

Date: 1<sup>st</sup> October-2026

**RANSOMWARE AS AN ECONOMIC CRIME: A DECISION-THEORETIC  
MODEL OF THE EXTORTION TRANSACTION AND AN EVALUATION OF  
DETERRENCE INSTRUMENTS**

**Odilov O.F.<sup>1,a</sup>, Bobonazarova M.Sh.<sup>1,b</sup>**

**Ashirmurotov M.N.<sup>1,c</sup>, Poziljonov O.U.<sup>1,d</sup>**

<sup>1</sup>Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

**Abstract.** This article analyses extortion by means of malicious encryption — ransomware — as an economic crime whose persistence is determined not by the cryptographic strength of the attack but by the structure of the incentives facing the victim, the offender and the state. The extortion transaction is formalised as a sequential decision problem in which the victim minimises expected loss over three branches: recovery from backup, payment of the ransom and refusal without recovery. The condition under which payment is rational for an individual victim is derived, and it is shown that this condition is satisfied in a wide region of the parameter space, so that the aggregate persistence of the offence is a predictable consequence of individually rational behaviour rather than of negligence.

**Keywords:** ransomware, extortion, economics of crime, decision model, double extortion, cryptocurrency, deterrence, incident reporting, backup, critical infrastructure.

**Annotatsiya.** Ushbu maqolada zararli shifrlash vositasida sodir etiladigan tovlamachilik — ransomware — iqtisodiy jinoyat sifatida tahlil qilinadi; uning barqarorligi hujumning kriptografik mustahkamligi bilan emas, balki jabrlanuvchi, jinoyatchi va davlat oldidagi ragʻbatlar tuzilishi bilan belgilanishi asoslanadi. Tovlamachilik bitimi jabrlanuvchi kutilayotgan zararni uchta tarmoq — zaxira nusxadan tiklash, toʻlovni amalga oshirish va tiklanmasdan rad etish — boʻyicha minimallashtiriladigan ketma-ket qaror masalasi koʻrinishida formallashtiriladi. Alohida jabrlanuvchi uchun toʻlov oqilona boʻladigan shart keltirib chiqariladi va bu shart parametrlar fazosining keng sohasida bajarilishi, demak jinoyatning umumiy barqarorligi beparvolikning emas, balki individual oqilona xulq-atvorning kutilgan natijasi ekanligi koʻrsatiladi.

**Kalit soʻzlar:** ransomware, tovlamachilik, jinoyat iqtisodiyoti, qaror modeli, ikki tomonlama tovlamachilik, kriptoalyuta, tiyish, insidentlar haqida xabar berish, zaxira nusxa, kritik infratuzilma.

**Introduction.** Extortion by means of malicious encryption occupies an unusual position among computer crimes. Technically it is unremarkable: it employs standard symmetric and asymmetric primitives in the manner for which they were designed, and the encryption itself contains no novelty whatever. Its distinguishing feature is economic. Unlike the theft of data, which requires the offender to find a buyer and to accept whatever the market offers, encryption creates a buyer who is already identified, whose valuation of the asset is known to be high and who cannot obtain the asset from any other supplier. The



Date: 1<sup>st</sup> October-2026

offender does not sell stolen property; the offender sells back to the owner the use of property that has never left the owner's possession.

The consequence is a stable criminal business model, and the empirical record bears this out. Payments traced on public distributed ledgers amounted to approximately 820 to 900 million United States dollars in 2025, against a comparable figure for 2024 [1]. Over the same period the share of attacked organisations that paid fell to a record low of 28 per cent while the median payment rose from 12,738 to 59,565 dollars, and the number of claimed attacks increased by approximately half [1]. These three movements appear contradictory and are not: they are the joint outcome of a shift in the offender's target selection, and the model developed below accounts for them within a single framework.

