Data & Policy (2025), 7: e80
doi:10.1017/dap.2025.10040

RESEARCH ARTICLE

From ransoms to ruin: Are extortion payments by ransomware victims insurable?

Divya Ramjee[1] and Eireann Leverett[2]

[1]Department of Public Policy, Department of Criminal Justice, Rochester Institute of Technology, Rochester, NY, USA
[2]Research and Development, Concinnity Risks, Cambridge, UK
Corresponding author: Divya Ramjee; Email: dqrgcj@rit.edu

Received: 08 April 2024; **Revised:** 14 August 2025; **Accepted:** 10 September 2025

Keywords: cryptocurrency; cyber insurance; cyber risk; ransomware; risk modelling

Abstract

Cyber risk is an important consideration in today's risk management and insurance industries. However, the statistical features of cyber risk, including concerns of solvency for cyber insurance providers, are still emerging. This study investigates the dynamics of ransomware severity, specifically focusing on different statistical dimensions of extortion payments from ransomware attacks across various ransomware strains and/or variants. Our results indicate that extortion payments are not identically distributed across ransomware strains/variants, and thus violate necessary assumptions for solvency determinations using classical ruin theory. These findings emphasize the importance of re-examining these assumptions under empirical data and implementing dynamic cyber risk modelling for portfolio losses from extortion payments from ransomware attacks. Additionally, such findings suggest that removing coverage for extortion payments from insurance policies may protect cyber insurance firms from insolvency, as well as create a potential deterrence effect against ransomware threat actors due to lack of extortion payment from victims. Our work has implications for insurance regulators, policymakers, and national security advisors focused on the financial impact of extortion payments from ransomware attacks.

Policy Significance Statement

The current study supports the claim that extortion payments by ransomware victims should not be considered insurable by cyber insurance providers that use assumptions of classical ruin theory in their solvency determinations. Cyber insurers and re-insurers should examine and consider reforming the practice and policy of covering extortion demands as part of insurance claims related to ransomware attacks. This study also encourages an evidence-based approach for creating and applying cyber risk solvency standards by insurance regulators to ransomware-related extortion payments.

1. Introduction

The already $16 billion yearly demand for insurance coverage for cybersecurity incidents is only expected to increase in the coming years, with more frequent incidents and evolving regulatory requirements worldwide (FBI, 2024; Fortune Business Insights, 2025). The incidents driving losses are varied, including, but not limited to, distributed denial of service (DDoS) attacks, business email compromises (BECs), network loss,

data breaches, financial fraud, and ransomware attacks. In particular, ransomware—i.e. malicious software or "malware" used for extortion—actors continue to target critical sectors, including healthcare and public health, government facilities, and information technology organizations (FBI, 2024; Verizon, 2024). In 2023, 32% of data breaches involved some type of extortion technique, including ransomware, and over the last five years (2019–2024), reported ransomware attacks have continued to increase and accounted for around 20–30% of insurance claims (FBI, 2024; SouthPoint Risk, n.d.; Verizon, 2024).

General insurance has two primary tasks: pricing and solvency. While insurance premiums are designed to reflect portfolio-wide risk, insurance providers may still face challenges if capital reserves and reinsurance strategies are insufficient to absorb tightly aggregated events over time. This study is concerned with solvency and issues that arise for cyber insurance providers and modelling catastrophic events, particularly for ransomware attacks and extortion payments. In insurance, solvency is assessed using numerous risk factors and determinations for regulatory capital and economic capital and is a balancing act between initial capital reserves, premiums collected, and first-party and third-party liability claims paid (Eling and Schnell, 2019). For cyber insurance providers, this means solvency is assessed based on risks, including cyber risk, first-party liability for insured (data recovery and restoration, customer notification, public relations assistance, business interruption reimbursements, extortion payments, etc.), and third-party liability for lawsuits from the insured's client(s) (Eling and Schnell, 2019; Romanosky et al., 2019; Woods et al., 2023). Thus, economic capital from collected premiums and regulatory capital based on mandated requirements, along with initial surplus, must not be vulnerable to insolvency or ruin after payment of claims.

It should be noted, premium pricing adequacy is not a sufficient proxy for avoidance of ruin if it ignores temporal parameters such as inter-arrival rates (Hult and Lindskog, 2011). In classic ruin theory, mathematical models for insolvency evaluate the risk of ruin based on the theory that premiums are collected at a constant rate while claim payments occur with values that are also stochastic and are independent and identically distributed (i.i.d.) (Hult and Lindskog, 2011; Lundberg, 1903). If an insurance provider must pay a claim prior to collecting sufficient premiums or finding additional customers, reserves may have to be exhausted immediately. With the diverse frequency of ransomware attacks and heavy-tailed distribution of extortion payments, complete depletion of reserves is potentially a realistic outcome, especially without sub-limits for extortion payments.

Given the increasing pattern for cybersecurity incidents to result in severe, widespread, and even systemic consequences, it is essential to better understand cyber risk to mitigate technical and operational risks and appropriately prepare for financial risks (Eling and Loperfido, 2017; Eling et al., 2021; World Economic Forum, 2022). This is important not only for stakeholders involved in designing safeguards and shaping standards policies but also for those assessing organizational cyber risk, such as cyber insurance providers (Eling et al., 2021). More informed risk assessments can enable a more accurate estimation of risk exposure and further inform evaluations of aggregate risk across insurance portfolios, particularly where interdependencies may lead to simultaneous failures across multiple systems or organizations (Axon et al., 2023).

To accurately understand the cost of ransomware attacks for society, we must be able to identify and measure many of the dynamic issues for extortion payments—a challenge compounded by data limitations. Unlike traditional property and casualty insurance, cyber risk underwriting must contend with a rapidly evolving set of threats, making risk assessment inherently more complex and uncertain. We make three contributions to the existing literature. First, the present study provides additional statistical analyses of aspects of cyber risk, specifically the distributions of extortion payments clustered by ransomware strain/variant, using novel data on ransomware attacks and payments. Second, our findings indicate that extortion payments are not an i.i.d. process and thus violate an underlying principle of solvency in classical ruin theory, suggesting that extortion payments are not insurable by firms using such solvency models. Third, our work positions fluctuating dynamics in extortion demands from ransomware attacks as a consideration in predator-prey frameworks for cybersecurity. Lastly, our work highlights an urgent need for reconsideration of solvency standards by insurance regulators for firms that provide coverage for ransomware extortion payments.

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

2. Literature review

2.1. Heavy-tailed distributions and cyber insurance

Heavy-tailed distributions, i.e. distributions with tails that take longer to approach zero than exponential distributions, appear frequently in statistical analyses regarding cybersecurity threats (e.g., Bryson, 1974; Edwards et al., 2016; Eling and Wirfs, 2016; Florêncio and Herley, 2011; Hult and Lindskog, 2011; Maillart and Sornette, 2010; Romanosky, 2016; Shevchenko et al., 2023). Such distributions can appear when investigating different types of cybersecurity threats, e.g. estimating infected devices amongst certain Internet of Things (IoT) manufacturers, as well as in studies related to actuarial assessments, insurance, and models of risk for cybersecurity threats (Biener et al., 2015; Dacorogna et al., 2023; Jung, 2021; Rodríguez et al., 2021). While there is some research that attempts to fit a single distribution to a loss model for cybersecurity threats, there is less peer-reviewed work that comprehensively examines the foundational underpinnings of why cybersecurity threats are heavy-tailed (August et al., 2022; Kolesnikov et al., 2022; Laszka et al., 2017; Santini et al., 2019). Some studies have sought to determine if different driving processes are independent and can be accounted for in modelling, though these have primarily used existing datasets related to data breaches and not ransomware incidents (e.g., Eling and Wirfs, 2016; Xu et al., 2018; Zeller and Scherer, 2022). Looking at ransomware attacks in particular, prior literature includes modelling of losses for ransomware attacks with traditional assessments of aggregate cyber risk across various cybersecurity threats and has not sufficiently explored evaluating risk based on the specific type of cybersecurity threat and any unique underlying driving processes (Axon et al., 2023; Caporusso et al., 2019).

Heavy-tailed distributions also appear in losses associated with financially motivated cybersecurity threats over time. Over the last two years, BECs and extortion breaches (including ransomware attacks) accounted for approximately one-fourth and one-third of financially motivated attacks, respectively. Additionally, BECs had a median transaction amount of $50,000 USD in both years, while according to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) ransomware incident complaint data, "the median loss associated with ransomware and other extortion breaches has been $46,000 [USD], ranging between $3 [USD] and $1,141,467 [USD] for 95% of cases" (FBI, 2024; Verizon, 2024). Extortion amounts vary by ransomware strain or variant[1] due to differences in the attack behaviours and choices of targets (perhaps specific to a sector). Extortion payments also vary over time, with these temporal factors having ramifications for risk management.

Previously, Leverett et al. (2020) used power laws to study the characterization of ransomware-related extortion payments by their averages. In particular, the authors highlighted that data from recent years suggests that the exponent of the power laws might be testing the boundaries of the insurability of paying ransoms with insurance policies. Their findings indicated this was the result of no stable, defined first moment under recent exponents. Additionally, Leverett et al. concluded that power laws perform a good distribution fit to ransom payments due to the diversity induced by multiple sub-population distributions. This is consistent with other research on mixture models and power law tails (Patriarca et al., n.d.). Furthermore, the work of Cartwright and Cartwright predicts that a mixed distribution would be an emergent property of a diversity of differential pricing by different groups (Hernandez-Castro et al., 2020).

General liability insurance to cover losses involves some type of risk assessment and related pricing. While some providers assess an overall risk, others use more advanced methods (e.g. spatial analysis, AI-driven modelling, etc.) to determine insurance tiers and premiums based on different subsets of risks. For cyber insurance providers, such granularity does not currently exist, and many providers focus coverage on cybersecurity threats as a monolith (i.e. treating DDoS, fraud, ransomware, etc. as one)

[1] We recognize that different threat actors are involved in ransomware attacks, including actors who use certain ransomware strains or variants as part of a paid service with the founding group for the specific ransomware family, i.e. Ransomware-as-a-Service (RaaS) (Baker, 2023). Additionally, we also recognize that certain threat actors use multiple ransomware strains and variants for different ransomware attacks. For simplicity, we associate our analyses and findings with ransomware strains and variants used in the attacks and not any specific threat actor.

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

despite the reality that the insureds incur different losses driven by different processes. For example, a qualitative analysis of cyber insurance policies from 5 years ago reports that the average premium for most insured parties is between $10,000 and $25,000 (USD), with some providers setting limits up to $10–$50 million (USD) and others offering extreme loss coverage for certain industries with limits in the hundreds of millions of dollars (Romanosky et al., 2019). At present, there is still limited publicly available information regarding how cyber risk is determined, how cyber risk changes based on industry and sector, and how premiums are ultimately determined (CISA, 2021; Romanosky et al., 2019; Woods et al., 2017).

Fundamentally, cybersecurity threats are merely technologically elevated forms of adversarial actions already in existence, such as theft, fraud, sabotage, and extortion/ransom. It follows then that cyber risk is no different than other types of uncertain adversarial risks that can be assessed as a straightforward function of threat, vulnerability, and impact (Geer et al., 2020). However, because of the ubiquity of technological systems and potential for wide-ranging and compounding consequences, cybersecurity threats can not only be thought of as their own new risk class but can also require providers to reassess many other risk classes (Wolff, 2022). A 2023 study found that providers were nearly split as to whether cyber risk is treated as its own unique class versus incorporated into other existing risk classes (Romanosky and Petrun Sayers, 2023).

Nearly 25 years ago, Dr. Ross Anderson aptly detailed the risk issues of cyber insurance that still ring true today: "Around 2000, the end of the dotcom boom created a downswing that coincided with the Millennium bug scare. Even now that markets are returning to normal, some kinds of cover are still limited because of correlated risks. Insurers are happy to cover events of known probability and local effect, but where the risks are unknown and the effect could be global (for example, a worm that took down the Internet for several days), markets tend to fail (Anderson, 2001)." Additionally, previous research has demonstrated how two tiers of cyber risk consideration creates potential barriers to a healthy cyber insurance market: "the first tier is the correlation of cyber-risks within a firm (i.e. correlated failure of multiple systems on its internal network) and the second tier is the correlation in risk at a global level (i.e. correlation across independent firms in an insurer's portfolio)" (Anderson, 2001; Böhme and Kataria, 2006). The second tier—of interest in our study—is often known as 'accumulation' or 'aggregation' of risk in a portfolio.

Alongside a split consensus as to how cyber risk is handled, cyber insurance providers are considerably varied on exclusions to coverage. While many providers offer policies that cover aspects of first-party liability with little to no variance in costs across customers, there is a pronounced division as to whether extortion payments are covered under the same policies (Woods et al., 2017; Romanosky et al., 2019). Cyber insurance firms that choose to exclude extortion payments from coverage can simplify considerations for solvency and premium pricing, though their offerings may not be as enticing to customers who are hoping for protection on extortion payments. However, insurance providers who do offer coverage of these payments face a challenging predicament of how to model high variability in losses incurred, including inconsistent extortion amounts demanded by different groups for different victim companies within different industries and sectors, varied clustering in time, and frequency of payments.

