ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Ransomware: Why It's Growing and How to Curb Its Growth

Joshua Jaffe | Oxford Internet Institute, Oxford University, UK |
ORCID: 0000-0001-8238-4949

Luciano Floridi | Digital Ethics Center, Yale University, USA |
ORCID: 0000-0002-5444-2280

Received: 11.06.2024

Accepted: 07.08.2024

Published: 09.11.2024

Cite this article as:
J. Jaffe, L. Floridi "Ransomware: Why it's growing and how to curb its growth," ACIG, vol. 3, no. 2, 2024, pp. 72–98. DOI: 10.60097/ACIG/192959

Corresponding author:
Joshua Jaffe, Oxford Internet Institute, Oxford University, UK; E-mail: joshua.jaffe@mansfield.ox.ac.uk
0000-0001-8238-4949

Copyright:
Some rights reserved (CC-BY):
Joshua Jaffe
Luciano Floridi
Publisher NASK

Abstract

Ransomware is an increasingly pernicious threat to individuals, businesses, economies, and societies. Ransomware attacks simplify the typical cybercrime value chain. Given the exponential growth of data, the wide distribution of connected devices, the so-called internet of things, and the power of artificial intelligence to exponentially scale attacks, ransomware is likely to continue to grow. Much research and analysis has focused on ransomware tool kits, malware samples, and the vulnerable victim landscape. However, this is only part of the picture. At its core, ransomware is a crime committed almost entirely for economic benefit. Yet, research on behavioural factors and market forces that incentivise the proliferation of ransomware is limited. The majority of what does exist comes in the form of media reporting and industry periodicals. Given their relevance, these sources should not be discounted out of hand. Yet, how critically should their findings be viewed and inherent conflicts within their findings be resolved? Further, as the profit motive of ransomware is similar to other economic crimes, how relevant is the vast body of research on criminality or on behavioural economics to understanding the growth of ransomware? In this article, we review the literature relevant to understanding the growth of ransomware by widening the lens to include a range of relevant multi-disciplinary academic sources as well as industry data. We then discuss our conclusions regarding

OPEN ACCESS

CC BY

the forces compelling its growth and identify areas requiring further study that could reverse the trend.

Keywords

Ransomware, cybercrime, cyber warfare, extortion, malware

1. Introduction

The ransomware trend in cybercrime is growing. Online virus database VirusTotal has received uploads of more than 80 million ransomware samples since 2020 [1]. According to global telecommunications company Verizon, the frequency of ransomware attacks doubled in 2021 [2]. In its survey from the same year, the International Data Corporation (IDC) found that 37% of companies reported having been the victim of ransomware, the highest percentage in the survey's history [3]. The Federal Bureau of Investigation reports that ransomware-related complaints have risen 62% year-on-year in the United States [4]. The World Economic Forum considers cybercrime the most significant threat to businesses in the United States, Canada, and Europe [5]. In 2020, Farahbod et al. estimated the cost of cybercrime on the global economy at 'up to $1 trillion' [6]. Editor-in-chief of *Cybercrime Magazine* Steve Morgan went further, estimating the overall cost of cybercrime would exceed $10 trillion by the end of 2025. He also noted that ransomware is increasingly becoming the go-to choice for cybercriminals [7].

Most of the data about the cost of cybercrime and the growth of ransomware come from industry sources. Though the above statistics are staggering in their claims, it should be noted from the outset that the methodology for calculating the cost of cybercrime, or a particular variety like ransomware, varies considerably by author. Further, many of these industry sources have a vested interest in certain perceptions of ransomware crime, so – while they fill a gap in the literature – their findings should be subject to skepticism. Anderson and coauthors address some of these challenges in their 2019 reprisal of their 2012 paper, noting that, in addition to challenges with availability of data, there is also a methodological issue as well [8]. They note some authors include only the direct losses to hackers, others consider the indirect societal costs and the invisible tax passed along to consumers in the form of growing cybersecurity budgets that inevitably find their way to the cost of goods sold [8].

Regardless, without attempting resolve the precise societal cost of ransomware, the growth of this crime observed by all the above

sources suggests that ransomware has become endemic, and this has far-reaching implications for individuals, corporations, societies, and economies. Despite the alarming increase in ransomware, the underlying social and ethical forces involved remain understudied. Most analyses focus on *what* and *when* questions. They enumerate the details of isolated attacks and adopt a technical approach to analysing specific malware tool kits and individual criminal actors. This kind of research is necessary but insufficient because it grants only a partial understanding of the growing ransomware phenomenon. It is inadequate for drawing societal conclusions to address the problem because it does not consider the actors' *motivations* and *values*.