The harm extends well beyond the ransom. The Internet Crime Complaint Center recorded more than 3,600 ransomware complaints in 2025 with confirmed losses of 32.3 million dollars and identified 63 new variants, with incidents reported across all sixteen sectors of critical infrastructure and concentrated in health care, manufacturing, financial services, government and information technology [2]. A single incident against a manufacturer in 2025 is estimated to have caused economic damage exceeding 2.5 billion dollars, a figure that bears no relation to any ransom that might have been demanded [1]. The average total cost of a data breach reached 4.99 million dollars globally and 11.5 million in the United States, with a mean time to identify and contain of 247 days [3]. The ransom, in other words, is a small and sometimes negligible component of the loss, which is precisely why a policy framed solely around whether victims pay addresses a secondary variable.

The question this article addresses is why the offence persists despite a decade of technical countermeasures and a falling payment rate, and which instruments actually reduce its profitability. The contribution is fourfold. First, the extortion transaction is formalised as a sequential decision problem and the condition under which payment is individually rational is derived. Second, the offender's revenue-maximising problem is stated and the observed shift towards large victims and double extortion is derived as its solution. Third, the model is calibrated against the reported and the independently measured data for 2024–2025. Fourth, four classes of deterrence instrument are evaluated against the parameters of the model, and those that alter the offender's revenue function are distinguished from those that do not.

**Literature review and methodology.** The economic treatment of crime originates with Becker, who modelled the decision to offend as a comparison of expected gain with the product of the probability of apprehension and the severity of sanction, and established that the probability of apprehension is the stronger deterrent [4]. The application of this framework to ransomware begins with the observation that the offence has the structure of a bilateral bargaining problem under incomplete information rather than of a simple appropriation.

Kharraz and co-authors provided the first systematic technical characterisation of the malware family, analysing more than a thousand samples and showing that the



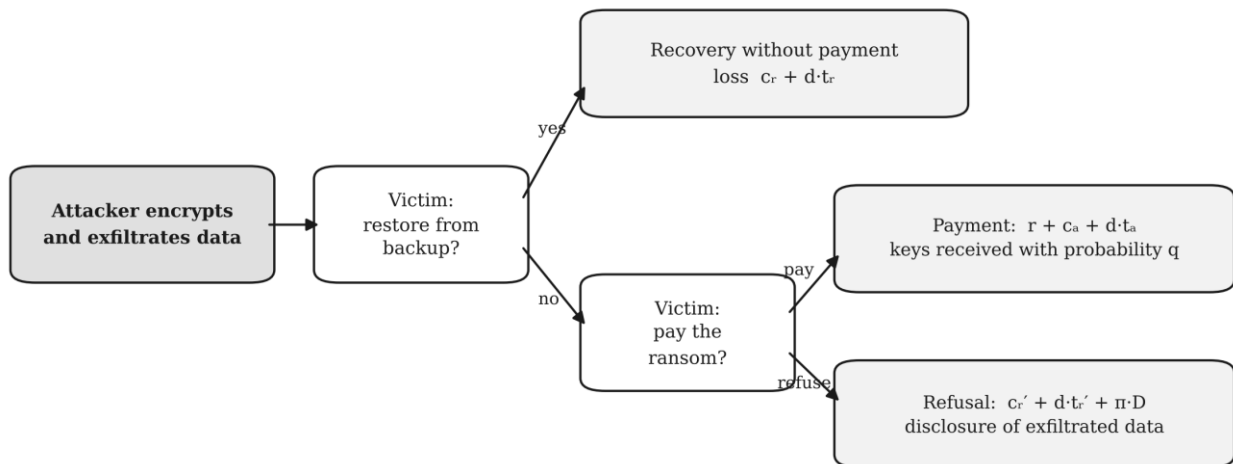
Date: 1<sup>st</sup> October-2026

destructive capability is modest and that the economic design — the pricing, the negotiation interface, the reputation for supplying keys — carries the business model [5]. Huang and co-authors measured the financial flows end to end and demonstrated that payments are observable in aggregate on public ledgers independently of victim reporting [6], a result that underlies the calibration performed here. Connolly and Wall analysed the organisational consequences of attacks against a set of victim organisations and documented the dominance of downtime and recovery costs over the ransom itself [7].