Pricing models in insurance are designed to have an underwriting loss ratio (ULR), and in the cyber insurance industry, it is not uncommon for that ratio to be 40–45 percent. For example, "although insurers experienced a range of outcomes in 2023…overall performance held strong in the face of market softening and rebounding frequency; the 2023 loss ratio of 42 percent [wa]s the lowest since calendar year 2018" (AON, 2023). This translates to premium pricing that leads to 42 cents of loss for every dollar generated in a given year. However, the ULR for some years can be worse than others, wherein losses may even exhaust the premium reserves. In these cases, the volatility of cyber risk has a cost outwith the pricing model, and the role of capital reserves and solvency determinations helps cover this (Mildenhall and Major, 2022). Solvency can be achieved with four components: 1) the evaluation of liabilities; 2) the evaluation of assets; 3) the level of the premiums of long-term policies; and 4) reinsurance (Pentikäinen, 1967). We also see similar statements when we examine only insurance pricing literature: "Premium covers only the cost of risk transfer…In practice capital costs are split between on-balance sheet costs, estimated via cost-of-capital, and the cost of reinsurance" (Mildenhall and Major, 2022).

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

This then leads to the fundamental question of the present study: should extortion payments be included in cyber insurance policies? Model risk—risk of potential loss an institution may incur due to decisions based on inadequacies in internal models (e.g. financial risk measurement and valuation models)—is an acknowledged and long-standing issue in the field of financial risk modelling (e.g., Sibbertsen et al., 2008; Klüppelberg et al., 2014; Blanchet and Murthy, 2019). As simplified representations of complex phenomena, models are inherently prone to inaccuracies. Understanding the contexts and mechanisms of model failure is crucial for effective decision-making and policy design. For cyber insurance providers, determining if extortion payments are or are not i.i.d., the latter violating the classical model of ruin theory, would reduce model risk in certain solvency determination circumstances. Thus, our null hypothesis for this study is that extortion payments made to threat actors are independent and identically distributed within and across ransomware strains and variants.

2.2. Dynamics of ransomware attacks and ransom demands

As discussed, traditional model risk calculations and solvency determinations assume a certain degree of environmental stability and predictability—conditions that do not hold for cybersecurity threats. The adversarial nature of such threats creates a feedback loop of escalation that undermines static risk models. As a result, cyber insurers face significant challenges in accurately assessing pricing coverage and capital reserve requirements in a market where risk conditions can shift rapidly and unpredictably. The predator–prey paradigm offers a compelling framework for conceptualizing the dynamic interplay between threat actors and defensive systems and has been investigated in prior research (e.g., Ford et al., 2006; Furnell, 2008; Kumar et al., 2016; Ud Din et al., 2017; Ding et al., 2019; Axon et al., 2023; Gorman et al., 2004).

Analogous to biological ecosystems, where evolutionary pressures drive reciprocal adaptations between predators and their prey, the cybersecurity domain is characterized by continuous cycles of offensive innovation and defensive response (Nye, 2010; Whyte, 2015; Axon et al., 2023). Threat actors, equipped with increasingly sophisticated tools and techniques, exploit vulnerabilities across digital infrastructures, prompting defensive countermeasures. These countermeasures, while temporarily reducing the efficacy of attacks, often induce adversaries to modify tactics, thereby perpetuating an evolutionary arms race. The resulting co-adaptive cycle mirrors ecological population fluctuations, where increases in attack prevalence are typically met with heightened defensive posture, and lulls in threat activity may inadvertently foster vulnerability through strategic or resource-driven complacency (Nye, 2010; Axon et al., 2023).

The Lotka–Volterra model (Lotka, 1925; Volterra, 1926), a foundational construct in mathematical biology for describing predator–prey population dynamics, can be repurposed to simulate the interaction between cyber attackers and defenders within digital ecosystems. In this adapted framework, attackers are analogized to predators whose success is contingent upon the availability and vulnerability of targets (prey), while defenders represent the adaptive capacity of systems to mitigate and withstand these threats (Gorman, 2004; Axon et al., 2023). The coupled differential equations describe how the "prey" population—symbolizing the robustness or density of defended assets—grows in the absence of attack, while the "predator" population—denoting the intensity or frequency of cyber threats—increases through successful exploitation (Gorman et al., 2004):

$$dH/dt = H(a - aP) \tag{2.1}$$

$$dP/dt = P(-b + bH), \tag{2.2}$$

where $H(t)$ and $P(t)$ represent the magnitude of prey and predator populations, respectively, a is the growth rate of the prey population in the absence of predators, and b is the rate at which a predator population will decrease without a sufficient amount of prey to feed upon. When transposed to cybersecurity threats, this model facilitates the quantitative examination of adversarial dynamics, enabling researchers to predict emergent threat behaviours, evaluate the temporal efficacy of defence strategies, and optimize proactive interventions in complex and evolving threat environments.

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

Ransomware attacks provide a particularly salient manifestation of predator–prey dynamics, wherein threat actors operate as strategic predators targeting digital ecosystems that often lag in defensive evolution. The cyclical nature of these attacks mirrors ecological interactions: as vulnerabilities proliferate through expanded digital infrastructure, inconsistent patching, stolen credentials, and human error, attackers adapt with increasing sophistication. This predator–prey relationship also has significant implications for the economics of ransomware. As defenders have improved response capabilities (i.e. stronger backup protocols, endpoint protections, and regulatory oversight) and refuse to pay extortion demands, ransomware threat actors have been forced to adapt. This can be seen in threat actors shifting to double and triple extortion techniques, including threats to leak stolen data or contact victims' customers directly.

The predator–prey framework also invites a deeper examination of the empirical patterns these interactions produce. As discussed, unlike in other insurance areas where past loss experience provides a relatively stable foundation for forecasting future claims, cyber risk is shaped by a volatile and fast-changing threat environment that complicates predicting changes in cyber risk (Marotta et al., 2017). The challenges posed by this dynamic nature for underwriting are additionally compounded by data availability issues. Existing literature has highlighted the diminishing value of historical data as cyber threats evolve more rapidly than underwriting models can (Eling and Wirfs, 2016). Thus, the relevance of historical data for quantifying cyber risk and informing premium-setting is inherently short-lived (Shetty et al., 2018). This temporal limitation challenges insurers' ability to differentiate between levels of cyber maturity across customers and may contribute to pricing strategies based more on market competition than on evidence-based risk segmentation—making reliance on premium pricing for solvency considerations even more hazardous.

2.3. Solvency and modelling considerations

The probability of ruin refers to the likelihood that an insurer's liabilities will exceed its assets in present value terms at a specified future date, resulting in insolvency. It serves as a key metric for evaluating an insurance company's risk of insolvency and overall risk exposure. Solvency determinations in classical ruin theory rely on a key assumption of independent and identically distributed (i.i.d.) claims based on a compound Poisson process characterized by a Poisson distribution (Lundberg, 1903). The i.d.d. assumption has been well-documented in existing literature (e.g., Gerber, 1988; Dickson, 2005; Hult and Lindskog, 2011), with more recent work also examining the assumption regarding heavy-tail distributions (Beck et al., n.d.). For a Poisson distribution, the assumption of i.i.d. is satisfied when random events in different time segments are independent and identically distributed. Additionally, a Poisson distribution also assumes that events in the sample are non-simultaneous, i.e. two or more events do not occur at the same time, and that the probability of an event occurring is not conditional on the number of previous events that have occurred within a small time period (Gill and Bao, 2024).

In classical ruin theory, the Cramér-Lundberg model is the foundational mathematical model for testing solvency against a stochastic claims process (Lundberg, 1903). Specifically, claims γ with i.i.d. inter-arrival times at time t according to a Poisson process $N(t)$ with claim frequency γ can be defined as

$$\Upsilon(t) = \sum_{i=1}^{N(t)} X_i, \tag{2.3}$$

where i.i.d. claim amounts X_i occur based on a compound Poisson process with distribution Γ and positive mean μ with finite variance. For an insurance provider that starts with initial capital reserves $\phi \geq 0$ and collects premiums at a constant rate $c > 0$, total assets Φ at time t for $t \geq 0$ can be defined as

$$\Phi(t) = \phi + ct - \sum_{i=1}^{N(t)} X_i. \tag{2.4}$$

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

With this model, the primary objective is to evaluate the probability of ultimate ruin Ψ, i.e. bankruptcy, denoted as

$$\Psi(\phi) = \mathbb{P}(\Phi(t) < 0, \text{for some } t | \Phi(0) = \phi) \tag{2.5}$$

which occurs when $\Phi(t) < 0$ at some t (Dufresne and Gerber, 1989; Constantinescu and Thomann, 2005; Wüthrich and Merz, 2013).

This classical model of ruin theory can also be adapted to account for i.i.d. claim amounts X_i occurring based on other distributions, including exponential distributions and other variations. The Sparre–Anderson model expands the Cramér–Lundberg model to consider the i.i.d. assumption where claim inter-arrival times follow arbitrary distribution functions (Andersen, 1957). Essentially, instead of assuming exponentially distributed inter-arrival times, the Poisson process allows for inter-arrival times to have any distribution as long as the inter-arrival times are i.i.d. with a finite mean. The Sparre-Anderson model is also defined as

$$\Phi(t) = \phi + ct - \sum_{i=1}^{N(t)} X_i, \text{for } t \geq 0, \tag{2.6}$$

but $N(t)_{t \geq 0}$ follows the Poisson process with arbitrary distribution functions for i.i.d. claim amounts X_i (Thorin, 1974).

The i.i.d. requirement is a common assumption underlying statistical analyses (Gill and Bao, 2024). Simply, a dataset of random variables is assumed to be i.i.d. if each random variable has the same probability distribution as the others but is produced without being conditional on any other variable in the dataset. In mathematical terms, the assumption of i.i.d. relies on random variables X and Y in a sample being *independent*, defined as

$$P(X \cap Y) = P(X)P(Y), \tag{2.7}$$

and the sample of n random variables, $X_i, X_2, \ldots, X_n$, being *identically distributed* with each variable X_i having the same mean μ and variance σ^2, defined as

$$E(X_i) = \mu \text{ and } Var(X_i) = \sigma^2. \tag{2.8}$$

Random variables that are identically distributed do not necessarily all have the same probability. Furthermore, the i.i.d. assumption is only met when n random variables are *both* independent *and* identically distributed—violation of either independence or being identically distributed within the sample means that the variables are not i.i.d. (Gill and Bao, 2024).

This study examines whether the *identically distributed* requirement for i.i.d. is satisfied for extortion payments, including common violations such as the underlying distribution of the sample shifting over time, known as "concept drift" (Webb et al., 2016). Random variables must share the same probability distribution, but that distribution can be of any type, such as normal distribution, exponential distribution, Poisson distribution, etc. More precisely, random variables in a sample are considered identically distributed if and only if the cumulative distribution function (CDF)—the probability that a random variable will take on a value equal to or less than said value in a sample—of each random variable is the same as that of other random variables in the sample. Additionally, as the CDF is the integral of the probability density function (PDF), which is the probability that a random variable will take on a value equal to said value in a sample, it follows that identically distributed random variables in a sample would have the same PDF (Gill and Bao, 2024).

In this study, we specifically assess whether the i.i.d. assumption for sub-claim cryptocurrency extortion payments within claim amounts X_i is satisfied for both Cramér-Lundberg and Sparre–Anderson models.

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

3. Data and methodology

3.1. Data

The data in this study are extortion payments paid in Bitcoin (BTC) cryptocurrency to ransomware threat actors using one of 145 ransomware strains or variants between 2011 and 2024. Cryptocurrency transaction data have been a source of data for research on ransomware threat actors and victims in previous studies (e.g., Wang et al., 2021; Turner et al., 2025). The dataset was created by the authors. Extortion payment amounts were collected from the public ledger for the Bitcoin blockchain using BTC addresses, as explained in the next subsection. The structure of our data does not reveal how many victims did not pay extortion amounts, as we are only able to conduct our analyses on observed transactions. Transactions of zero do not show up in the blockchain, but we do discuss payment ratios below.

Regarding the completeness of our aggregated dataset, one limitation is that the data included are a sample of convenience, and we acknowledge that there are many payments not present. Regarding the reliability of our data, each extortion amount was verified by transaction information on the BTC blockchain, and sometimes in the news as well. We excluded any extortion amounts that could not be confirmed by the blockchain public ledger; thus, the data included in this study are traceable and peer-reviewable. Replication and validation of this study's findings can be conducted by requesting data from authors; independently recreating the dataset based on our Methodology; or using crowdsourced data, e.g. the ransomware project, or data from a blockchain analytics firm such as Chainalysis (Cable, 2024).

3.2. Methodology

Bitcoin addresses were gathered by extracting BTC addresses from malware binary samples and ransom notes from confirmed ransomware attacks, following existing accepted practices. For example, one could acquire malware binary samples from publicly available repositories used by security researchers, incident responders, and/or forensic analysts (e.g. VirusShare), as well as publicly available scanning and verification tools for malware (e.g. VirusTotal). Malware binary samples are executable files that contain code for executing the malware on a device or system for an attack, and these samples are often used for reverse engineering for cybersecurity research (Ferguson et al., 2008).

