers should measure enforcement against the ecosystem's resilience variables — affiliate migration costs and criminal-economy trust — rather than the lifespan of a brand. Resilience, in the end, is the only variable in the ransomware exchange that defenders control completely; 2024 made the case for spending there.

Declarations

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

CRedit contribution statement. Anushka Nehra: conceptualization, investigation, event reconstruction, writing – original draft, writing – review & editing. Nishu Bansal: conceptualization, validation, supervision, writing – review & editing (corresponding author).

Competing interests. The authors declare no competing interests.

Ethics and dual-use. This paper analyzes publicly documented enforcement actions and incidents only. It contains no attack tooling, no negotiation guidance for attackers, and no information that materially enables criminal activity; incident details are limited to publicly reported facts appropriate for defensive analysis.

Data and code availability. No new datasets were generated. All quantitative claims are attributed to their published sources [5][6][7][8]; the event timeline (Table 1) is reconstructed from the cited primary documents [1][2][3][4][13][14][15].

AI assistance declaration. The authors used AI-based tools to assist with literature discovery, source verification, figure preparation, and manuscript drafting; all content was reviewed, verified against primary sources, and approved by the authors, who take full responsibility for the work.

References

- [1] National Crime Agency (UK), "Operation Cronos: international action against the LockBit ransomware group," Feb. 19, 2024. [Online]. Available: <https://www.nationalcrimeagency.gov.uk/news>
- [2] Europol, "Law enforcement disrupt world's biggest ransomware operation," Feb. 20, 2024. [Online]. Available: <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>
- [3] U.S. Department of Justice, "Justice Department Announces Court-Authorized Disruption of the LockBit Ransomware Group," Press Release, Feb. 20, 2024. [Online]. Available: <https://www.justice.gov/news>
- [4] U.S. Department of State, "Rewards for Justice: Reward Offer for Information on LockBit Ransomware Administrator Dmitry Khoroshev," May 2024. [Online]. Available: <https://www.rewardsforjustice.net>
- [5] Chainalysis, "The 2024 Crypto Crime Report," Jan. 2024. [Online]. Available: <https://www.chainalysis.com/reports/2024-crypto-crime-report/>
- [6] Verizon Business, "2024 Data Breach Investigations Report (DBIR)," May 2024. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>
- [7] Microsoft, "Microsoft Digital Defense Report 2024," Oct. 2024. [Online]. Available: <https://www.microsoft.com/security/security-insider>
- [8] Sophos, "The State of Ransomware 2024," Apr. 2024. [Online]. Available: <https://www.sophos.com>
- [9] Cybersecurity and Infrastructure Security Agency, National Security Agency, and Federal Bureau of Investigation, "StopRansomware Guide," Sep. 2023. [Online]. Available: <https://www.cisa.gov/stopransomware>
- [10] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
- [11] Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2), Official Journal of the European Union, Dec. 2022 (transposition deadline 17 October 2024).
- [12] U.S. Securities and Exchange Commission, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Final Rule, Release No. 33-11216, adopted Jul. 26, 2023, effective Sep. 5, 2023; the Form 8-K material-incident disclosure requirement became operative for most registrants on Dec. 18, 2023.
- [13] A. Witty, "Written Testimony before the U.S. House Committee on Energy and Commerce on the Change Healthcare Cyberattack," May 1, 2024. [Online]. Available: <https://energycommerce.house.gov>

- [14] NHS England, "Statement on the cyber incident affecting Synnovis and south east London providers," Jun. 2024. [Online]. Available: <https://www.england.nhs.uk>
- [15] Europol, "Operation Endgame: major operation disrupts malware dropper infrastructure," May 2024. [Online]. Available: <https://www.europol.europa.eu>
- [16] M. Conti, A. Gangwal, and S. Ruj, "On the economic significance of ransomware campaigns: a Bitcoin transactions perspective," *Computers & Security*, vol. 79, Nov. 2018. doi: 10.1016/j.cose.2018.08.008.
- [17] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the Gordian knot: a look under the hood of ransomware attacks," in *Proc. 12th Int. Conf. on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2015)*, LNCS 9148, 2015.
- [18] A. Laszka, S. Farhang, and J. Grossklags, "On the economics of ransomware," in *Decision and Game Theory for Security - 8th International Conference, GameSec 2017*, Vienna, Austria, Springer, 2017. [Online]. Available: <https://arxiv.org/abs/1707.06247>