The game-theoretic strand is of particular relevance. Laszka, Farhang and Grossklags modelled the interaction between a population of potential victims investing in backups and an attacker choosing a ransom, and identified the free-rider structure of the problem: investment in restoration capability by one organisation reduces the attacker's expected revenue and therefore benefits others, so that the socially optimal level of investment exceeds the individually optimal level [8]. Cartwright, Hernandez-Castro and Cartwright examined the credibility of the offender's commitment to supply a key and showed that the offender's incentive to maintain a reputation for delivery is what makes the market viable at all [9]. The present article extends this literature in one specific direction: it incorporates exfiltration — double extortion — into the decision structure, which changes the result qualitatively, because the threat of disclosure is not neutralised by the possession of a backup.

The methodology is analytical and empirical in combination. A decision model of the victim is constructed and the rationality condition for payment is derived; the offender's revenue function is then stated over the induced demand and its maximum characterised. The model is calibrated against two independent empirical series for 2024–2025: officially reported incidents and losses, and payment flows measured directly on public blockchains. Deterrence instruments are finally evaluated by identifying the parameter of the model on which each one acts. No primary data were collected by the authors; all empirical material is drawn from published reports.

**The extortion transaction as a decision problem.** The interaction is modelled as the sequential decision problem shown in Figure 1. The attacker has encrypted the victim's data and, in the contemporary form of the offence, has also exfiltrated a copy of them before encryption. The victim then chooses between three branches.



$r$  — ransom demanded;  $c$  — recovery cost;  $d$  — cost of one day of downtime;

$t$  — recovery time;  $q$  — probability that usable keys are supplied;  $\pi$  — probability of disclosure;  $D$  — harm from disclosure

**Figure 1. Decision structure of the extortion transaction and the points at which deterrence instruments act**

Let the following quantities be defined for a given victim and incident:

- $r$  — the ransom demanded;
- $d$  — the cost to the victim of one day of interruption of operations;
- $t_r$  — the time required to restore operations from backups, and  $c_r$  the direct cost of that restoration;
- $t_a$  — the time required to restore operations using a decryption key supplied by the attacker, and  $c_a$  the associated direct cost;
- $q$  — the probability that a usable key is in fact supplied after payment;
- $\pi$  — the probability that exfiltrated data are published if the ransom is not paid, and  $D$  the harm resulting from publication, comprising regulatory penalties, contractual liability and loss of reputation;
- $t_r'$  and  $c_r'$  — the time and cost of reconstructing operations without backups and without a key.

The expected loss on each branch is then as follows. If a usable backup exists, the loss is

$$L_r = c_r + d \cdot t_r + \pi \cdot D,$$

where the last term is retained because the possession of a backup does not prevent the publication of data already exfiltrated. If the victim pays, the expected loss is

$$L_p = r + c_a + d \cdot [q \cdot t_a + (1 - q) \cdot t_r'] + (1 - \theta) \cdot \pi \cdot D,$$

where  $\theta$  denotes the probability that the attacker honours the undertaking to delete the exfiltrated copy — an undertaking for which no verification mechanism exists. If the victim refuses and has no backup, the loss is

$$L_n = c_r' + d \cdot t_r' + \pi \cdot D.$$

Payment is individually rational when  $L_p < \min(L_r, L_n)$ . Comparing the payment branch with the no-backup refusal branch and rearranging gives the condition

Date: 1<sup>st</sup> October-2026

$$r < d \cdot q \cdot (t_r' - t_a) + (c_r' - c_a) + \theta \cdot \pi \cdot D.$$

The inequality states the economics of the offence compactly. The victim's willingness to pay is governed by the daily cost of interruption multiplied by the time that payment is expected to save, by the difference in direct recovery costs and by the value of the disclosure threat weighted by the credibility of the attacker's deletion undertaking. Three implications follow immediately.

The first is that the willingness to pay is proportional to  $d$ , the daily cost of interruption, and not to the size of the organisation as such. This explains why hospitals, municipal utilities and manufacturers with continuous processes are disproportionately represented among victims who pay: for these organisations an interruption is not a loss of revenue but a loss of function, so that  $d$  is large and may be only loosely bounded. The second is that the term  $\theta \cdot \pi \cdot D$  is, by construction, unaffected by the quality of the victim's backups. The introduction of exfiltration therefore restored the attacker's leverage over precisely those victims whom restoration capability had rendered immune, which is why double extortion became the dominant form of the offence within a few years of its appearance. The third is that the entire structure depends on  $q$ , the probability that a usable key is delivered. If  $q$  were zero the market would collapse, since no rational victim would pay; the attacker's investment in a reputation for delivery is thus not an ethical residue but a necessary condition of the business model, and it is the reason why organised groups maintain support channels and, on occasion, provide technical assistance to the victims they have attacked.