The process for aggregating BTC addresses involved using a regular expression to extract BTC addresses from malware binary samples and text files associated with ransomware attacks. To protect against false positives, every BTC address was validated with the address validation mechanisms publicly available on the Rosetta Code website (RosettaCode, n.d.). After a BTC address was validated as a legitimate BTC address, soft attribution was performed via fuzzy hashing—a matching technique using a hash function to focus on common patterns or structures and allow for small variations or differences—of the ransom note or the malware itself, e.g. with TLSH (Trendmicro Locality Sensitive Hash). With this technique, each malware binary sample was assigned a ransomware strain or variant by matching the binary malware sample or the ransom note to previous samples from a known ransomware strain or variant. Many of these soft attributions have been validated with other data sources, such as Ransomlook, that classify BTC addresses into ransomware strains and variants (Dulaunoy et al., 2024). When this soft attribution was not possible, the BTC address was put into a bucket known as "unaffiliated" until soft attribution may be possible in the future. All of these unaffiliated addresses (N = 2022) were excluded from this study.

Once collated into a ransomware strain or variant, extortion payments to the BTC address were traced using the public BTC blockchain. We focused only on the incoming transactions (extortion payments from victims) and not on outgoing transactions (withdrawals by threat actors). Confirmed transactions were converted to US dollar (USD) amounts using the average price of BTC on the day of the transaction, which is a standard practice in any research assessing the value of cryptocurrency or other digital assets over time (Conti et al., 2018; Cable et al., 2024). Additionally, to explore if the demand value of extortion amounts was independent of fluctuating BTC price, we analysed a 3-year moving average of both BTC price and extortion payments to establish a lack of correlation (see Appendix A).

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

Herein, we conduct descriptive statistics of our data, as well as empirical analyses of specific ransomware strains/variants and incidents. We then determine whether the i.i.d. assumption is valid for extortion payments across and within our data using multiple tests, including a Kruskal–Wallis, Spearman's Correlation, Cramer von Mises, and Kolmogorov–Smirnov. Violations of either independence or identical distribution for extortion payments violate the i.i.d. assumption, suggesting that ransom demands are generated by the different processes (tools, tactics, and procedures) associated with certain ransomware strains/variants or specific threat actors.

4. Results

4.1. Descriptive statistics

Table 1 displays summary statistics for our ransom paid dataset. The data include 121,762 extortion payments paid to threat actors, totalling more than a billion dollars (USD) in extortion payments ($1,275,242,024.72 USD). The largest extortion payment included in the study is $24,837,732.88. The median extortion payment across the entire timespan of our dataset was $251.90 (all USD herein), and more recently, over the last three years, the median extortion payment was $396.36. Overall, our data indicate that from 2011 through 2024, 92% of extortion payments were below the average of $10,473.23, and over the last three years, 93% of extortion payments were below the average of $186,277.40. Beyond these aggregate statistics, we also investigated the mean-to-median ratio of extortion payment amounts across all ransomware strains and variants in the dataset (see Appendix B). The mean-to-median ratio is an indicator of distributional skewness, as discussed in Florêncio and Herley (2011), which suggests a range of variability in ransom demand behaviours that are associated with ransomware strain or variant used by a threat actor.

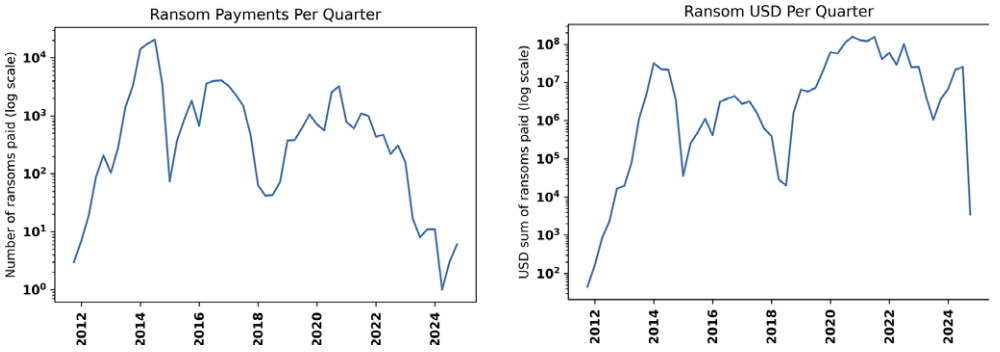
As discussed, the frequency and severity of cybersecurity incidents, especially those involving large-scale breaches or high-impact attacks, often exhibit heavy-tailed distributions, deviating substantially from the expectations of normal or Poisson-like event models. These fat-tailed characteristics suggest that extreme events, though rare, occur with disproportionate impact and frequency. Figure 1 provides an overview of the frequency and severity of extortion payments in our dataset. In reference to the two tiers of cyber risk, while extortion payments stem from tier 1 risks, these payments also represent tier 2 risks, with the number of payments in a certain time frame stochastically fluctuating.

Shown in Figure 1a, there is high variance in the frequency of extortion payments, with some quarters having thousands of extortion payments by victims, accumulating in a global level impact. Further complicating the issue is the varying adjusted USD amount for these payments as well, as seen in Figure 1b. To additionally visualize the differences between ransomware strain variants, Figure 2 provides a graphical representation of the log variances in extortion payments across all of the ransomware strains and variants in our data. Along with the extortion amount, the frequency of extortion payment also varies between ransomware strains/variants, as well as over time (see Appendix C).

Table 1. *Summary statistics*

Statistic	USD
Median	$251.90
Mean	$10,473.23
Standard deviation	$221,603.70
Minimum	$0.01
25% Quartile	$16.83
50% Quartile	$111.74
75% Quartile	$635.60
Maximum	$24,837,730.27

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press



(a) *Number of extortion payments by quarter*

(b) *USD summed amount for extortion payments by quarter*

Figure 1. *Characteristics of extortion payments by ransomware victims over time in our dataset. (a) Quarterly plot of the number of extortion payments by ransomware victims from 2011 to 2024. (b) Quarterly plot of the summed USD amount for extortion payments by ransomware victims from 2011 to 2024. Note particularly that the decrease in payments in (a) does not lead to reductions in (b): bigger payments are happening less often for equivalent profits.*

4.2. Anecdotal case examples

With known differences in extortion payments between ransomware strains/variants, we provide case examples of unique distributions of extortion payments for three different ransomware strains or variants to qualitatively and empirically investigate the i.i.d. assumption. Some ransomware strains/variants used a fixed-price business model where a ransom demand amount was fixed regardless of the victim, and others used a negotiated-price business model where victims negotiated with ransomware actors on the amount of the extortion payment. Fixed-price extortion payments are uniformly distributed, as expected for such a business model, and the negotiated extortion payments are characterized by a variety of distributions from normal distribution to power-law distribution. Our first case example is the *WannaCry* ransomware attack.

4.2.1. WannaCry *ransomware*

The 2017 *WannaCry* ransomware attack was wide-ranging, affecting more than 300,000 computers across 150 countries (see Figure 3) (Akbanov et al., 2019; BBC, 2017). The initial ransom demand for victims was $300 USD to be paid in Bitcoin (Figure 3a), but doubled to $600 USD during the ongoing campaign (Gibbs, 2017). While the threat actor behind the attack was using a fixed-price model, the price doubling makes clear that the distribution of extortion amounts can change over time, even within one ransomware attack, highlighting the 'concept-drift' breaking element of the i.i.d. assumption.

The initial attack on May 12, 2017, was massively curtailed within hours by a researcher who discovered a kill-switch, and though there were attempts to update the mechanisms of attack to continue spreading, the initial campaign was ultimately ended in about a week's time. This is shown in Figure 3b with the extreme spike in extortion payment frequency in a short time frame in 2017 followed by a much lower frequency, though still continuing into 2023. This can be attributed to numerous *WannaCry* ransomware variants and old software. *WannaCry* is a ransomware family, with the 2017 attack involving the *WannaCry* 2.0 strain out of three strains currently in existence (Yang, 2017), and those strains have now led to thousands of variants that continue to be used by threat actors. Additionally, *WannaCry* ransomware relies upon the EternalBlue exploit for older Microsoft systems that are still vulnerable if they have not been effectively patched (Goodin, 2017).

While there has been debate as to attribution, the United States and United Kingdom formally announced that North Korea's Reconnaissance General Bureau was responsible for the ransomware

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

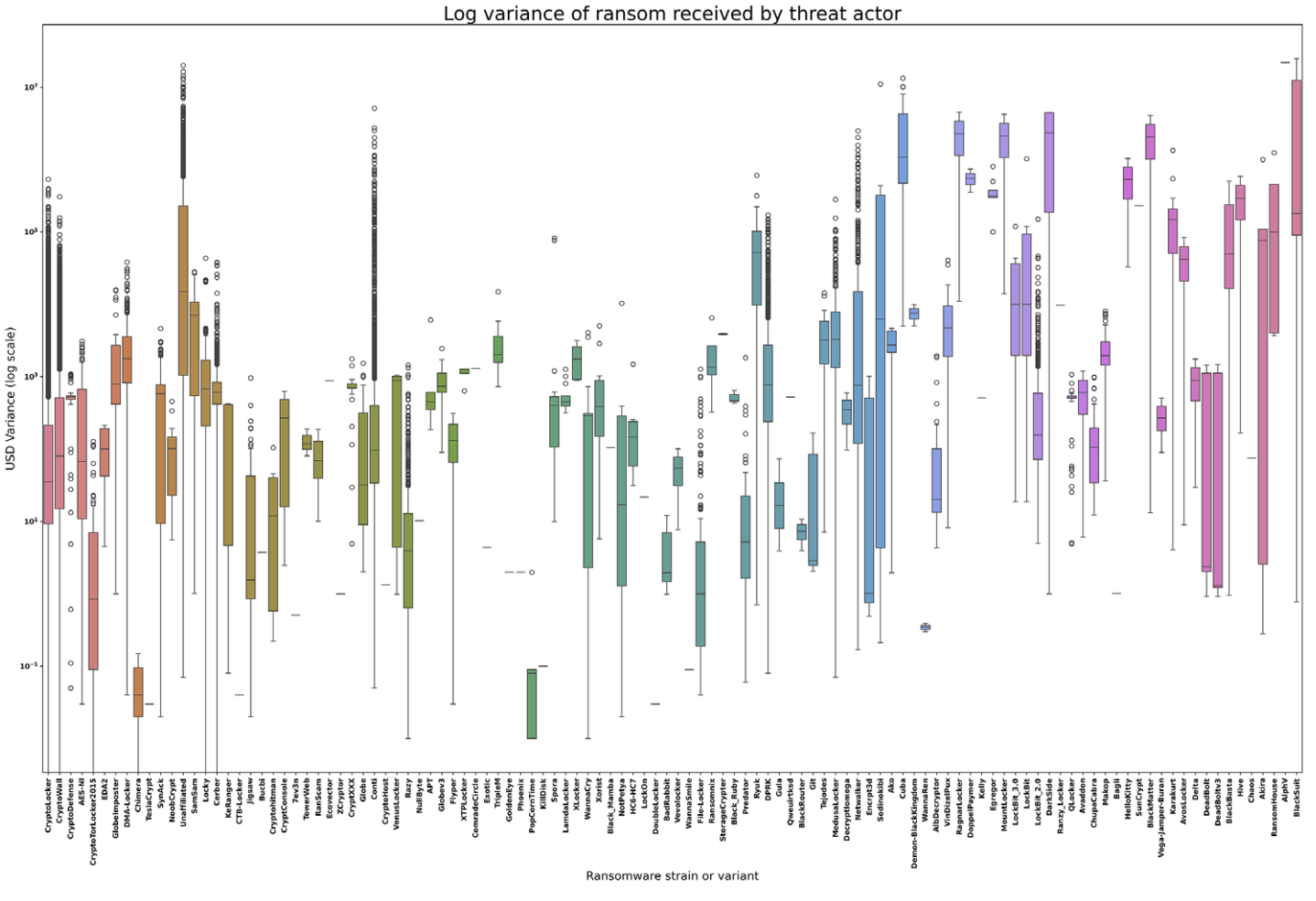
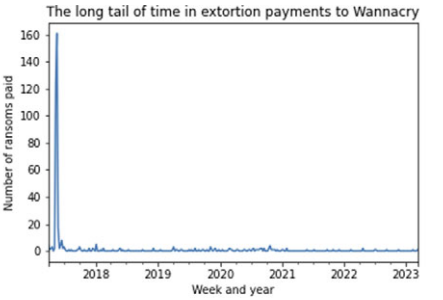
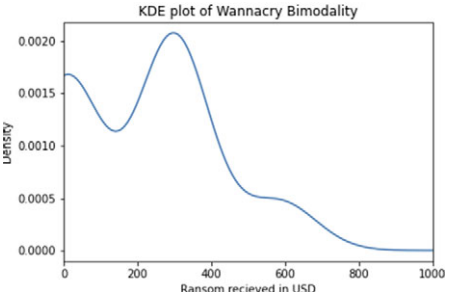


Figure 2. *Variance of extortion payments according to ransomware strain or variant. Boxplot of log variance of extortion payments for each of the ransomware strains and variants in the data, including lower and upper quartiles and outliers. Variance was logged for numerical stability and to maintain positive values.*

