A Codebook for Police and IR Dataset

This appendix provides the coding protocol used to extract variables from unstructured police and incident response (IR) reports. Variables are defined based on observable evidence in the reports and aligned with the six-stage negotiation framework. Coding prioritizes precision over recall: variables are recorded only when explicitly supported by the source data. Ambiguous or incomplete cases are coded as missing.

A.1 General Coding Principles

- **Unit of analysis:** Individual ransomware incident affecting an organization.
- **Inclusion criteria:** Cases must explicitly describe both (i) file encryption and (ii) a corresponding ransom demand note or contact details to receive this information from the attackers.
- **Exclusion criteria:** Attempted intrusions without encryption, incidents targeting individuals, and cases without a ransom demand or contact details.
- **Deduplication:** Duplicate records referring to the same incident are identified using victim identifiers, timestamps, and contextual descriptions, and merged into a single case.
- **Missing data:** Variables are coded as missing (*NA*) when no explicit information is available.

A.2 Variable Definitions and Coding Rules

1a. Revenue (log).

- **Definition:** Estimated yearly revenue of the victim organization.
- **Coding:** Recorded as numerical value where available; $\log_{10}$ transformation applied in analysis.
- **Criteria:** Based on victim business information from the Dutch Chamber of Commerce, as available in the Dutch police information system. For multinational organizations, total estimated annual revenue is used.

1b. RaaS affiliation.

- **Definition:** Whether the ransomware group is identified as operating under a ransomware-as-a-service (RaaS) model.
- **Coding:** 1 = known RaaS group; 0 = non-RaaS or unknown.
- **Criteria:** A group is coded as RaaS only when explicit evidence of affiliate recruitment is observed, such as public advertisements on darknet forums, leak sites, or ransomware group blogs. Secondary sources are used only when they provide verifiable evidence (e.g., screenshots) of such advertisements, in line with [52].

1c–1e. Backup status.

- **Definition:** Availability and usability of backups at the time of the incident.
- **Coding:**
  - 0 = no backups
  - 1 = backups destroyed/unusable
  - 2 = partially recoverable backups
  - 3 = fully recoverable backups
- **Criteria:** Based on explicit statements regarding backup functionality.

1f. Data exfiltration.

- **Definition:** Whether data was exfiltrated during the attack.
- **Coding:** 1 = yes; 0 = no.
- **Criteria:** Data exfiltration is coded when explicitly evidenced by (i) monitoring logs indicating data transfer, or (ii) exposure of victim data in negotiation chats or on the attacker's public leak site.

1g. Negotiation (attacker).

- **Definition:** Whether the attacker allowed negotiation beyond an initial ransom demand.
- **Coding:** 1 = negotiation possible (e.g., contact details provided); 0 = fixed demand only (as stated in the ransom note).
- **Criteria:** Negotiation is coded as present when the attacker provides a communication channel (e.g., chat link, email address) or explicitly invites interaction. It is coded as absent when only a fixed ransom demand is presented without any means of communication.

2a. Cyber insurance.

- **Definition:** Whether the victim had cyber insurance relevant to ransomware.
- **Coding:** 1 = yes; 0 = no.
- **Criteria:** Based on explicit statements regarding insurance in the Police or IR report.

2b. IR firm involvement.

- **Definition:** Whether a professional incident response firm was involved.
- **Coding:** 1 = yes; 0 = no.
- **Criteria:** Based on either (i) included in the IR dataset, or (ii) explicitly mentioned in Police report.

2c. Negotiation (victim).

- **Definition:** Whether the victim initiated or engaged in communication with the attacker.
- **Coding:** 1 = yes; 0 = no.
- **Criteria:** Based on explicit statements regarding negotiation in the Police or IR report.

3a. Negotiation duration (log).

- **Definition:** Duration of attacker-victim communication.
- **Coding:** Number of days between first and last recorded communication; $\log_{10}$ transformation used in analysis.
- **Criteria:** Based on explicit statements regarding negotiations in the Police or IR report, or negotiations themselves if provided with time stamps.

3b. Initial ransom demand (log).

- **Definition:** Initial ransom demand communicated by the attacker.
- **Coding:** Recorded in EUR where available or converted from USD, Bitcoin, or other currencies using the exchange rate on the date of the incident; $\log_{10}$ transformation applied.
- **Criteria:** Must be explicitly stated in report or provided negotiation chats.