Conventional approaches limit our capability to circumscribe and minimise ransomware attacks because they provide an incomplete understanding of the scope and scale of the problem. This is inconsistent with how we usually address other social and criminal ills. Typically, policymakers focus on *who, why*, and *how* questions. For example, law enforcement does not develop strategies for combating violent crime by evaluating individual shootings and context-specific forensic evidence from an individual event. Public safety officials do not write building codes based on a detailed study of an individual residential fire. Nor do national security officials develop strategy solely based on an individual adversary's infantry forces. Stated this way, common sense, and general familiarity with each broad category of policy, make the above examples unsuitable for drawing macro conclusions about combatting violent crime, improving residential building standards, or securing a national defence. Each of these domains is composed of a mosaic of factors, and the relevant actors have a complex range of motivations. Effective policing strategy considers the motivations of criminal actors and the forensic specifics of individual crimes. Fire prevention requires the thoughtful selection of materials, construction in accordance with building code requirements, and responsible behaviour on the part of individuals. Defence policy does not rely solely on analyses of an adversary's military capabilities but also on national interests and the character of their respective leaders. As a result, in this review, we widen the aperture and consider a range of literature relevant to better understanding the motivations of ransomware actors as well as the scale of ransomware crime.

1.1. Scope of Analysis

Individuals, governments, and societies solve systemic problems by understanding and addressing all the relevant factors

that drive behaviour. Also visible against the backdrop of these examples is the fact that the success of the policy is not dependent on criminal code and legal redress alone. They also depend on a degree of convergence between the norms and values within a society and the problem in question. For example, most individuals in a society do not merely avoid criminal behaviour because it has been defined as illegal but also because social pressures are applied which cause a criminal record to carry a social penalty. Construction companies don't comply with civil building codes simply because they are legally required to but also because there are commercial penalties associated with a poor safety reputation. And, a strong national defence is not merely the product of defensive arms but also strong alliances, social cohesion, and economic resilience. When all works well, this can align individual motivations with desirable ends, such as social progress and the collective good.

This article is intended to provide the grounds for future analyses of how the growth of ransomware might be curtailed through socio-economic interventions. In doing so, we aim to (1) provide a systematic overview of the problem, (2) assess the state of the current debate, and (3) suggest underexplored areas of both practical and theoretical interest for tackling the ransomware problem. We focus on governance, ethical, legal, and social implications (GELSI). We also engage with well-studied cases from the social sciences relevant to our topic (e.g. issues around paying conventional ransoms to kidnappers).

In our analysis, we focus on (1) single ransomware, which refers to the encryption of data and then the holding of the decryption keys for ransom, and (2) double ransomware, which is like single ransomware but with the addition of extortion involving the public disclosure of stolen data to compel ransom payments [9]. These two types of ransomware account for most of its growth. They also share a common motivation: compelling a data owner or custodian to act against their interests through extortion. We do not discuss purely destructive cyberattacks, nor do we discuss so-called false-flag ransomware, which disguise attacks intended to be purely destructive as ransomware attacks [10]. We make this distinction because we consider destructive cyberattacks and false-flag ransomware to be different kinds of phenomena because the motivations of the actors are different.

1.2. Methodology

Motivated by an interest in understanding the forces driving ransomware's growth, we conducted a *state of the art review* of

the literature relevant to the social and behavioural analysis of ransomware crimes [11]. We structured our review of the relevant literature by focusing on articles that can help answer the *who, why,* and *how* questions. We reviewed more than 100 sources and ultimately selected 50 for inclusion on the basis of their novelty and relevance to answering these questions. We relied on academic journal articles that describe the origin and nature of ransomware crimes committed over the course of the past four decades. However, this review also subjects a wide range of industry research and statistics on ransomware to critical review. While we did ultimately include some industry estimates of the scope and scale of ransomware we considered most credible, we focused primarily on those sources able to help characterise the behaviour of cybercriminals and answer the *who, why,* and *how* questions noted above.

Given that ransomware has many similarities with conventional economically motivated crimes, this review also considers literature in the fields of Criminology and Economics that we believe adds to the collective understanding of ransomware's growth. We conducted further analysis, applying conventional techniques used in these disciplines to reach indirect conclusions about these ransomware questions, where no direct contextual data relevant to a specific aspect of the ransomware problem was uncovered through our research. Finally, we also interviewed some experts, including their insights into our findings (see Figure 1).