(a) *WannaCry Ransom Note*



(b) *Weekly Frequency of WannaCry Extortion Payments*



(c) *KDE of Bimodal Distribution of WannaCry Extortion Payments.*

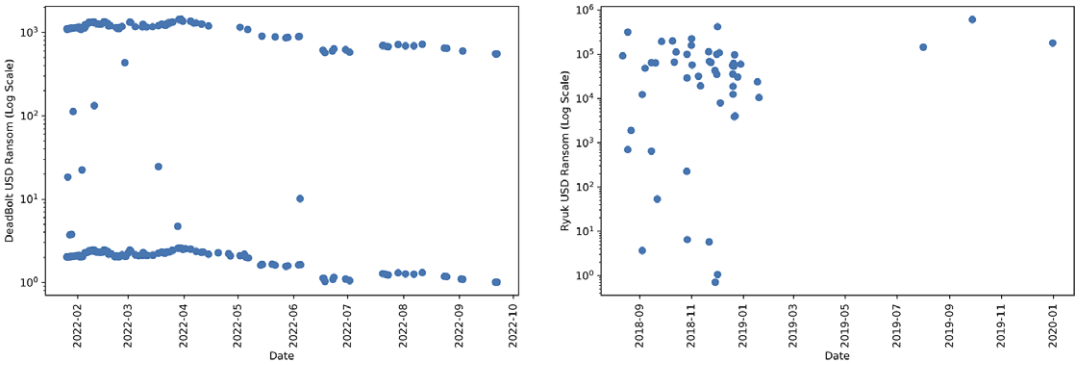
Figure 3. *Ransom demand for* WannaCry 2.0 *ransomware and distributions of extortion payments. (a) Example* WannaCry *extortion demand note requesting a USD extortion payment be transferred in BTC. (b)* WannaCry *extortion payment frequency on a weekly basis, with extortion payments continuing after the initial primary campaign. (c) Kernel density estimation (KDE) of the bimodal distribution of fixed-price* WannaCry *extortion payments.*

attack (DOJ, 2018). North Korea may have benefited geopolitically by targeting states deemed adversarial to their interests, but the attacks were predominantly financially motivated, considering the increase in ransom demand amount during the attack, and knowledge from the intelligence community that North Korea uses such attacks to fund military objectives (CISA, 2023). The extortion amounts in USD had a bimodal distribution (see Figure 3c for estimation of PDF with kernel smoothing), and while other ransomware strains/variants in the dataset also have bimodal distributions, each is distinctly different. This speaks to the twinned issues of ransomware as an economic national security threat, which is distinct from national security threats that use ransomware as a cover story; it benefits everyone to sort the financially motivated crime from the espionage.

4.2.2. Deadbolt *ransomware*

We next examined *Deadbolt* ransomware attacks. Compared to *WannaCry*, one may expect that more recent ransomware attacks would involve negotiations for ransom demands due to technological leverage, but there are still examples, such as *Deadbolt* ransomware attacks, of a fixed-price approach to reject this notion (Figure 4). *Deadbolt* ransomware attacks operate with a flexible flat fee demand of between 0.03 BTC and 0.05 BTC (see Figure 4a) without any mechanism for negotiation if desired (no email address, chat handle, or domain listed in the ransom demand notes) (Chainalysis, 2023; Ellzey, 2022; Muncaster, 2022). There is an additional pattern of low-high extortion payments due to how the decryption key is sent to victims who pay ransoms. Once a victim pays the ransom, the decryption key is sent automatically via

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press



(a) *Value of Deadbolt Extortion Payments Over Time* ***(b)*** *Value of Ryuk Extortion Payments Over Time*

Figure 4. *Value of* Deadbolt *and* Ryuk *extortion payments over time. (a) Value of* Deadbolt *extortion payments from January 2022 through September 2022. (b) Value of* Ryuk *extortion payments from August 2018 through January 2022.*

the blockchain as a low-value Bitcoin transaction to the ransom address with the decryption key written in the OP_RETURN field of the transaction (Chainalysis, 2023).

It is also important to note that other variants of *Deadbolt* don't necessarily follow the same behaviour. *Deadbolt* ransomware specifically targets network-attached storage (NAS) devices, and while there is a fixed-price model for end customers, another variant targets NAS vendors for much higher amounts that vary, e.g. $192,000 USD to $959,000 USD (Muncaster, 2022). Though attribution remains unclear, intelligence agencies have advised that *Deadbolt* ransomware is also routinely used by North Korean actors, state-sponsored or otherwise. Compared to the *WannaCry 2.0*'s extortion payment bimodal distribution (PDF in Figure 5a, CDF in Figure 5d), *Deadbolt* has a similar bimodal distribution for extortion payments but is still distinctly different based on extortion payment amount and frequency over time (PDF in Figure 5b, CDF in Figure 5e). One possible explanation for the difference is that *Deadbolt* has also been observed to be used by other actors outside of North Korea (CISA, 2023).

4.2.3. Ryuk *ransomware*

Lastly, we examined *Ryuk* ransomware for our third case example. *Ryuk* ransomware first emerged in February 2018, and by 2021, threat actors had made more than $150 million USD (Cimpanu, 2021). The ransomware, which is actually a variant of *Hermes* ransomware, has been attributed to the Wizard Spider group of Russian affiliation (Micro, 2024). *Ryuk* ransomware attacks followed a negotiated-price business model and specifically targeted high-profile victims for maximum profit, including healthcare facilities, schools, government facilities, etc. (CISA, 2020) (Micro, 2024). In contrast to the fixed-price models of the *WannaCry* and *Deadbolt* strains/variants in our data, *Ryuk*'s negotiated-price model is observably different in frequency of and variance in extortion payment amounts, as shown in Figure 4b, as well as in the PDF and CDF, as shown in Figure 5c and Figure 5f, respectively (Gray et al., 2023).

Alongside the negotiated-price business model, the Wizard Spider group also had distinct patterns in their methods of attack, using specific malware like Trickbot and Emotet to compromise systems and other commercial products to gain access to ultimately execute *Ryuk* (CISA, 2020) (Micro, 2024). Additionally, the group is also associated with other notable ransomware strains and variants, including *Conti* ransomware. We analysed the PDF and CDF of *Conti*, as well as *LockBit* (Russian-affiliated with double extortion business model) and *Cuba* (Russian-affiliated with negotiated-price model for high-profile targets) (see Appendix D). While comparing frequencies, ransomware business models, PDFs, and

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

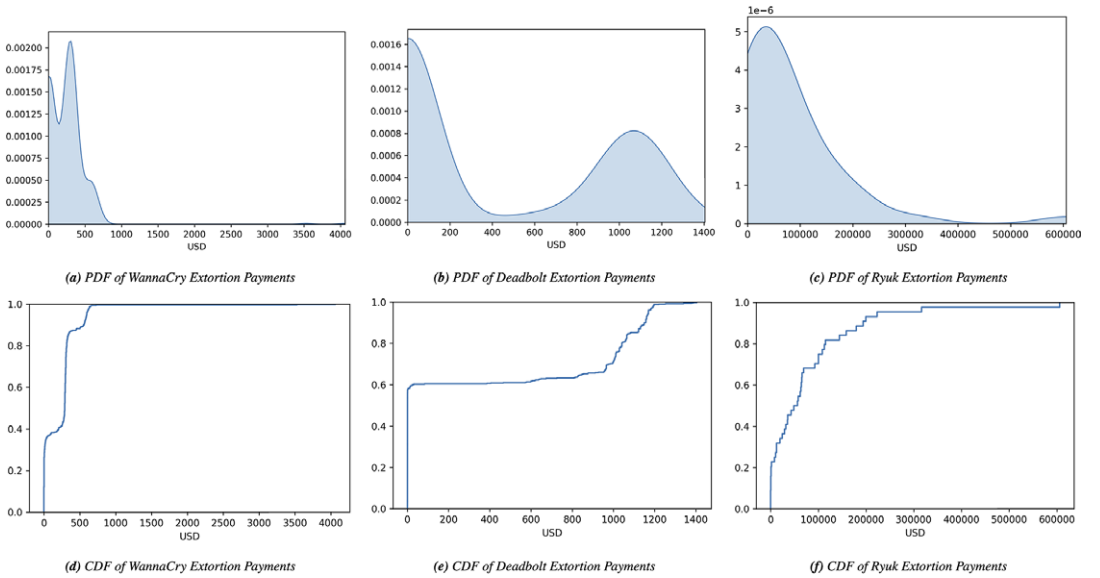


Figure 5. *(top) Probability density function (PDF) graphs for (a)* WannaCry*, (b)* Deadbolt*, and (c)* Ryuk *extortion payments demonstrating the probability density at specific amounts across the range of payment values, respectively. (bottom) Cumulative distribution function (CDF) graphs for (d)* WannaCry*, (e)* Deadbolt*, and (f)* Ryuk *extortion payments demonstrating the probability that a random extortion payment is less than or equal to an extortion amount across the range of payment values, respectively.*

CDFs is not quantitatively causal for rejecting our null hypothesis, it does anecdotally indicate that there is high variability in ransomware attacks and ransom payments, which does not support the use of monolithic insurance coverage from cyber insurance providers.

4.3. Testing for i.i.d. assumptions across ransomware strains/variants

We first conducted the Kruskal–Wallis (KW) test (also known as the one-way ANOVA on ranks test) to determine if multiple samples are produced from the same distribution for non-parametric data (Kruskal and Wallis, 1952). The null hypothesis for the KW test for our study is that a randomly observed extortion amount from any ransomware strain/variant is neither more nor less likely to be larger in value than a randomly observed extortion amount from any other ransomware strain/variant in our dataset. Our analysis of variance of extortion payment against ransomware strain/variant resulted in a Kruskal H-value of 21732.919363219826 (p-value = 0.00000) (DATAtab, n.d.).

Since the KW test is insensitive to outliers, the H-value calculation generally relies only on extortion amounts within each ransomware strain or variant having identically distributed values with finite means and variances (Kruskal and Wallis, 1952). Under the strict assumption of identical distribution, our high H-value and significant p-value would suggest that we could reject the KW null and assume that at least one randomly observed extortion amount from any ransomware strain/variant is more likely to be larger in value than a randomly observed extortion amount from any other ransomware strain/variant. However, if we accept that the distributions in our dataset are not each identically distributed, as we have shown with our case examples, our interpretation of the result is that though we may reject the null, there is evidence that least one ransomware strain/variant is stochastically larger than at least one other ransomware strain/variant at the level of $p \leq 0.05$ significance.

We next conducted an analysis of Spearman's rank correlation coefficient, a non-parametric measure of statistical dependence between the rankings of two variables, to check for correlations between

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

extortion payments and time (Spearman, 1904). The coefficient assesses the strength and direction of the relationship between two variables based on a monotonic function, which is less restrictive than that of Pearson correlation coefficient based on a linear relationship (Kowalski, 1972). The calculation uses the assumption that the two variables represent paired observations, and these observations are independent. For our analysis, we calculated Spearman's coefficient to determine if time has an impact on extortion amounts, and our results of a low Spearman's coefficient of 0.311502709075461 (p-value = 0.00000) indicates statistically dissimilar ranks between extortion payment amounts and time. This result suggests that the assumption of i.i.d. may not hold, as extortion payment amounts appear to be dependent on the ransomware strain/variant. While they may be independent of time, their dependence on strain/variant introduces a potential source of non-independence in the data.