3c. Discount offered.

- **Definition:** Whether the attacker reduced the ransom demand during negotiation.
- **Coding:** 1 = reduction between initial and final demand observed; 0 = no reduction observed.
- **Criteria:** Requires explicit documentation of both initial and final demand.

4. Discount size.

- **Definition:** Size of reduction between initial and final ransom demand.
- **Coding:** Calculated as difference between initial and final demand.
- **Criteria:** Only coded when both demands are available, otherwise coded as missing (*NA*).

5. Payment.

- **Definition:** Whether the victim paid the ransom.
- **Coding:** 1 = payment confirmed; 0 = explicitly not paid.
- **Criteria:** Payment is coded when (i) the victim explicitly reports having paid the ransom, (ii) a (bitcoin) transaction is confirmed by the police or IR firm and attributed to the incident, or (iii) payment is explicitly indicated in the negotiation chat.

6. Post-payment outcomes.

- **Definition:** Outcomes following ransom payment.
- **Coding:**
  - **Decryptor failure:** No key delivered or key non-functional.
  - **Renegotiation:** Additional payment demanded after initial settlement.
  - **Reinfection:** Subsequent ransomware incident affecting same victim.
- **Coding:** Each outcome coded as 1 = observed; 0 = not observed.
- **Criteria:** Must be explicitly described in reports.

B Factors Influencing Negotiations (RQ1): Regression analysis results

Model fit. For the regression analyses of the six-stage negotiation framework, we report the following fit statistics. For M1 (attacker willingness to negotiate, logit) the McFadden's pseudo-R^2 is 0.2438. For M2 (victim willingness to negotiate, logit) the McFadden's pseudo-R^2 is 0.0549. For M3 (discount offered, logit) the McFadden's pseudo-R^2 is 0.2712. For M4 (discount size, OLS) the adjusted R^2 is 0.3028 (with a multiple R^2 of 0.3415). Finally, for M5 (payment decision, logit) the McFadden's pseudo-R^2 is 0.3369.

For logistic models, McFadden's pseudo-R^2 values between approximately 0.20 and 0.40 are generally considered indicative of good model fit in applied settings, particularly for behavioral and decision-making processes. The reported values therefore suggest substantial explanatory power for models capturing attacker behavior, discounting, and payment decisions, while lower fit for victim negotiation initiation reflects greater heterogeneity at earlier stages of the process.

Table 6: Stage-wise regression coefficients (β) and p-values across the first five stages of ransomware negotiation and payment. Cells report estimated coefficients with p-values in parentheses; "." indicates the predictor is not applicable at that stage.

Predictor	M1: Attacker negotiation	M2: Victim negotiation	M3: Discount offered	M4: Discount size	M5: Payment
Structural and attack characteristics (inputs from Stage 1 onward)					
1a. Revenue (log)	0.04 (0.624)	0.30 (0.048)*	0.39 (0.116)	−0.12 (0.001)**	0.44 (0.085)$^{\circ}$
1b. RaaS affiliation	0.31 (0.207)	−0.17 (0.654)	0.75 (0.159)	−0.17 (0.005)**	−0.19 (0.723)
1c. Backups: Unrecoverable (vs No Backups)	0.86 (0.015)*	0.10 (0.831)	0.36 (0.648)	−0.00 (0.986)	0.61 (0.353)
1d. Backups: Partial (vs No Backups)	0.91 (0.010)*	−0.82 (0.127)	0.14 (0.875)	−0.01 (0.960)	−0.84 (0.246)
1e. Backups: Recoverable (vs No Backups)	0.72 (0.029)*	−1.60 (0.007)**	−2.15 (0.033)*	0.20 (0.151)	−2.47 (0.002)**
1f. Data exfiltration	0.66 (0.044)*	0.77 (0.102)	0.89 (0.142)	−0.16 (0.026)*	0.10 (0.878)
Stage 1 outcome / later-stage inputs					
1g. Negotiation (attacker)	*Outcome*	.	.	−0.07 (0.537)	0.18 (0.775)
Stage 2: Victim-side preparedness and response					
2a. Cyber insurance	.	0.38 (0.472)	−0.09 (0.885)	−0.11 (0.039)*	0.14 (0.832)
2b. IR firm involvement	.	3.47 (< .001)***	2.04 (0.004)**	−0.04 (0.696)	0.06 (0.945)
2c. Negotiation (victim)	.	*Outcome*	.	0.08 (0.679)	4.80 (0.001)**
Stage 3: Interaction dynamics					
3a. Negotiation duration (log)	.	.	1.22 (< .001)***	0.08 (0.061)$^{\circ}$	−1.63 (0.012)*
3b. Initial ransom demand (log)	.	.	.	0.50 (< .001)***	−0.25 (0.068)$^{\circ}$
3c. Discount offered	.	.	*Outcome*	.	1.41 (0.039)*
Stage 4: Price adjustment					
4. Discount size (log)	.	.	.	*Outcome*	−0.30 (0.343)
Stage 5: Payment					
5. Payment	.	.	.	.	*Outcome*