**The offender's problem and the migration towards large victims.** The attacker chooses  $r$  so as to maximise expected revenue over a population of victims. Let  $F(r)$  denote the share of attacked victims for whom the condition above is satisfied at a demand of  $r$  — that is, the induced payment rate — and let  $n$  be the number of victims attacked. Expected revenue is

$$\Pi(r) = n \cdot F(r) \cdot r - n \cdot \kappa,$$

where  $\kappa$  is the cost per attacked victim, comprising access acquisition, tooling and negotiation effort. The first-order condition for an interior maximum is the familiar elasticity rule

$$F(r) + r \cdot F'(r) = 0, \quad \text{that is} \quad \varepsilon = -r \cdot F'(r) / F(r) = 1,$$

so that the attacker sets the demand at the point where the elasticity of the payment rate with respect to the ransom equals unity. Two comparative-static results follow and they jointly explain the paradoxical empirical record of 2024–2025.

Suppose first that the population of potential victims improves its restoration capability, reducing  $t_r'$  and  $c_r'$ . The condition for payment then holds for fewer victims at any given  $r$ , so  $F$  shifts downward and the payment rate falls. Suppose second that the attacker responds by selecting victims with a higher  $d$  — organisations whose operations cannot be interrupted — and by adding exfiltration, which raises the term  $\theta \cdot \pi \cdot D$ . Both changes raise the right-hand side of the rationality condition for the selected sub-population, which permits a higher  $r$  at the same elasticity. The observable consequence is



Date: 1<sup>st</sup> October-2026

exactly what the measured data show: a falling share of victims who pay, a sharply rising median payment and an approximately constant aggregate flow. The offence has not been suppressed; its incidence has been redistributed towards victims for whom interruption is intolerable.

The parameter  $\kappa$  is equally consequential and is the one most often neglected in policy discussion. The industrialisation of initial access — the sale of credentials harvested by information-stealing malware, the automated exploitation of exposed edge devices — has driven the cost of access to very low levels; the average price of access to a victim organisation on criminal markets is reported to have fallen from approximately 1,400 to 439 dollars [1]. A fall in  $\kappa$  does not change the optimal  $r$ , but it raises  $n$ , since attacks against victims with a low probability of payment become profitable in expectation. This accounts for the growth of approximately fifty per cent in claimed attacks during 2025 concurrently with a falling payment rate: the attacker is not extracting more from each victim population but is attacking a larger one at lower unit cost.

**Empirical calibration.** Table 1 assembles the available measurements for 2024 and 2025 from two independent sources: officially reported complaints and losses, and payment flows observed directly on public distributed ledgers.

Table 1. Measured parameters of the extortion market, 2024–2025

| Parameter                                                  | 2024          | 2025                 | Source and nature of the measurement                     |
|------------------------------------------------------------|---------------|----------------------|----------------------------------------------------------|
| Aggregate payments traced on public ledgers, million USD   | approx. 892   | approx. 820–900      | Blockchain analysis; independent of victim reporting [1] |
| Share of attacked victims who paid (payment rate $F$ )     | n/a           | 28 %<br>(record low) | Incident-response and negotiation data [1]               |
| Median payment, USD                                        | 12 738        | 59 565               | Blockchain analysis [1]                                  |
| Change in the number of claimed attacks                    | n/a           | + approx. 50 %       | Counts published on leak sites [1]                       |
| Average price of access to a victim organisation, USD      | approx. 1 400 | 439                  | Monitoring of criminal markets [1]                       |
| Complaints recorded by the IC3, units                      | n/a           | more than 3 600      | Voluntary reporting by victims [2]                       |
| Confirmed losses recorded by the IC3, million USD          | approx. 12.5  | 32.3<br>(+159 %)     | Voluntary reporting by victims [2]                       |
| New variants identified                                    | n/a           | 63                   | Analysis of samples [2]                                  |
| Average total cost of a breach, million USD (global / USA) | 4.45 / 10.2   | 4.99 / 11.5          | Survey of affected organisations [3]                     |
| Mean time to identify and contain, days                    | approx. 241   | 247                  | Survey of affected organisations [3]                     |

*Note. Figures designated n/a are not reported separately for the year in question by the cited source. The 2024 payment figure was subsequently revised upward by the source*



Date: 1<sup>st</sup> October-2026

as additional addresses were attributed, which illustrates that blockchain measurements are lower bounds that are refined over time.