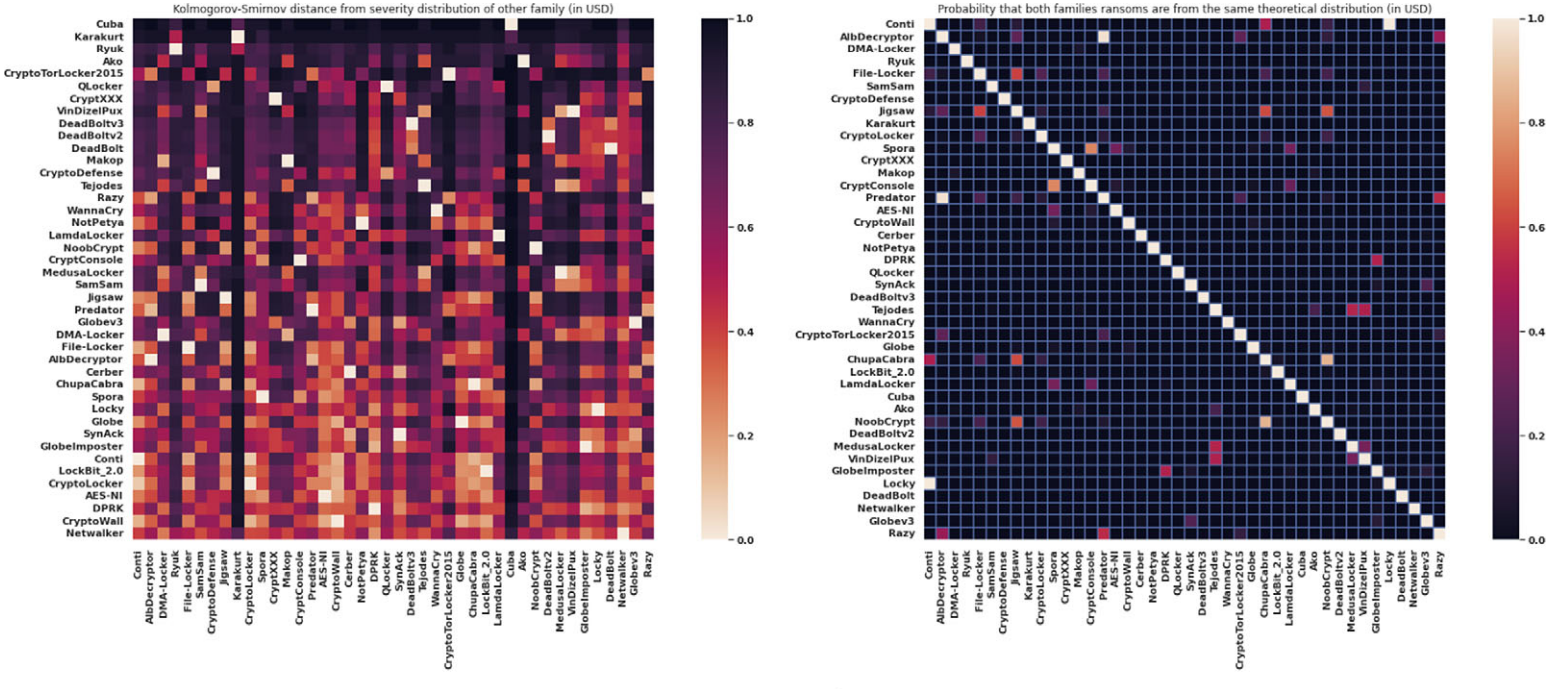
To further investigate the relationship between extortion payment amounts in our data, we conducted various tests to ascertain distance metrics—degree of similarity or difference between two data points—within our dataset. The Kolmogorov–Smirnov test (KS test) takes two forms: 1) a one-sample KS test that compares whether an empirical sample comes from a theoretical probability distribution, and 2) a two-sample KS test that compares whether two independent empirical samples come from the same theoretical probability distribution (Massey, 1951). Both tests involve comparing the CDFs to determine whether samples come from the same underlying distribution. We used the two-sample KS test to evaluate extortion payments of different amounts matched in their timestamp distributions (Figure 6). Additionally, the use of the two-sample KS test also mirrors a widely accepted approach for pricing distribution fitting (Parodi, 2023), adding relevance to the discussion of pricing and solvency.

With inspiration from Liao et al. (2016), we used a time-series analysis of the data, expanding across multiple ransomware strains/variants, to examine how likely it is that extortion payments for two ransomware strains/variants are drawn from the same probability distribution. In particular, we compared different strains/variants across the entire dataset, as well as compared variants of the same strain against each other (Figure 6a). We additionally assessed the p-value of these two-sample KS tests (Figure 6b) for assessment of the significance of the results across all ransomware strains/variants. While the KS test is a regularly used goodness-of-fit test for non-parametric data, it does have some weaknesses. In particular, since the KS test compares the underlying CDFs for heavy-tailed distributions, the tails of the CDFs are more precise than the middle of the function, leading to the overall KS test losing sensitivity in the tails. Thus, we decided to examine distribution distance with higher sensitivity metrics than the KS test, including Wasserstein distance and the Cramer von Mises metric (see Supplementary Appendix E).

Wasserstein distance determines the minimum cost for transforming one probability distribution into another with considerations for spatial arrangements of the data and overall shapes of the distributions (Patriarca et al., 2016). This method is more sensitive to shifts in the central data than outliers and more robust to differences in the tails of distributions. The Cramér von Mises metric assesses the goodness of fit of a CDF compared to the empirical distribution function, i.e. the distribution function of the empirical measure of the sample, by evaluating the sum of squares of differences (Cramér, 1928). The metric modifies the parameters of a normal distribution to account for positive and negative deviations. The results from the Wasserstein distance Supplementary Figure S4a) and the Cramer von Mises metric (Supplementary Figure S3a) further support that ransomware payments do not have similar probability distributions across families.

We performed additional testing for distribution fit and autocorrelation within our dataset, though it should be noted that further investigation along these lines of inquiry is beyond the scope of the present study. The Anderson–Darling test (AD test) is a statistical method for evaluating the goodness-of-fit between empirical data and a theoretical distribution, including those with heavy-tailed characteristics (Anderson and Darling, 1952). Unlike the KS test, the AD test applies greater weight to discrepancies in the distribution's tails, thereby enhancing its sensitivity to extreme values often encountered in finance and risk modelling. This property makes it particularly well-suited for assessing distributions where tail behaviour—often indicative of rare but high-impact events—is of analytical importance. We conducted the AD test using well-established distributions (normal, exponential, logistic, Weibull min, and Gumbel (Extreme Value Type I) distributions) at different levels of significance. Our results indicate that ransom

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press



(a) *Pairwise Kologorov-Smirnov Distance by Ransomware Strain/Variant*

(b) *Pairwise Kologorov-Smirnov p-Value by Ransomware Strain/Variant*

Figure 6. *Pairwise Kolmogorov–Smirnov test (KS test) heat maps for distance with p-values. (a) Heat map of pairwise KS test between all ransomware strains/variants in our dataset. (b) Heat map of corresponding p-values for the results of the KS test in (a).*

payments across ransomware strains/variants in the dataset do not fit these chosen distributions, though a limited number of observations within strain/variant showed alignment with these distributions (see Appendix E).

Lastly, we performed two tests for autocorrelation between observations, given the time span of our dataset and considerations for temporal activity in claim payments for solvency. Again, it should be noted that further time-series analyses of the data are beyond the scope of the present study. Understanding the non-normal distribution of our data, we conducted the Durbin-Watson test (DW test) (Durbin and Watson, 1971) and the Ljung–Box test (LB test) (Ljung and Box, 1978) for serial correlation. Neither test requires normality, though they do assume independence under their respective null hypotheses for no autocorrelation. Our results indicated that ransom payments within ransomware strains/variants in the dataset have positive serial correlation, though a few ransomware strains/variants demonstrated no autocorrelation (see Supplementary Appendix E). Taken with the other results from our analyses, this suggests that even within ransomware strain/variant groupings, the assumption of independence is predominantly violated across strains/variants in our dataset.

5. Discussion

The findings of this study raise critical concerns about the applicability of classical solvency models—particularly those grounded in the assumption of independent and identically distributed loss events i.e. Classic Ruin models—in the context of ransomware incidents. Empirical analyses of extortion payment data reveal significant departures from i.i.d. assumptions, calling into question the reliability of classical ruin theory when used to assess financial resilience against solvency in the face of ransomware extortion. These violations are not merely statistical artifacts; they reflect deeper structural features of the ransomware threat landscape, including temporal clustering of attacks, heavy-tailed payment distributions, and potential for coordinated threat actor behaviour. As such, our results suggest that existing frameworks may systematically underestimate the risk of insolvency for cyber insurers providing coverage for extortion payments, necessitating new models and updated regulatory standards.

Overall, the results of the present study suggest an underlying tension between observed ransomware extortion payment data and the core assumptions underpinning classical ruin theory. The distribution of ransom payments violates key conditions necessary for solvency assessment within this framework—most notably, the assumptions of independence and identical distribution in both severity and inter-arrival times, as well as the requirement of a finite mean. The violation of ruin theory conditions affects not only cyber insurance firms offering extortion payment coverage based on these specific model assumptions, but also self-insured organizations, third-party negotiators, and risk modellers operating in adjacent spaces. Many stakeholders may assume that ransom payments and associated losses are closely related, even interchangeable from a modelling perspective, but such assumptions have not been empirically validated and should not be assumed. If the distribution of ransomware payments lacks a finite mean, as heavy-tailed behaviour would suggest, then the perceived insurability of these events may be an artefact of insufficient data rather than a reflection of actual risk structure. As ransomware threats continue to evolve, any risk assessment framework that overlooks these distributional properties is likely to underestimate the true exposure facing firms and insurers alike.

We do not argue that ransomware extortion payments are difficult to insure solely due to their statistical variance or volatility. Rather, our findings suggest that insuring ransoms as a sub-coverage introduces significant solvency concerns, rooted not in randomness but in the underlying heterogeneity of causal processes that generate ransomware claims. Modern ransomware operations employ a range of coercive tactics, including data exfiltration, system encryption, and operational disruption, often within a single campaign. These tactics represent distinct mechanisms of leverage, reflecting varied threat actor objectives and capabilities. To assume that ransom demands emerge from an i.i.d. process is to overlook the strategic heterogeneity among threat actors and the resulting complexity in how extortion is executed and monetized.

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

Once we acknowledge that extortion amounts are neither identically distributed nor reliably independent, a deeper causal inquiry becomes necessary. This variation is not incidental; it is shaped by both predator and prey dynamics. Specifically, it is important to consider whether this variability is primarily driven by characteristics of the threat actors (i.e. *predator* effect) or by the attributes and behaviours of the targeted organizations (i.e. *prey* effect). On the threat actor side, technological factors such as the preferred exploits of initial access brokers, the quality of lateral movement tools, or the ability to scale across networks can all influence the magnitude of potential losses. Additionally, targeting preferences, whether based on geography, sector, or organization size, are not static, but evolve in response to shifting incentives and observed payer behaviour. For instance, there is evidence that threat actors adjust their targeting to focus on jurisdictions or industries with a higher historical likelihood of ransom payment. These behavioural adaptations reflect learning processes that further disrupt any assumption of statistical independence or distributional uniformity.

Victim-side characteristics introduce further heterogeneity in loss outcomes. Factors such as industry sector, revenue size, and negotiation practices may all contribute to the heterogeneity observed in extortion payment outcomes. Additionally, organizational factors such as sectoral regulation, technological maturity, incident response capabilities, and the economic cost of downtime contribute to the severity and composition of ransomware-related losses. For example, while privacy breaches may be of paramount concern in healthcare or finance, downtime may be far more consequential for energy utilities or logistics firms. Losses are thus a complex mixture of paid and unpaid ransoms, operational and reputational impacts, and idiosyncratic, systematic, and systemic risks—echoing frameworks described by Awiszus et al. (2023).

The complexity deepens with the involvement of state-sponsored or state-sanctioned ransomware operations, where the motivations of threat actors may shift away from purely financial gain toward geopolitical disruption. This possibility introduces a significant source of model risk, particularly for insurers and regulators relying on attribution-based exclusions to delineate the boundaries of insurable events. As several cyber war exclusions hinge explicitly on attributing intent or affiliation, models premised on rational economic actors may fail under scenarios where the primary objective is systemic damage rather than ransom extraction. In such contexts, the underlying assumptions of risk modelling and not just the statistical distributions require fundamental re-examination.

Attribution is a difficult task, and association with a nation-state actor can be murky, though there are some organized groups who are well known to be proxies for adversarial nation states (Egloff, 2017; Egloff and Egloff, 2022; Nershi and Grossman, n.d.). Studying victimization statistics has the potential to identify what is 'targeted' and what is "opportunistic." For instance, the *WannaCry* ransomware attacks in 2017 are widely believed by multiple countries to be attributable to North Korea's Reconnaissance General Bureau (Horsley, 2018; Bendiek and Schulze, 2021; Sumortier et al., 2020). North Korea, one of the major global threat countries, is also known to have a modus operandi of using such types of cybercrimes for monetary gain, specifically in cryptocurrency. In *WannaCry*, the ransomware attacks were conducted for financial gain, though of significance was the damage and disruption to critical sectors and services globally. However, it is important to note that these attacks were opportunistic, taking advantage of technological vulnerability, rather than specifically targeting certain victims.

Ransomware threat actors emanating from Russia behave differently, wherein threat actors are not state-sponsored but behave as indirect proxies for state interests. These threat actors follow a similar tactic of primarily pursuing financial gain alongside causing significant levels of damage and disruption. However, Russian-based actors tend to be more politically strategic in the choice of target and what type of disruption and damage they cause, which in turn increases their chances of safe harbour and Russia's indifference towards extradition efforts. Many of these ransomware incidents contribute to differences in ransom demand distributions and victim payment distributions. Furthermore, many ransomware threat actors operate as Ransomware-as-a-Service (RaaS), providing their ransomware variant to be used by other threat actors for a cut of the profits in return. From a cyber insurance perspective, insurers must be cautious as to how categorization and potential attribution of ransomware attacks are used for coverage determinations. We are thus careful to call out potential, directly state-sponsored threat actors or

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

campaigns in this study, as well as note that attribution to a ransomware strain herein may represent actions by the respective organized group and actions by other threat actors using said strain (or respective variants).