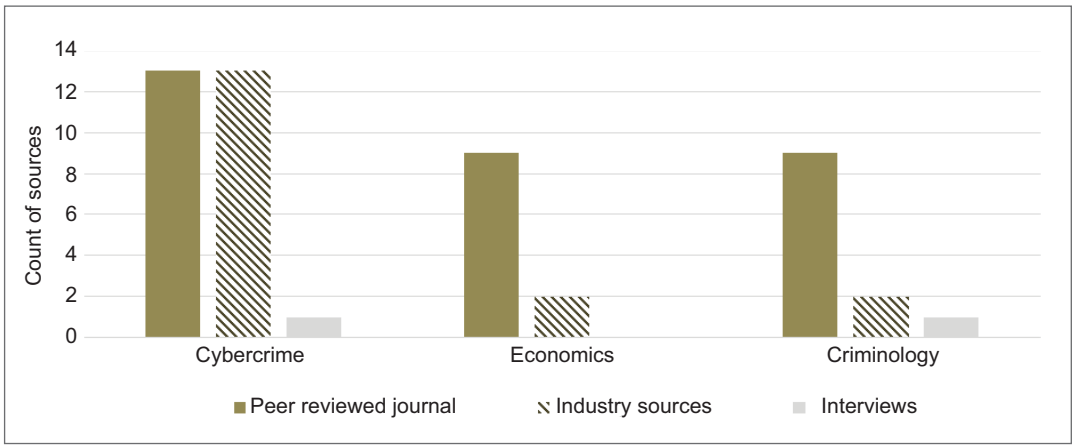

Figure 1. Included sources by field of study.

1.3. Structure and Framing of Analysis

Our findings organise the literature on the social forces involved in the rise of ransomware into five sections. Following the

introduction found in Section 1, we proceed to Section 2, where we describe the *what* and *when* questions about ransomware. This establishes the foundational claim that ransomware is an endemic problem. In Section 3, we address the *who* question by reviewing the research on ransomware actors and the origin of attacks. This supports the claim that actor-analyses are mostly descriptive and lack an understanding of motivating factors. In Section 4, we focus on the *why* question. We consider the literature on the illicit marketplace for ransomware, the exchange of value in the marketplace, and how this drives actor behaviour. In Section 5, we discuss the *how* question. We evaluate the effects of various practices on the ransomware problem and the adverse selection bias involved. In Section 6, we conclude our analysis and consider some areas for further study.

2. What and When: A Brief Summary of the Evolution of Ransomware Tactics

The increase in ransomware attacks may have surprised many in government and industry, but the core reason for such growth is not a mystery. Ransomware attacks simplify the typical cybercrime value chain, where reduction in complexity drives growth. In this section, we discuss how ransomware has been employed as an attack method to extract value over the past two decades.

Ransomware attacks were common but not epidemic until 2013. Since 2013, they have grown by more than 500% [12]. Ransomware evolved in the late 1990s from simple user interface (UI)-lockers to disk-encrypting cryptographic ransomware. More recently, they have advanced to include file-exporting tool kits that encrypt users' data and enable data theft [13]. For over a decade, most attacks opportunistically targeted individuals, typically with random mass-mail Spam or indiscriminate drive-by downloads.[1] Over this period, almost all attacks originated in Russia, and targets were mostly in Russia or countries on the Russian periphery [14].

The number of ransomware malware samples doubled each quarter in 2011, mainly owing to the development of commercialised ransomware tool kits and anonymous payment systems [14]. This sharp growth continued as the illicit market for ransomware tool kits, know-how, and payment mechanisms expanded. Ransomware attacks exploded in 2016 when there was a tactical shift towards targeting large corporations with so-called wormable ransomware (ransomware that can burrow through a computer network without direct control from the hacker). This naturally correlated with

1——A drive-by download is a method of exploiting a victim computer that can infect a vulnerable web browser software if a user visits a compromised website.

increasingly high ransom demands. This coincided with a rise in cyber extortion over the same period of time, where not only was data held for ransom but the threat of exposing to regulators the fact that an organisation had been hacked is used to compel speedy payment [15].

Only a negligible fraction of this reported growth can be explained by improved methods for detecting ransomware attacks. The online computer virus aggregator VirusTotal counts 11.7 billion ransomware malware samples uploaded to its services since 2005 [1]. When plotted over time, the increase represents a growing wave, rather than a sudden jump. Leveraging data collected and reported by Verizon, we find that ransomware accounted for less than 1% of all reported cyberattacks in 2013 but more than 25% in 2021 (see Figure 2) [16]. The compounded annual growth rate (CAGR) for this period exceeds 50% per annum, a significant increase and one that supports the observed trends.