Two features of the table are decisive for the argument. The first is the ratio between the two measurements of the same phenomenon: confirmed losses reported to the authorities amount to 32.3 million dollars, while payments measured on-chain for the same period lie between 820 and 900 million. The officially recorded figure captures of the order of four per cent of the ransom flow alone, and a far smaller share of total harm. Any policy calibrated on reported losses therefore operates on a signal that understates the phenomenon by more than an order of magnitude, and the apparently modest position of ransomware in national crime statistics is an artefact of reporting rather than a fact about harm.

The second is the relation between the median payment and the average total cost of a breach. The median payment of 59.6 thousand dollars is approximately one per cent of the average total cost of an incident. The ransom is thus a marginal component of the loss, and the policy debate about whether victims should be permitted to pay, although important for the suppression of the criminal revenue stream, addresses a variable that is close to irrelevant for the victim's own balance sheet. What determines the victim's loss is the product  $d \cdot t$  — the daily cost of interruption multiplied by its duration — and a mean containment time of 247 days indicates that this product is large in most incidents and that it has not improved.

**Evaluation of deterrence instruments.** Each deterrence instrument acts on a specific parameter of the model, and its effectiveness can therefore be assessed analytically rather than by assertion. Table 2 presents this assessment.

Table 2. Deterrence instruments and the parameters of the model on which they act

| Instrument                                                                   | Parameter affected                                       | Effect on the offender's revenue $\Pi$                   | Principal limitation                                                      |
|------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|---------------------------------------------------------------------------|
| Offline, tested backups and rapid restoration                                | reduces $t_r'$ , $c_r'$ ; raises $L_r$ relative to $L_p$ | Direct: shifts $F(r)$ downward, reduces the payment rate | Does not act on $\pi \cdot D$ ; ineffective against the disclosure threat |
| Prevention of exfiltration (segmentation, egress control, data minimisation) | reduces $\pi \cdot D$                                    | Direct: removes the leverage that survives restoration   | Technically demanding; ineffective once data have been removed            |
| Sanctions and controls on payment channels, regulation of exchanges          | reduces the attacker's realisable share of $r$           | Direct: lowers net revenue per transaction               | Displacement towards unregulated channels and jurisdictions               |
| Takedown of infrastructure and arrests                                       | raises $\kappa$ and $p_a$                                | Indirect: raises unit cost, fragments the ecosystem      | Effect is temporary; groups reconstitute under new names                  |

Date: 1<sup>st</sup> October-2026

| Instrument                   | Parameter affected                        | Effect on the offender's revenue $\Pi$ | Principal limitation                                                       |
|------------------------------|-------------------------------------------|----------------------------------------|----------------------------------------------------------------------------|
| Mandatory incident reporting | raises $\rho$ , the reporting coefficient | None directly                          | Improves measurement and response but does not alter the offender's payoff |
| Prohibition of payment       | sets $r$ to zero in the admissible set    | Direct and maximal in principle        | Shifts the entire loss onto the victim; risks concealed payment            |

The classification exposes a distinction that is routinely blurred in practice. Instruments that act on  $F(r)$  or on the realisable revenue alter the attacker's objective function and therefore reduce the incentive to commit the offence at all. Instruments that act on  $\kappa$  or on  $p_a$  raise the cost of offending without altering its profitability at the margin, and their effect is accordingly temporary: the coordinated operations conducted by European and American agencies in 2024 and 2025 — in which more than a hundred servers and two thousand domains were seized in the first phase and more than a thousand servers and twenty domains in a later phase, together with the arrest of the operator of a widely used remote access tool [10] — fragmented the ecosystem into smaller groups and measurably reduced the reliability of the tooling, but did not reduce the aggregate payment flow. Mandatory reporting, finally, acts on no parameter of the offender's problem at all; its value is informational, and it should be defended on that ground rather than presented as a deterrent.