This discussion of attribution is not dialectical—there are real implications for the payout of insurance claims (attribution can impact policy coverage when involving nation state threat actors. For example, see Lloyd's Market Associations cyber war clauses and requirements regarding state-backed cyber attack exclusions; (Lloyd's Market Association, 2025)). Millions of dollars (USD) can and will be denied from insurance payouts if a claim is found to be generated by a nation-state threat actor. Moreover, a threat actor seeking to maximize damage rather than achieve financial gain also supports our findings that ransom payments are not i.i.d., as these ransom payments are more side effects than natural variance from an underlying generating function. Ransomware threat actors operate with distinct monetization strategies and business models, which influence not only how access is priced but also how victims are selected and engaged. These strategic differences suggest that ransomware attacks may reflect both predator effects (e.g. the chosen strain or operational variant) and prey effects, including sector, geography, and the target's willingness to pay extortion demands. For example, a ransomware variant tailored to German-speaking users or designed to exploit infrastructure in US-based firms will inevitably shape the demographic and economic profile of affected victims, and these prey-driven dynamics may result in observed ransom amounts that are more reflective of victim attributes than attacker intent (Rose-Ackerman and Palifka, 2016; Ridinger, 2018; Cimpanu, 2019).

Supporting this view, a pioneering study by Cybersecurity Centre Belgium found that the frequency of ransomware attacks correlates more strongly with national GDP than with population size, suggesting that financial capacity and not sheer exposure is a key determinant of targeting (Centre for Cybersecurity Belgium, 2024). This introduces a potentially endogenous relationship between victim demographics and ransom payment valuations, complicating assumptions of randomness or uniformity often used in risk models. Understanding this interaction between attacker behaviour and victim characteristics is crucial for refining both threat intelligence and actuarial assumptions in ransomware risk assessment. Additionally, this cultural variability applies both to perpetrators and victims in different but important ways (Banuri and Eckel, 2012). These dynamics would affect victims' Willingness To Pay (WTP) extortion demands, as well as the amount that victims can or do ultimately pay (Everett, 2016; Hernandez-Castro et al., 2020). Our study has only gently explored this as a causal factor in why extortion amounts are not identically distributed and future research will hopefully expand on these themes.

While our findings challenge the assumption that extortion payments are identically distributed and thus readily insurable, we do not extend this argument to ransomware losses in general. The distinction between extortion payments and losses is both practical and conceptual: ransom demands may correlate with observed losses, but correlation alone is insufficient to establish equivalence or causality. It is entirely possible for a ransom-related loss to correlate with both threat actor behaviour and victim characteristics, yet emerge from distinct underlying distributions. In fact, we suggest that ransomware losses may align more closely with organizational factors such as revenue, sector, and geography than with the statistical properties of ransom demands and extortion payments. The misconception of equivalency persists in both public discourse and industry practice and warrants careful correction in both actuarial modelling and policy development.

Ultimately, the continued practice of insuring ransomware extortion payments without addressing the underlying statistical irregularities raises important questions about the rationale guiding both insurer behaviour and broader market practices. Regulatory bodies tasked with overseeing financial risk in the cyber domain should treat these findings as a signal for urgent re-evaluation.

5.1. Implications for regulatory standards and policy

Ransomware presents a complex and escalating risk management challenge for both governments and the global economy. In the absence of reliable data on the frequency and cost of attacks, organizations struggle to justify sustained investment in cybersecurity defence measures, perpetuating a cycle of

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

vulnerability and loss. This uncertainty contributes to a growing economic burden, with ransomware-related damages now estimated to exceed $ 1 billion (USD) annually (Chainalysis, 2024). From a regulatory and policy standpoint, there are two critical paths forward: 1) the promotion of open, transparent risk models that enable organizations to quantify cyber risk and allocate defensive resources accordingly; and 2) coordinated efforts to de-monetize ransomware through legislative, regulatory, and insurance-based interventions. However, as our findings demonstrate, the statistical properties of extortion payments, specifically their non-i.i.d. nature, potentially undermine the reliability of insurance as a stand-alone solution. Any regulatory strategy aimed at managing ransomware risk must therefore account for the limitations of classic Ruin Theory in modelling and mitigating this uniquely dynamic threat.

Ransomware operates as a globally correlated risk, and the continued payment of ransoms may be artificially inflating cyber insurance premiums by introducing a direct path to insolvency. The inability to achieve effective risk pooling in the face of systemic cyber threats has been well documented in industry analyses (Lee, 2023), and it offers empirical validation for predictions made by Böhme and Kataria (Böhme and Kataria, 2006). Our findings suggest that when insurers repeatedly cover ransom payments, they expose themselves not just to increased claim frequency but to a compounding solvency threat. In effect, insurers that routinely finance extortion payments take on an accumulating tail risk, one that brings them incrementally closer to ruin. It is essential to emphasize that ransomware has already proven capable of bankrupting organizations across sectors (Bilton, 2025)—cyber insurance providers are not exempt. These firms face at least two existential exposures, including the threat of becoming targets themselves and the financial consequences of underwriting a class of risk that defies underlying model assumptions. Without intervention through regulatory oversight, revised underwriting practices, or market-wide norms, this dynamic may undermine the long-term viability of ransomware sub-coverages altogether.

The distinction between pricing adequacy and solvency assurance is central to the regulatory oversight of insurance markets, particularly when confronting dynamic risks such as ransomware. As defined by the Actuarial Standards Board of America, capital represents "the funds intended to assure payment of obligations from insurance contracts, over and above those funds backing the liabilities" (Actuarial Standards Board, 1997). This highlights a crucial point: while accurate pricing is necessary, it is not sufficient to guarantee solvency, particularly in the presence of non-i.i.d. processes that undermine certain models. Ruin Theory, rather than pricing alone, provides a formal framework for assessing long-term solvency. From this perspective, the insurability of ransom payments depends on whether their statistical properties satisfy the assumptions underpinning that theory, specifically independence and identical distribution. In the absence of such conditions, it is incumbent upon regulators to reevaluate solvency requirements for insurers engaged in ransomware payment coverage, potentially mandating more conservative capital buffers.

This regulatory imperative is echoed in established guidance on general insurance pricing, which states that "regulation may prescribe a minimum amount of capital that an insurer has to hold for the risks it underwrites" (Parodi, 2023). Moreover, the guidance reinforces that "specifically for pricing, the firm will need to be able to demonstrate that all pricing decisions and assumptions are documented, monitored, and linked to the firm's capital model" (Parodi, 2023). In the context of pricing and ransomware coverage, such documentation should explicitly account for the tail-risk properties of ransom payments and their divergence from standard distributional assumptions. Without this linkage, pricing decisions may appear actuarially sound while still exposing firms to unacceptable solvency risk.

Addressing these challenges will require more than technical adjustments to existing models; it demands a reconsideration of the data and assumptions that underpin cyber risk assessment. Heavy-tailed phenomena, by their nature, require substantially more data to produce reliable statistical inferences. However, the opacity of ransomware incidents, under-reporting, and inconsistent disclosure practices continue to limit the availability of comprehensive datasets. Regulators, insurers, and cybersecurity firms must collaborate to develop data-sharing mechanisms that respect privacy and legal

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

constraints while enabling rigorous empirical analysis. Without such efforts, the modelling of ransomware risk will remain constrained by structural blind spots, leading to potentially flawed pricing, inadequate reserves, and misplaced confidence in the insurability of extreme events. In this context, regulatory guidance could play a catalytic role in setting minimum standards for disclosure, particularly where systemic cyber risk threatens broader financial stability.

Another critical regulatory implication of our findings is the need for enhanced transparency and oversight of solvency models used by insurers offering ransomware extortion payment coverage. Given the demonstrated violation of i.i.d. assumptions in ransom payment distributions, regulators should require firms to rigorously document the assumptions, limitations, and data sources underlying their capital models. This documentation would not only support more accurate solvency assessments but also create the conditions for improved regulatory monitoring and cross-firm comparison. The benefits of such oversight include greater confidence in insurers' financial resilience, reduced systemic exposure, and the ability to identify market-level modelling blind spots. However, there are potential drawbacks to this approach. Increased documentation requirements may impose administrative burdens on firms, especially smaller insurers, or incentivize overly conservative capital holdings that reduce market competitiveness. There is also a risk that regulatory standardization could stifle innovation in modelling methodologies or create incentives for firms to align with regulatory expectations rather than empirical realities. Nevertheless, on balance, transparent solvency model governance remains a necessary step toward ensuring the insurability of cyber risks does not rest on unexamined or outdated assumptions.

Lastly, and perhaps most controversially, is the implementation of a ban on payment of ransoms to ransomware threat actors. Policy discussions in both the United States (Logue and Shniderman, 2022) and the United Kingdom (Office, 2025) have considered the prospect of banning ransom payments to cybercriminals—a move that reshapes the role of insurers in managing ransomware risk. In particular, the UK government recently announced its intention to ban ransomware payments for public sector bodies and critical infrastructure operators (Office, 2025). While outright prohibition remains politically and logistically complex, our findings suggest that a more targeted intervention may offer a pragmatic alternative. Specifically, regulators might consider restricting cyber insurers from directly covering ransom payments, thereby shifting the burden of that decision, and its associated costs, to the affected organization's leadership.

Under such a framework, insurers would continue to support recovery through coverage for forensic investigation, business interruption, and remediation, but ransom payment itself would become a board-level decision, not an insured event. Companies would still be obligated to comply with sanctions regimes, such as those enforced by OFAC in the United States or OFSI in the United Kingdom, and this compromise preserves organizational autonomy while reducing the perverse incentives associated with risk externalization. Importantly, it also reinforces the need for insurers offering ransomware extortion payment coverage to demonstrate their own solvency, particularly if ransom payments remain part of their offerings. As ransomware continues to evolve, regulatory innovation must strike a balance between reducing harm, discouraging payment, and preserving institutional resilience, but the fundamental message is clear: insuring ransom payments without recognizing their structural risk may not just be unsustainable, it may be part of the problem.

6. Limitations and future work

As with any empirical analysis of cyber risk, this study is subject to several limitations. First, while our dataset is reflective of real-world ransomware payment events, it under-represents the full spectrum of incidents, particularly those that go unreported due to reputational, legal, or regulatory concerns. As with many studies in this space, our dataset captures only a subset of the overall landscape, and we are aware that larger institutions may have access to more comprehensive or proprietary data. Additionally, the opacity of ransomware payments continues to constrain the field's ability to make definitive claims about distributional properties across all sectors and geographies. That said, we have documented our approach and provided sufficient methodological detail to allow others to reproduce and extend this analysis on

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

alternative datasets. We view this openness as a necessary step toward improving the empirical foundations of ransomware research.

Second, while both frequency and severity are fundamental dimensions of cyber risk, this study has focused exclusively on the severity of ransom payments. A rigorous treatment of frequency dynamics would require a separate analytical framework, alongside additional assumptions to handle common data quality issues, such as right-censoring, under-reporting, and time lags in disclosure. These complexities place such an analysis beyond the scope of the present study but offer fertile ground for future research into the temporal evolution and recurrence risk of ransomware attacks. Third, in terms of statistical methodology, we note that the Anderson-Darling test used in our analysis is not inherently limited to a narrow set of heavy-tailed distributions. Other distributions could be tested through bootstrapping or Monte Carlo simulations to generate appropriate critical values. We also acknowledge that under certain conditions, central limit theorems can still apply even with non-identically distributed data as covered by the Lyapunov condition (Taleb, 2022). Additionally, the Cramer condition may hold if sub-population distributions have finite moments. However, this places the burden of proof on showing that all active ransomware threat actors produce ransom demands with finite moments, rather than across a single aggregate distribution—a demanding requirement in both theory and practice. This raises the possibility that while some threat actors' ransom demand behaviour may meet insurability thresholds, others may not, particularly those driven by non-financial or geopolitical motives.

Fourth, though our work may demonstrate significant violations of i.i.d. assumptions in ransom payments, we do not claim to have exhaustively characterized the full set of causal mechanisms driving this heterogeneity. This study focuses primarily on ransom payments as a sub-coverage within cyber insurance products, rather than on total ransomware losses. Although we emphasize the conceptual and statistical distinction between ransoms and losses, more research is needed to clarify the relationship between these two variables, especially under different regulatory and threat landscapes. Additionally, although this study has focused on variations in ransom demands as signals of threat actor (predator) behaviour, we stress the need for future research to more fully examine victim-side (prey) dynamics. Organizational revenue, sectoral regulation, geographic location, and technological preparedness may all influence both the likelihood and severity of ransomware losses. Furthermore, we also do not model the effect of ransom payment bans or other policy interventions—an important next step for evaluating the behavioural responses of both attackers and defenders under constrained insurance markets. Future work should explore more granular correlates of ransom variation, including organizational maturity, enforcement regimes, and cybersecurity hygiene investments. Exploring how these factors interact with threat actor strategies will be essential to improving pricing and solvency models, informing regulatory design, and developing a more complete understanding of the conditions under which ransomware risks may or may not be considered insurable.

Further interdisciplinary collaboration between researchers, cybersecurity threat intelligence experts, economists, insurers, and regulators will be essential for addressing the challenges identified here. In particular, there is an urgent need for the development of open, standardized datasets and transparency mechanisms that enable the robust evaluation of solvency models under adversarial risk. As ransomware continues to evolve in tactics and scope, policy and risk modelling frameworks must evolve in parallel—not only to reflect the empirical realities of the threat landscape but also to ensure that insurance remains a tool for resilience rather than a vector for systemic vulnerability.