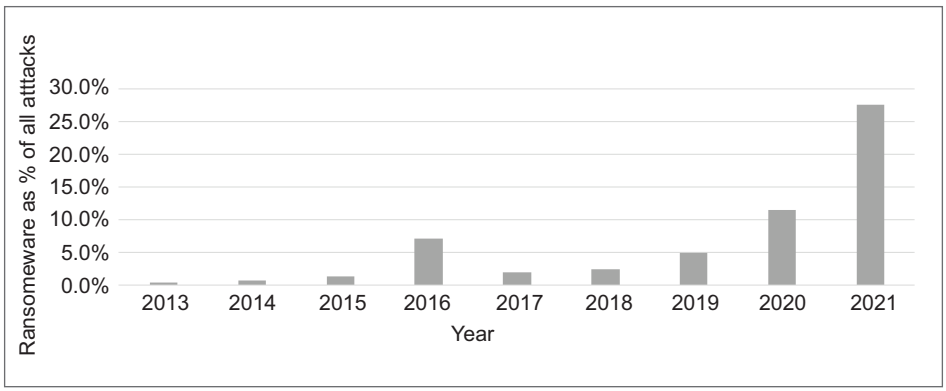

Figure 2. Ransomware as Percent of Total Reported Attacks in Verizon VERIS Data Base and DBIR Report.

That said, a closer look at the data suggests a couple of caveats. Firstly, although the general trend in reported ransomware crimes has trended up, the overall number of cybercrimes reported in VERIS has declined consistently since 2013. Part of the ransomware's annual percentage growth could be attributed to this decline in the denominator.[2] Secondly, significant regulation in this period created new reporting and remuneration obligations for corporations affected by ransomware. This likely impacted the number willing to publicly report any cyberattack, possibly resulting in gross undercounting. Although it is impossible to know for sure, we think that the decline in general cybercrimes being reported

2———At the time of these analyses, the raw total of attacks in VERIS was available only for the year 2017. The 2022 DBIR Report, which is calculated on the raw VERIS data, provided the percentage of attacks categorised as ransomware from 2017 to 2021. It is therefore possible to complete the table in Figure 1 only as a comparison of percentages.

is attributable to a shift in emphasis away from nuisance crimes towards more significant cases. Given several reporting disincentives, it seems likely that ransomware events are undercounted. We suspect that the trend in ransomware crimes is more severe than represented in Figure 2.

Regardless of which sources are consulted, ransomware is a prevalent and growing method by which cybercriminals seek to extract value. It also appears that the wave has not yet crested. In their survey of ransomware techniques, McIntosh and colleagues note that there is a consensus expectation that ransomware attacks will not only continue to grow but also shift towards more disruptive tactics that are more difficult to combat [13]. According to McIntosh et al. [13],

1. There will be a reduction in attacks on private individuals and an increase in attacks on organisations, further optimising the time-to-value ratio in favour of the attackers.
2. There will be a shift in tactics towards active exploitation of technology vulnerabilities and away from passive infiltrations (e.g. via phishing, vishing, or fraud).
3. There will be a broadening of the mechanism to deprive enterprises of access to their systems, possibly renewing the focus on distributed denial of services (DDoS) attacks instead of only file encryption.

With these forecasts as the backdrop, the proliferation of network-connected industrial internet of things (IIoT) devices upon which vital social enterprises rely raises stark concerns. Many of these have been summarised by Yaqoob et al. [17], who stress the vital functions that connected IIoT devices perform. These devices have also proven to be significantly vulnerable to ransomware attacks. At the macro level, Yaqoob et al. discuss ransomware risks to hospital centres, water treatment facilities, the electrical grid, pharmaceutical production, and nuclear reactors [17]. At the micro level, autonomous vehicles and implantable medical devices appear particularly at risk. Society is becoming increasingly dependent on technology, and connected devices play an increasingly vital role in human safety and societal well-being. It is insufficient to consider ransomware attacks within the limited view of technical exploits and countermeasures. Ransomware requires a response similar to approaches addressing other grave societal threats. Such a response, we contend, must recognise the motivations of the bad actors involved and realign their interests with those of society at large.