The prohibition of payment deserves separate treatment because it is the instrument most often proposed and the one whose analysis is least often carried through. Within the model its effect is unambiguous: if  $r$  cannot be paid, the attacker's revenue from the encryption branch is zero and the offence against the prohibiting jurisdiction becomes unprofitable, subject to the attacker's belief about compliance. The difficulty is distributional rather than analytical. The prohibition transfers the full loss  $c_r' + d \cdot t_r' + \pi \cdot D$  onto a victim who may be a hospital or a municipal water utility, and it does so in the individual case in order to obtain a benefit that accrues collectively and in the future. This is the structure of a public-good problem, and it implies that a prohibition is defensible only when accompanied by a capability for state-supported restoration; otherwise it converts an economic crime into a direct threat to the continuity of essential services. A graduated form — prohibition for public bodies and operators of critical infrastructure, combined with obligatory reporting and licensing of intermediaries for all other victims — preserves most of the deterrent effect while limiting the transfer of loss to entities that the state is in any event obliged to restore.

**The legal framework and its application in the Republic of Uzbekistan.** Conduct of this kind is qualified under the law of the Republic of Uzbekistan through the combination of two groups of provisions. The encryption of data and the resulting disruption of information systems fall within Chapter XX<sup>1</sup> of the Criminal Code, which



Date: 1<sup>st</sup> October-2026



establishes liability for offences in the sphere of information technologies: unlawful access to computer information, modification of computer information, computer sabotage and the creation and dissemination of malicious software are addressed in Articles 278<sup>2</sup> and 278<sup>4</sup>–278<sup>6</sup> [11]. The demand for property accompanied by a threat is extortion within the meaning of Article 165, and where the attacker threatens to publish exfiltrated information the demand is accompanied by a threat to disclose information the victim wishes to keep confidential, which is an aggravated form of the same offence. The receipt and conversion of the ransom falls under Article 243 on the legalisation of proceeds obtained from criminal activity. The unlawful exfiltration of personal data engages separately the obligations of the operator under the Law 'On Personal Data' [12], so that a single incident generates both criminal liability for the offender and administrative exposure for the victim organisation — a configuration that reduces  $\rho$ , the propensity to report, and thereby degrades the state's own visibility of the phenomenon.

The preventive and organisational framework is established by the Law 'On Cybersecurity' of 15 April 2022, No. ZRU-764, which defines the subjects of cybersecurity and the requirements applicable to critical information infrastructure [13], and by the Law 'On Informatisation' [14]. Within the terms of the model, the requirements addressed to operators of critical infrastructure act on  $t_r'$  and  $c_r'$  — that is, on the restoration branch — and are therefore among the few instruments that shift  $F(r)$  downward. The task of creating a system for countering cybercrime set by the Strategy of Development of New Uzbekistan for 2022–2026 [15] may accordingly be given an operational reading: it requires, as a minimum, a verified restoration capability for operators of essential services, a channel for the rapid freezing of suspicious transfers and a reporting regime that does not penalise the victim for reporting.

International cooperation is indispensable because the offender, the infrastructure and the proceeds are almost invariably located outside the jurisdiction of the victim. The Council of Europe Convention on Cybercrime remains the principal operative instrument for expedited preservation of data and mutual assistance [16]; the United Nations Convention against Cybercrime, opened for signature at Hanoi on 25 October 2025, extends a comparable framework to a global membership and is of particular significance for states that are not parties to the earlier instrument [17]. In the terms of the present model, cooperation acts on  $p_a$  and on  $\kappa$ , and its effects are therefore of the indirect and temporary class identified in Table 2 — which is an argument for pursuing it in combination with, and not instead of, measures that act on  $F(r)$ .