7. Conclusion

While the use of ruin theory for solvency calculations is suitable for a single distribution risk framework, such determinations do not account for the non-i.i.d. multi-distribution of ransom payments as shown in our findings. Compounding this problem is the industry's prevailing emphasis on pricing over solvency in underwriting ransomware coverage. Actuarial pricing approaches are fundamentally ill-equipped to capture the deliberate, strategic, and intentional nature of ransomware events and ransom payments. Cyber insurance firms often prioritize competitive premium structures and market share when offering

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

ransom payment coverage, with far less scrutiny given to whether their solvency models can withstand the extreme tail risks posed by ransom demand payments and/or coordinated ransomware campaigns.

Beyond identifying this methodological shortfall, our work also highlights a pressing regulatory vacuum. The pricing-centric approach of cyber insurance firms is mirrored—and in many ways enabled—by regulatory frameworks that continue to endorse ruin theory-based solvency standards for cyber risks without examining assumptions robustly. These models, grounded in assumptions of statistical independence and loss regularity, offer little resilience in the face of systemic cyber threats that violate such premises. At present, insurance regulators lack coherent solvency standards tailored to the realities of ransomware or even general cyber risk. This absence permits cyber insurance firms to underestimate their exposure, compromising not only firm-level stability but also the broader economic resilience of the insurance ecosystem. As a corrective, our work calls for the establishment of minimum solvency requirements for cyber insurance firms and a regular re-examination of the assumptions underpinning the insuring of cyber risks.

Cyber risks also include the potential for criminal enterprises or nation-state adversaries to intentionally induce simultaneous, overwhelming attritional losses via coordinated ransomware attacks, in a strategic bid to severely disrupt or destroy the cyber insurance industry. Extortion is an intentional act, and it is erroneous to assume that all the threat actors are solely financially motivated. Insurance regulators should factor not just catastrophic cybersecurity incidents but also intentionally designed market failures into any solvency metrics and requirements.[2] Ransomware represents a paradigm shift in cyber risk—one that breaks the assumptions of traditional actuarial logic. Without urgent regulatory reform and a rethinking of risk modelling frameworks, the cyber insurance industry may find itself structurally unprepared for the threats it purports to underwrite.

Supplementary material. The supplementary material for this article can be found at http://doi.org/10.1017/dap.2025.10040.

Data availability statement. The data that support the findings of this study are available on request from the corresponding author, D.R. The data are not publicly available due to the sensitive nature of the data.

Author contribution. Conceptualization: E.L.; Data curation: E.L.; Formal analysis: D.R., E.L.; Investigation: D.R., E.L.; Methodology: D.R., E.L.; Resources: D.R., E.L.; Software: D.R., E.L.; Validation: D.R., E.L.; Visualization: D.R., E.L.; Writing - original draft: D.R., E.L.; Writing - review & editing: D.R.

Funding statement. The authors would like to thank the DNS Federation for their financial support of this project while author D.R. was previously at American University in Washington, DC. Author E.L.'s work was supported by a grant from the Lighthill Risk Network, which also supports the economic portfolio modelling of ransomware at Oasis Loss Modelling Framework. Author E.L. would also like to thank the members of the MSR-SIG at FIRST.org for their continued pressure on the ransomware ecosystem.

Competing interests. The authors report no competing interests.

Ethical standard. The research meets all ethical guidelines, including adherence to the legal requirements of the study countries.

References

Actuarial Standards Board (1997) Actuarial Standard of Practice No. 30: Treatment of Profit and Contingency Provisions and the Cost of Capital in Property/Casualty Insurance Ratemaking. Available at: https://www.actuarialstandardsboard.org/asops/treatment-profit-contingency-provisions-cost-capital-propertycasualty-insurance-ratemaking/.

Akbanov M, **Vassilakis VG and Logothetis MD** (2019) Wannacry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. *Journal of Telecommunications and Information Technology 75*(1), 113–124.

Andersen ES (1957) On the collective theory of risk in case of contagion between claims. *Bulletin of the Institute of Mathematics and its Applications 12*(2), 275–279.

[2] For example, such stress test scenarios to determine solvency standards should shift from Lloyd's of London might look less like "asbestos" (see https://www.theactuary.com/features/2015/03/2015/02/27/critical-developments-lloyds-early-1990s) and more like "attacking the peg" (see https://www.investopedia.com/terms/b/black-wednesday.asp).

Anderson RJ (2001) *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. John Wiley & Sons, Inc., USA.

Anderson TW and Darling DA (1952) Asymptotic theory of certain "goodness-of-fit" criteria based on stochastic processes. *Annals of Mathematical Statistics 23*, 193–212.

AON (2023) U.S. cyber insurance profits and performance. *U.S. Cyber Market Update* (2024, August). Available at: https://www.aon.com/getmedia/4afa8654-6534-48c3-91c1-b27d57170cdb/20240806-US-Cyber-Market-Update.pdf.

August T, **Dao D and Niculescu MF** (2022) Economics of Ransomware: Risk Interdependence and Large-Scale Attacks. *Management Science 68*(12), 8979–9002.

Awiszus K, **Knispel T**, **Penner I**, **Svindland G**, **Voß A and Weber S** (2023) Modeling and Pricing Cyber Insurance. *European Actuarial Journal 13*, 1–53.

Axon L, **Erola A**, **Agrafiotis I**, **Uuganbayar G**, **Goldsmith M and Creese S** (2023) Ransomware as a predator: Modelling the systemic risk to prey. *Digital Threats: Research and Practice 4*(4), 1–38.

Baker K (2023, January 30) Ransomware as a service (RAAS) explained how it works & examples. *CrowdStrike*. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/?srsltid=AfmBOoqvBeVM3Ecqkec2vZLDKew1aCCjyH9j9LMi0ZAs2N2-iHyNGAPu.

Banuri S and Eckel C (2012) *Chapter 3 Experiments in Culture and Corruption: A Review*. In *New Advances in Experimental Research on Corruption*. Emerald Group Publishing Limited.

BBC (2017, December 19) Cyber-attack: U.S. and U.K. blame North Korea for WannaCry. *BBC*. Available at: https://www.bbc.com/news/world-us-canada-42407488.

Beck S, **Blath J and Scheutzow M** (2015) A new class of large claim size distributions: Definition, properties, and ruin theory. *Bernoulli 21*(4), 2457–2483.

Bendiek A and Schulze M (2021) *Attribution: A major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW.* Technical Report. SWP Research Paper.

Biener C, **Eling M and Wirfs JH** (2015) Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice 40*, 131–158.

Bilton R (2025, July 21) Weak password allowed hackers to sink a 158-year-old company. *BBC*. Available at: https://www.bbc.com/news/articles/cx2gx28815wo.

Blanchet J and Murthy K (2019) Quantifying distributional model risk via optimal transport. *Mathematics of Operations Research 44*(2), 565–600.

Böhme R and Kataria G (2006) Models and measures for correlation in cyber-insurance. *WEIS 2*, 3.

Bryson MC (1974) Heavy-tailed distributions: Properties and tests. *Technometrics 16*(1), 61–68.

Cable J (2024) Ransomwhere: A Crowdsourced Ransomware Payment Dataset (1.1.0) [Data set]. *Zenodo*. Available at: https://doi.org/10.5281/zenodo.6512122.

Cable J, **Gray IW and McCoy D** (2024) Showing the receipts: Understanding the modern ransomware ecosystem. *ArXiv abs/2408.15420.*

Caporusso N, **Chea S and Abukhaled R** (2019) *A Game-Theoretical Model of Ransomware*. In *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, Advances in Intelligent Systems and Computing 782*. Springer, pp. 69–78.

Cartwright A, **Cartwright E**, **MacColl J**, **Mott G**, **Turner S**, **Sullivan J and Nurse JR** (2023) How cyber insurance influences the ransomware payment decision: Theory and evidence. *The Geneva Papers on Risk and Insurance-Issues and Practice 48*(2), 300–331.

Centre for Cybersecurity Belgium (2024) Research Report: Uncovering Patterns between GDP size and ransomware gang's choice of targets. Available at: https://ccb.belgium.be/sites/default/files/RansomwareResearchReport_GDP%26targeting_2024-02-01.pdf.

Chainalysis (2023, March 1) How the dutch national police tricked prolific ransomware strain deadbolt into giving up victim decryption keys. *Chainalysis Blog*. Available at: https://www.chainalysis.com/blog/deadbolt-ransomware-strain-tricked-into-giving-up-decryption-keys/.

Chainalysis (2024, February 7). Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 decline. *Chainalysis Blog*. Available at: https://www.chainalysis.com/blog/ransomware-2024/.

Cimpanu C (2019, August 2) Germanwiper ransomware hits Germany hard, destroys files, asks for ransom. *ZDNET*. Available at: https://www.zdnet.com/article/germanwiper-ransomware-hits-germany-hard-destroys-files-asks-for-ransom/.

Cimpanu C (2021, January 7) Ryuk gang estimated to have made more than $150 million from ransomware attacks. *ZDNET*. Available at: https://www.zdnet.com/article/ryuk-gang-estimated-to-have-made-more-than-150-million-from-ransomware-attacks/.

CISA (2020, November 2). *Ransomware Activity Targeting the Healthcare and Public Health Sector*. Cybersecurity Advisory. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a.

CISA (2021, August 4) Assessment of the cyber insurance market. *Economic Analysis*. Available at: https://www.cisa.gov/sites/default/files/publications/20_0210_cisa_oce_cyber_insurance_market_assessment.pdf.

CISA (2023, February 9) Stopransomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities. Cybersecurity Advisory. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a.

Constantinescu C and Thomann E (2005) Analysis of the ruin probabilty using Laplace transforms and karamata tauberian theorem. In *ARCH 2005.1 Proceedings 39th Actuarial Research Conference, Iowa City, Iowa.*

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

Conti M, **Gangwal A and Ruj S** (2018) On the economic significance of ransomware campaigns: A bitcoin transactions perspective. *Computers and Security 79*, 162–189.

Cramér H (1928) On the composition of elementary errors. *Scandinavian Actuarial Journal 1*(1928), 13–74.

Dacorogna M, **Debbabi N and Kratz M** (2023) Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. *European Journal of Operational Research 311*(2), 708–729.

DATAtab (n.d.) Kruskal-Wallis-Test. Available at: https://numiqo.com/tutorial/kruskal-wallis-test.

Dickson DCM (2005) *Classical ruin theory.* In *International Series on Actuarial Science*. Cambridge University Press, pp. 125–156.

Ding J, **Zhang Z and Chen X** (2019) A delayed predator-prey model for worm propagation in computer systems. *IEEE 16th International Conference on Networking, Sensing and Control (ICNSC'19)*, 41–45.

DOJ (2018, September 6). *North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. Technical Report, U.S. Department of Justice. Available at: https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

Dufresne F and Gerber HU (1989) Three methods to calculate the probability of ruin. *Astin Bulletin 19*(1), 71–90.

Dulaunoy A, **FafnerKeyZee U and Harper T** (2024, October) *Ransomlook.* Available at: https://www.ransomlook.io/ (accessed 15th May 2025).

Durbin J and Watson GS (1971) Testing for serial correlation in least squares regression.III. *Biometrika 58*, 1–19.

Edwards B, **Hofmeyr S and Forrest S** (2016) Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity 2*(1), 3–14.

Egloff F (2017) Cybersecurity and the age of privateering. In *Perkovich/Levite (Hg.): Understanding Cyber Conflict. Fourteen Analogies*. Washington, DC, pp. 231–247.

Egloff FJ and Egloff FJ (2022) *Semi-State Actors in Cybersecurity*. Oxford University Press.

Eling M and Loperfido N (2017) Data breaches: Goodness of fit, pricing, and risk measurement. *Insurance: Mathematics and Economics 75*, 126–136.

Eling M and Schnell W (2019) Capital requirements for cyber risk and cyber risk insurance: An analysis of solvency II, the U.S. risk-based capital standards, and the Swiss solvency test. *North American Actuarial Journal 24*, 370–392.

Eling M and Wirfs JH (2016) *Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class*. Technical Report. Institute of Insurance Economics.

Eling M, **McShane M and Nguyen T** (2021) Cyber risk management: History and future research directions. *Risk Management and Insurance Review 24*, 93–125.

Ellzey M (2022, September 10) The neverending story of Deadbolt. Censys. Available at: https://censys.io/the-neverending-story-of-deadbolt/ (accessed 15th May 2025).

Everett C (2016) Ransomware: To pay or not to pay? *Computer Fraud & Security 4*, 8–12.

FBI (2024, December 3) *Internet crime report 2024.* Technnical Report, Internet Crime Complaint Center (IC3). Available at: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

Ferguson J, **Kaminsky D**, **Larsen J**, **Miras L and Pearce W** (2008) *Reverse Engineering Code with IDA Pro*, 1st edition. Syngress Publishing Inc.; Elsevier, Inc.

Florêncio DAF and Herley C (2011) Sex, lies and cyber-crime survey. *Workshop on the Economics of Information Security.*

Ford R, **Bush M and Bulatov A** (2006) Predation and the cost of replication: New approaches to malware prevention? *Computers & Security 25*, 257–264.

Fortune Business Insights (2025) *Cyber insurance market: Market research report (report id: Fbi106287).* Available at: https://www.fortunebusinessinsights.com/cyber-insurance-market-106287 (accessed 15th May 2025).

Furnell S (2008) It's a jungle out there: Predators, prey and protection in the online wilderness. *Computer Fraud & Security 2008*(10), 3–6.