Notes: Logit models are used for M1–M3 and M5, OLS for M4. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{\circ}p < 0.10$.

C Negotiation Strategy and Discount (RQ2): Ransomware Groups

Negotiation outcomes per ransomware group. Table 7 reports descriptive negotiation outcomes by ransomware group in the transcript dataset (N=237). The table highlights substantial heterogeneity in initial demands, negotiation rates, discounting, and observed payments across groups, but several groups have small sample sizes so group-level percentages should be interpreted cautiously. These descriptives motivate the transcript-based regressions in Section 4.2, where we model discount offering and payment conditional on negotiation length.

Table 7: Negotiation outcomes per ransomware group (source: ransomware.live, N=237)

Group	*n*	Init. %	Paid %	Negot. %	Med. Init	Mean Init	Med. Neg	Mean Neg	Med. Paid	Mean Paid	Mean Disc. % (Med.)
Akira	61	67.2	32.8	44.3	390k	948k	150k	248k	150k	256k	22.4 (0.0)
Avaddon	7	85.7	14.3	57.1	190k	304k	90k	103k	1.3k	1.3k	32.3 (33.3)
Avos	1	100.0	0.0	100.0	150k	150k	85k	85k	–	–	43.3 (43.3)
Babuk	2	100.0	0.0	100.0	700k	700k	293k	293k	–	–	64.4 (64.4)
BlackBasta	5	80.0	80.0	100.0	600k	1.09M	300k	632k	225k	275k	31.2 (28.6)
BlackMatter	2	100.0	0.0	100.0	10.0M	10.0M	14.3M	14.3M	–	–	-95.0 (-95.0)
Cloak	2	0.0	0.0	0.0	–	–	–	–	–	–	0.0 (0.0)
Conti	32	93.8	31.2	65.6	1.04M	7.93M	325k	1.68M	171k	224k	40.9 (40.0)
Darkside	5	80.0	60.0	60.0	1.50M	3.40M	250k	283k	250k	283k	24.7 (0.0)
Dragonforce	14	50.0	0.0	21.4	1.01M	859k	124k	464k	–	–	5.8 (0.0)
Hive	8	100.0	0.0	62.5	1.10M	3.78M	276k	3.98M	–	–	21.4 (15.4)
Hunters International	1	100.0	0.0	0.0	10.0M	10.0M	–	–	–	–	0.0 (0.0)
Mallox	3	66.7	33.3	100.0	28.8k	28.8k	20k	23.3k	19.9k	19.9k	6.7 (0.1)
NoEscape	2	50.0	0.0	0.0	80k	80k	–	–	–	–	0.0 (0.0)
Qilin	2	0.0	0.0	0.0	–	–	–	–	–	–	0.0 (0.0)
REvil	20	70.0	35.0	50.0	2.75M	3.12M	290k	425k	280k	348k	34.9 (20.6)
RansomHub	1	0.0	0.0	0.0	–	–	–	–	–	–	0.0 (0.0)
Ranzy	2	0.0	0.0	0.0	–	–	–	–	–	–	0.0 (0.0)
RunSomeWares	1	0.0	0.0	0.0	–	–	–	–	–	–	0.0 (0.0)
fog	6	100.0	50.0	50.0	245k	329k	150k	917k	150k	917k	-3.7 (12.5)
lockbit3.0	45	91.1	6.7	31.1	1.40M	5.80M	1.00M	3.11M	40k	40k	7.7 (0.0)
mount-locker	1	100.0	0.0	100.0	9.00M	9.00M	4.12M	4.12M	–	–	54.3 (54.3)
trinity	14	42.9	7.1	0.0	30k	139k	–	–	15k	15k	0.0 (0.0)