**Discussion.** The analysis yields three propositions of practical consequence.

The first is that the persistence of ransomware is a predictable consequence of individually rational behaviour and not of negligence on the part of victims. The condition derived above is satisfied over a wide region of the parameter space, particularly for organisations whose daily cost of interruption is high and whose exposure to disclosure is material. Policies that proceed from the assumption that victims pay because they are unprepared will therefore fail, because they misidentify the mechanism. What changes

Date: 1<sup>st</sup> October-2026

behaviour is a change in the parameters: a restoration capability that reduces  $t_r'$ , and the prevention of exfiltration, which is the only measure that acts on the term that backups cannot touch.

The second is that aggregate indicators of the health of the criminal market must be interpreted jointly. A falling payment rate taken alone suggests that deterrence is succeeding; a rising median payment taken alone suggests the opposite; the two together, with an approximately constant aggregate flow, indicate a market that is reallocating towards victims with inelastic demand. The correct inference is that defensive improvement has been real but has been unevenly distributed, and that the organisations which have not improved are precisely those for which interruption is least tolerable — hospitals, utilities, local administrations and manufacturers. This is an argument for directing public support to exactly those categories rather than for general exhortation.

The third is that the ransom is the wrong variable to optimise. A median payment equal to about one per cent of the average total cost of an incident indicates that the decisive quantity is the duration of the interruption, not the price of the key. Investment in the capacity to resume operations quickly dominates investment in the capacity to avoid paying, because the former reduces  $d \cdot t$  on every branch of the decision tree whereas the latter affects only one. A mean containment time of 247 days, which has not improved over several years, indicates that this is where the greatest unrealised gain lies.

Several limitations should be stated. The model treats the victim as a single rational agent minimising expected loss, whereas the decision is in practice taken under severe time pressure by several actors with divergent interests — management, legal counsel, insurer, regulator — and insurance coverage in particular alters the effective value of  $r$  for the decision-maker in a manner the model does not capture. The parameters  $\pi$ ,  $\theta$  and  $q$  are not directly observable and were not estimated numerically; their values are inferred qualitatively from reported behaviour. The calibration relies on two sources whose coverage differs, and the aggregate on-chain figures are lower bounds that are revised upward as addresses are attributed. Finally, the analysis is conducted at the level of the market and does not model the internal structure of ransomware-as-a-service arrangements, in which the division of revenue between developer and affiliate alters the incentives of each.

These limitations define the direction of further work. The authors intend to estimate the distribution of the daily cost of interruption  $d$  for categories of organisation in the national economy, to model the effect of insurance on the payment decision, and to evaluate the feasibility of a state-supported restoration capability for operators of essential services as an alternative to a prohibition on payment.

**Conclusion.** This article has analysed extortion by malicious encryption as an economic crime and has formalised the extortion transaction as a sequential decision problem over three branches. The condition under which payment is individually rational was derived and shown to depend on the daily cost of interruption, on the time saved by obtaining a key, on the credibility of key delivery and on the value of the disclosure threat



**Date: 1<sup>st</sup> October-2026**

weighted by the credibility of the attacker's deletion undertaking. The last of these terms is unaffected by the victim's backups, which explains the transition of the offence to its double-extortion form.

The offender's problem was stated as the maximisation of expected revenue over the induced payment rate, and the apparently contradictory empirical record of 2024–2025 — a payment rate falling to a record low of 28 per cent, a median payment rising from 12.7 to 59.6 thousand dollars, an approximately constant aggregate flow and a growth of some fifty per cent in the number of attacks — was derived as the comparative-static response of that problem to improved restoration capability in the victim population and to a fall in the cost of initial access.

Four classes of deterrence instrument were evaluated against the parameters of the model. Only restoration capability, the prevention of exfiltration and the disruption of payment channels act directly on the offender's revenue function; the takedown of infrastructure raises unit cost temporarily, and mandatory reporting has informational rather than deterrent value. The comparison of reported losses with independently measured payment flows showed that official statistics capture of the order of four per cent of the ransom flow, so that policy calibrated on reported loss is calibrated on a systematically understated signal. The compliance of the proposed measures with the legislation of the Republic of Uzbekistan was substantiated, and it was shown that a prohibition of payment is defensible only in combination with a state-supported restoration capability for operators of essential services.