Geer D, **Jardine E and Leverett E** (2020) On market concentration and cybersecurity risk. *Journal of Cyber Policy 5*(1), 9–29.

Gerber HU (1988) Mathematical fun with ruin theory. *Insurance: Mathematics and Economics 7*(1), 15–23.

Gibbs S (2017, August 3) Wannacry: Hackers withdraw £108,000 of bitcoin ransom. *The Guardian*. Available at: https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom.

Gill J and Bao L (2024) *Bayesian social science statistics: From the very beginning*. In *Elements in Quantitative and Computational Methods for the Social Sciences*. Cambridge University Press.

Goodin D (2017) Nsa-leaking shadow brokers just dumped its most damaging release yet. *Ars Technica*. Available at: https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/.

Gorman SP, **Kulkarni RG and Schintler LA** (2004) A predator prey approach to the network structure of cyberspace. *ACM Winter International Symposium on Information and Communication Technologies (WISICT)*, 1–6.

Gray IW, **Cable J**, **Brown B**, **Cuiujuclu V and McCoy D** (2023) Money over morals: A business analysis of conti ransomware. *Cryptography and Security.* Available at: arXiv:2304.1168.

Hernandez-Castro J, **Cartwright A and Cartwright E** (2020) An economic analysis of ransomware and its welfare consequences. *Royal Society Open Science*, 7190023190023.

Home Office (2025) *Ransomware Legislative Proposals: Reducing Payments to Cyber Criminals and Increasing Incident Reporting-Government Response*. Technical Report, U.K. Government. Available at: https://assets.publishing.service.gov.uk/media/687faaaafdc190fb6b8468db/Government_Response_Ransomware_proposals_to_increase_incident_reporting_and_reduce_payments_to_criminals.pdf.

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

Home Office (2025) *Ransomware Legislative Proposals: Reducing Payments to Cyber Criminals and Increasing Incident Reporting*. Technical Report, U.K. Government. Available at: https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible.

Horsley EF (2018) State-sponsored ransomware through the lens of maritime piracy. *Georgia Journal of International and Comparative Law 47*, 669.

Hult H and Lindskog F (2011) Ruin probabilities under general investments and heavy-tailed claims. *Finance and Stochastics 15*, 243–265.

Jung K (2021) Extreme data breach losses: An alternative approach to estimating probable maximum loss for data breach risk. *North American Actuarial Journal 25*(4), 580–603.

Klüppelberg C, **Straub D and Welpe IM** (2014) *Risk-A Multidisciplinary Introduction*. Springer.

Kolesnikov O, **Markov A**, **Smagulov D and Solovjovs S** (2022) Cyber Loss Distribution Fitting: A General Framework towards Cyber Bonds and Their Pricing Models. *International Journal of Mathematics and Mathematical Sciences 7689828*, 1–20.

Kowalski CJ (1972) On the effects of non-normality on the distribution of the sample product-moment correlation coefficient. *Journal of the Royal Statistical Society: Series C (Applied Statistics) 21*(1), 1–12.

Kropotov V, **Matsukawa B**, **McArdle R**, **Yarochkin F**, **Matsugaya S**, **Burns E, and Leverett E** (2023) What decision-makers need to know about ransomware risk: Data science applied to ransomware ecosystem analysis. *Trend Micro*. Available at: https://documents.trendmicro.com/assets/white_papers/wp-what-decision-makers-need-to-know-about-ransomware-risk.pdf.

Kruskal WH and Wallis WA (1952) Use of ranks in one-criterion variance analysis. *Journal of the American Statistical Association 47*(260), 583–621.

Kumar M, **Mishra B and Panda T** (2016) Predator-prey models on interaction between computer worms, trojan horse and antivirus software inside a computer system. *International Journal of Security and Its Applications 10*(1), 173–190.

Laszka A, **Farhang S and Grossklags J** (2017) *On the economics of ransomware*. In *Decision and Game Theory for Security: 8th International Conference, GameSec 2017, Vienna, Austria, October 23–25, 2017, Proceedings.* Springer, pp. 397–417.

Lee F (2023) Cyber insurance rate hikes slow – but exclusions expand. Financial Times Professional. Available at: https://professional.ft.com/en-gb/blog/cyber-insurance-rate-hikes-slow-but-exclusions-expand/.

Leverett E, **Jardine E**, **Burns E**, **Gangwal A and Geer D** (2020) Averages don't characterise the heavy tails of ransoms. In *2020 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–12, Available at: https://doi.org/10.1109/eCrime51433.2020.9493256.

Liao K, **Zhao Z**, **Doupé A and Ahn G-J** (2016) Behind closed doors: Measurement and analysis of cryptolocker ransoms in bitcoin. In *2016 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–13, Available at: https://doi.org/10.1109/ECRIME.2016.7487938.

Lloyd's Market Association (2025) Cyber war clauses. Available at: https://lmalloyds.com/specialist-areas/underwriting/wordings/cyber-war-clauses/?WebsiteKey=6b59f78b-a7b1-4030-bd9a-63b40fe39ac4.

Ljung GM and Box GEP (1978) On a measure of a lack of fit in time series models. *Biometrika 65*, 297–303.

Logue K and Shniderman A (2022) The case for banning (and mandating) ransomware insurance. *Connecticut Insurance Law Journal 28*(1), 247–316.

Lotka AJ (1925) *Elements of Physiological Biology.* Dover Publications.

Lundberg F (1903) *Approximations of the Probability Function/Reinsurance of Collective Risks*. PhD dissertation, University of Uppsala.

Maillart T and Sornette D (2010) Heavy-tailed distribution of cyber-risks. *The European Physical Journal*, 357–364.

Marotta A, **Martinelli F**, **Nanni S**, **Orlando A and Yautsiukhin A** (2017) Cyber-insurance survey. *Computer Science Review 24*, 35–61.

Massey Jr. F. J. (1951) The Kolmogorov-Smirnov test for goodness of fit. *Journal of the American Statistical Association 46*(253), 68–78.

Mildenhall S and Major J (2022) *Pricing insurance Risk: Theory and Practice*. Wiley, pp. 5.

Muncaster P (2022) Deadbolt ransomware extorts vendors and customers. *Infosecurity Magazine*. Available at: https://www.infosecurity-magazine.com/news/deadbolt-ransomware-extorts/.

Nershi K and Grossman S (2023) Assessing the Political Motivations Behind Ransomware Attacks. Available at *SSRN*: http://doi.org/10.2139/ssrn.4507111.

Nye J (2010) *Cyber Power*. Technical Report, Belfer Center for Science and International Affairs, Harvard Kennedy School.

Parodi P (2023) *Pricing in General Insurance*. Chapman and Hall/CRC.

Patriarca M, **Heinsalu E**, **Marzola L**, **Chakraborti A and Kaski K** (2016) *Power-laws as statistical mixtures*. In *Proceedings of ECCS 2014*. Springer, pp. 271–282.

Pentikäinen T (1967) On the solvency of insurance companies. *Astin Bulletin 4*(3), 236–247.

Ridinger G (2018) Cultural Transmission and Extortion. *Games 9*(3), 49–59.

Rodríguez E, **Noroozian A**, **van Eeten M and Gañán C** (2021) Superspreaders: Quantifying the role of iot manufacturers in device infections. *Workshop on the Economics of Information Security (WEIS)*.

Romanosky S (2016) Examining the costs and causes of cyber incidents. *Journal of Cybersecurity 2*(2), 121–135.

Romanosky S and Petrun Sayers EL (2023) Enterprise risk management: How do firms integrate cyber risk? *Management Research Review 47*(1), 1–17.

https://doi.org/10.1017/dap.2025.10040 Published online by Cambridge University Press

Romanosky S, **Ablon L**, **Kuehn A and Jones T** (2019) Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity 5*(1), tyz002.

Rose-Ackerman S and Palifka BJ (2016) *Culture and Corruption*, 2nd Edn. Cambridge University Press, pp. 233–272.

RosettaCode. (n.d.) *How to Calidate a BTC Address.* Available at: https://rosettacode.org/wiki/Bitcoin/address_validation#:~:text=To%20check%20the%20bitcoin%20address,digest%20library%20for%20SHA%2D256.

Santini P, **Gottardi G**, **Baldi M and Chiaraluce F** (2019) A data-driven approach to cyber risk assessment. *Security and Communication Networks 2019*, 1–8.

SouthPoint Risk (n.d.) *Insurance Claims in the Last Five Years.* https://www.southpointrisk.com/blog/ransomware-largest-driver-of-cyber-insurance-claims-in-the-last-five-years/ (accessed 15th May 2025).

Shetty S, **McShane M**, **Zhang L**, **Kesan JP**, **Kamhoua CA**, **Kwiat K and Njilla LL** (2018) Reducing informational disadvantages to improve cyber risk management. *The Geneva Papers on Risk and Insurance-Issues and Practice 43*, 224–238.

Shevchenko PV, **Jang J**, **Malavasi M**, **Peters G**, **Sofronov G and Trueck S** (2023) The nature of losses from cyber-related events: Risk categories and business sectors. *Journal of Cybersecurity 9*, tyac016.

Sibbertsen P, **Stahl G and Luedtke C** (2008) *Measuring Model Risk.* Technical Report, Diskussionsbeitrag.

Spearman C (1904) The proof and measurement of association between two things. *The American Journal of Psychology 15*(1), 72–101.

Dumortier F, **Papakonstantinou V and De Hert P** (2020) EU sanctions against cyber-attacks and defense rights: Wanna Cry? *European Law Blog*. Available at: https://researchportal.vub.be/en/publications/eu-sanctions-against-cyber-attacks-and-defense-rights-wanna-cry/.

Taleb NN (2022) *Statistical Consequences of Fat Tails: Real World Preasymptotics, Epistemology, and Applications.* STEM Academic Press.

Trend Micro (2024) What is Ryuk ransomware? *Trend Micro.* Available at: https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html.

Thorin O (1974) Some comments on the sparre andersen model in the risk theory. *Astin Bulletin 8*(1), 104–125.

Turner AB, **Ikram M and Uhlmann AJ** (2025) Classifying Ransomware-Bitcoin Nodes using Graph Embeddings. *Pacific Asia Journal of the Association for Information Systems 17*(1), 4.

Ud Din S, **Masood Z**, **Samar R**, **Majeed K and Raja MAZ** (2017) Study of epidemiological based dynamic model of computer viruses for sustainable safeguard against threat propagations. *IEEE 14th International Bhurban Conference on Applied Sciences and Technology IBCAST 17*, 434–440.

Verizon (2024*) Data breach investigations report*. Technical Report. Verizon. Available at: https://www.verizon.com/business/resources/Td83/reports/2024-dbir-data-breach-investigations-report.pdf.

Volterra V (1926) Fluctuations in the abundance of a species considered mathematically. *Nature 118*, 558–560.

Waldman A (2024) Coalition: Ransomware severity up 68. *TechTarget.* Available at: https://www.techtarget.com/searchsecurity/news/366613275/Coalition-Ransomware-severity-up-68-in-first-half-of-2024.

Wang K, **Pang J**, **Chen D**, **Zhao Y**, **Huang D**, **Chen C and Han W** (2021) A large-scale empirical analysis of ransomware activities in bitcoin. *ACM Transactions on the Web 16*, 2.

Webb GI, **Hyde R**, **Cao H**, **Nguyen HL and Petitjean F** (2016) Characterizing concept drift. *Data Mining and Knowledge Discovery 47*(4), 964–994.

Whyte C (2015) Power and predation in cyberspace. *Strategic Studies Quarterly 9*, 100–118.

Wolff J (2022) *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*. The MIT Press.

Woods DW and Moore T (2020) Does insurance have a future in governing cybersecurity? *IEEE Security & Privacy 18*(1), 21–27.

Woods DW, **Agrafiotis I**, **Nurse JRC and Creese S** (2017) Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications 8*(1), 8.

Woods DW, **Böhme R**, **Wolff J and Schwarcz D** (2023) *Lessons lost: Incident response in the age of cyber insurance and breach attorneys*. In *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim: USENIX Association, pp. 2259–2273.

World Economic Forum (2022) *Systemic Cybersecurity Risk and Role of the Global Community: Managing the Unmanageable*. Technical Report. Available at: https://www3.weforum.org/docs/WEF_GFC_Cybersecurity_2022.pdf.

Wüthrich MV and Merz M (2013) *Financial Modeling, Actuarial Valuation and Solvency in Insurance*. Berlin/Heidelberg: Springer.

Xu M, **Schweitzer KM**, **Bateman RM and Xu S** (2018) Modeling and predicting cyber hacking breaches. *IEEE Transactions on Information Forensics and Security 13*(11), 2856–2871.

Yang K (2017) Wannacry: Evolving history from beta to 2.0. *Fortinet*. Available at: https://www.fortinet.com/blog/threat-research/wannacry-evolving-history-from-beta-to-2-0.

Zeller G and Scherer M (2022) A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal 12*, 33–85.

Cite this article: Ramjee D and Leverett E (2025). From ransoms to ruin: Are extortion payments by ransomware victims insurable? *Data & Policy*, 7: e80. doi:10.1017/dap.2025.10040