3. Who: On Actors, Motivations, and Public Perception

Data on cybercriminals is difficult to gather, given the shadowy and opaque nature of cybercrime. As such, cybercriminals' motivations can be challenging to assess and categorise. These issues make it difficult for the public to perceive the problem accurately. It also makes developing a framework or standard for ethical behaviour challenging. Cyberattacks also have effects beyond strictly financial ones. For example, ransomware attacks against hospitals in the United States and Europe have prolonged patients' wait times for critical care.[3] Nonetheless, public perception and ethical criticism of cybercriminals and cybercriminal activity remain mixed owing to the cyber domain's opacity. Social pressure on cyber criminals also remains only mildly influential.

3———In one case, a patient in a German hospital died while waiting for emergency treatment [5].

3.1. Public Perception of Cybercrime and Ransomware

Mulhall's survey of public perceptions of cybercriminals is dated, but it shows some interesting trends [18]. When viewed from the largely benign perspective of hacking, public perceptions tend to be mixed. Many survey respondents had a negative association with terms connected with cybercriminal behaviour. This was most closely associated with news of attacks that personally affected people. Negative associations were especially acute when attacks risked the health or lives of individuals. However, when hackers targeted nameless/faceless corporations, especially those with poor public reputations, then public opinion was less condemning (Mulhall focuses on the targeting of the US and British Telcom giants at the height of their profits).

Given the age of this survey, we should supplement it with more recent corroboration. There is evidence to suggest a parallel in current public sentiment. Pawlicka and colleagues illustrate this by citing examples of so-called hacktivism [19]. Hacktivism targets organisations that the hackers believe are perpetrating a systemic injustice. As such, most attacks do not cause general public alarm. Harford, from marketing and sales services company TechTarget, notes that, prior to 2016, ransomware attacks were mostly limited in scope and sophistication [20]. They targeted individuals, ransoming personal files, photos, and financial documents. Attackers often adopted a friendly approach, sometimes even apologising for the inconvenience and offering support to fix the problem after the ransom was paid [20]. There is not much literature on the effect of this tactic, but public outrage was generally muted. This changed in 2016 with the *Petya* and *WannaCry* attacks. These attacks leveraged

the EternalBlue exploit, which allows malware to worm through a victim's network. This new capability led to the targeting of enterprises, large-scale damage, and the extraction of much larger ransoms [4]. This and other similar tactics increased the scope of the attacks and led to wider ripples throughout the society, often affecting individuals well beyond the targeted company. Examples include the attack on the British NHS in 2017, staple food producer JBS in 2021, and the energy company Colonial Pipeline in 2021. These directly impacted consumers' convenience, health and/or financial well-being. The result was stark shift in perceptions of this kind of crime and the actors who perpetrate it [21].

Applying these findings to the modern ransomware context leads to two conclusions, both suggesting the need for further study. Firstly, public outrage was limited when wealthy corporations were targeted and where members of the public were not directly impacted (either financially or socially) [18]. Secondly, this sentiment reverses after 2015. This correlates with a shift to more risky tactics, more impactful and prominent targets, and increased public concern.

3.2. Motivations of Cybercriminals

Direct, first-person accountings of what motivates those involved in ransomware or other types of cybercrime often suffer from bias. Journalistic reporting about those engaged in this type of criminal activity is often overly influenced by a few sensational cases. They range from the comical Kindergarten Hacker [22] to the legendary Evil Corp [23]. However, a few more grounded analyses do exist, which provide some insights about motivations.

A 2016 analysis of self-described hackers from the United States, the United Kingdom, and Germany was conducted by PaloAlto Networks and the Ponemon Institute. They found that most cybercriminals fit the stereotype. Most were underemployed (the average annual income from cybercrime was slightly more than £20,000). More than two-thirds claimed that monetary gain was their sole or primary motivation. On average, they completed only two successful attacks per year. These were, however, sufficiently lucrative to make the attacks worth the investment of time and resources. The typical attack took less than 24 hours to execute and yielded an average return of between £8,600 and £10,900, depending on the country of the respondent [24].

Security periodical *CSO Online* estimates that the aggregate cost of cybercrime likely exceeded $6 trillion in 2021 [25]. Similar surveys

also provide some insights into cybercriminal motivations. However, they likely suffer from sampling error. For both the Ponemon Institute and the *CSO Online* estimates to be correct, approximately one in ten people would need to be engaged in cybercrime. This seems highly implausible. Ian Thornton-Trump [26] offers a more likely explanation. Many cybercriminals are freelancers, but most losses result from professional cybercriminals working full-time. Professional cybercriminals use much more sophisticated methods and therefore cause much more damage. Most are organised into criminal cartels [16]. They share the profit motive identified by PaloAlto Networks and the Ponemon Institute but execute their attacks more frequently and precisely [24]. Further, Gragido et al. shed some light on the big business of cybercrime. They demonstrate the approach of mature syndicates taking a structured approach to cybercrime research and development (R&D), often investing millions of dollars with the realistic prospect of achieving many millions more in return on their investments [27].