#### **REFERENCES:**

1. Crypto Crime Report 2026. – New York: Chainalysis Inc., 2026.
2. Internet Crime Report 2025. – Washington: Internet Crime Complaint Center, Federal Bureau of Investigation, 2026.
3. Cost of a Data Breach Report 2026. – Armonk: IBM Security, 2026.
4. Becker G.S. Crime and Punishment: An Economic Approach // Journal of Political Economy. – 1968. – Vol. 76, No. 2. – P. 169–217.
5. Kharraz A., Robertson W., Balzarotti D., Bilge L., Kirda E. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks // Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2015). – Cham: Springer, 2015. – P. 3–24.
6. Huang D.Y., Aliapoulos M.M., Li V.G., Invernizzi L., Bursztein E., McRoberts K., Levin J., Levchenko K., Snoeren A.C., McCoy D. Tracking Ransomware End-to-end // 2018 IEEE Symposium on Security and Privacy (SP). – San Francisco: IEEE, 2018. – P. 618–631.
7. Connolly L.Y., Wall D.S. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures // Computers & Security. – 2019. – Vol. 87. – 101568.
8. Laszka A., Farhang S., Grossklags J. On the Economics of Ransomware // Decision and Game Theory for Security (GameSec 2017). – Cham: Springer, 2017. – P. 397–417.



**Date: 1<sup>st</sup> October-2026**

9. Cartwright A., Cartwright E., Hernandez-Castro J. To Pay or Not: Game Theoretic Models of Ransomware // Journal of Cybersecurity. – 2019. – Vol. 5, No. 1. – tyz009.
10. Operation Endgame: results of the coordinated international actions of 2024 and 2025. – The Hague: Europol, 2025.
11. Criminal Code of the Republic of Uzbekistan of 22 September 1994, No. 2012-XII (as amended), Articles 165, 243 and Chapter XX<sup>1</sup>, Articles 278<sup>1</sup>–278<sup>6</sup>. – URL: <https://lex.uz/docs/111457>
12. On Personal Data: Law of the Republic of Uzbekistan of 2 July 2019, No. ZRU-547 (as amended). – URL: <https://lex.uz/ru/docs/4396428>
13. On Cybersecurity: Law of the Republic of Uzbekistan of 15 April 2022, No. ZRU-764. – National Database of Legislation of the Republic of Uzbekistan, No. 03/22/764/0330.
14. On Informatisation: Law of the Republic of Uzbekistan of 11 December 2003, No. 560-II (as amended). – URL: <https://lex.uz/ru/docs/82956>
15. On the Strategy of Development of New Uzbekistan for 2022–2026: Decree of the President of the Republic of Uzbekistan of 28 January 2022, No. UP-60. – URL: <https://lex.uz/docs/5841063>
16. Convention on Cybercrime, ETS No. 185. – Budapest: Council of Europe, 23 November 2001.
17. United Nations Convention against Cybercrime: adopted by General Assembly resolution 79/243 of 24 December 2024, opened for signature at Hanoi on 25 October 2025. – New York: United Nations, 2025.
18. #StopRansomware Guide. – Washington: Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, 2023. – 46 p.
19. ENISA Threat Landscape 2025. – Athens: European Union Agency for Cybersecurity, 2025.
20. Anderson R., Barton C., Bohme R., Clayton R., Ganan C., Grasso T., Levi M., Moore T., Vasek M. Measuring the Changing Cost of Cybercrime // Proceedings of the 18th Annual Workshop on the Economics of Information Security (WEIS). – Boston, 2019. – 32 p.
21. Meland P.H., Bayoumy Y.F.F., Sindre G. The Ransomware-as-a-Service economy within the darknet // Computers & Security. – 2020. – Vol. 92. – 101762.
22. Oosthoek K., Cable J., Smaragdakis G. A Tale of Two Markets: Investigating the Ransomware Payments Economy // Communications of the ACM. – 2023. – Vol. 66, No. 8. – P. 74–83.
23. Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0. – Gaithersburg: National Institute of Standards and Technology, 2024.
24. Contingency Planning Guide for Federal Information Systems: NIST Special Publication 800-34, Rev. 1. – Gaithersburg: National Institute of Standards and Technology, 2010. – 148 p.