4. Why: On the Marketplace for Ransomware

Cybercrime Magazine calculated that the cost of ransomware grew from $325 million in 2015 to $5 billion in 2017 [28], an increase of more than 1500%. According to the threat research team at Verizon, ransomware attacks represented 3% of all cyberattacks in 2017 [2]. By the end of 2021, ransomware attacks accounted for 25% of all cyberattacks. The associated value lost is estimated to grow to an aggregate of $265 billion by the end of the decade [29]. This, too, likely represents a significant underestimation of the damages due to the severe disincentives to public reporting of ransomware attacks noted above.

Interestingly, the illicit trade in ransomware malware seems quite efficient despite the large volume of malicious ransomware code. Cyber actors, like conventional actors, engage in a rational evaluation of tradeoffs before choosing to commit a crime. This is consistent with application of the Rational Choice Theory, now widely applied to other conventional crimes [30]. Ransomware exhibits higher benefits and lower costs than other types of cybercrime. The macro factors driving the growth of ransomware (apart from other types of cybercrime) appear to be related to its ability to convert criminal activity into value efficiently. Historically, cybercriminals needed to go through the following nine steps: (1) discover a vulnerability in a system, (2) create malware capable of exploiting the vulnerability, (3) 'weaponised' that malware to gain access to a victim system, (4) conduct 'reconnaissance' until data considered valuable is recognised, (5) exfiltrate

those data without being blocked, (6) market the data for sale at illicit marketplaces, (7) find a prospective buyer, (8) gain the buyer's trust regarding validity and uniqueness of the data, and finally (9) conduct an exchange of value. Contrast this with ransomware, where the data can be assumed to be valuable because they are currently being used by the custodian, nothing needs to be exfiltrated, and the buyer is built into the equation from day one.

4.1. The Market Concentration of Ransomware Malware

This efficiency does not stop with the attack itself; it extends into the ransomware 'ecosystem'. Analysing the data reported by VirusTotal, it appears that the commercial hacker market operates in a near-frictionless, highly consolidated fashion, where capital is allocated to the most efficient software. Traditionally, economists use the Herfendahl–Hirschman Index (HHI) to assess market concentration. The HHI sums the square of each vendor's market share in a market segment. It does so by using the following simple formula: $HHI = s_1^2 + s_2^2 + \cdots + s_n^2$, where s denotes market share and n denotes the number of competitors in the market. When evaluating monopolistic market power in anti-trust cases, the US Department of Justice considers an HHI of more than 2500 to be highly concentrated. If we apply the HHI model to the selection of ransomware malware samples reported by VirusTotal, then we get an HHI score of 6250 (see Table 1). This

Table 1. Top ransomware families as percentage of total reported ransomware malware samples described to VirusTotal.

Top 10 malware families	% of Samples	HHI score
Gandcrab	78.5%	6162.3
Babuk	7.6%	57.9
Cerber	3.1%	9.7
Matsnu	2.6%	6.9
Wannacry	2.4%	5.8
Congur	1.5%	2.3
Locky	1.3%	1.7
Teslacrypt	1.1%	1.3
Rkor	1.1%	1.2
Reveton	0.7%	0.5
Total	**100.00%**	**6249.5**

is more than 2½ times the Department of Justice bar for highly concentrated. Of more than 60 million samples organised into 130 malware families in 2020, cybercriminals chose the *Grandcrab* malware more than 75% of the time. The top three malware families accounted for approximately 90% of all attacks; malware families 11–130 accounted for less than 1% of all attacks.

The frequency with which cybercriminals use a piece of malware is only partially attributable to functionality and vulnerabilities exploited. A tool kit's flexibility for payment mechanisms and the built-in ability to obscure traceability are also important. Kharraz and colleagues thoroughly analysed the most popular ransomware software [12]. They reached some interesting conclusions about attacker behaviour. Analysing 1359 samples, they found that more than 80% of tool kits included features for obscuring payment traceability. Not surprisingly, cryptocurrencies were most popular for receiving extorted money, with bitcoin being the cryptocurrency most demanded by attackers at the time of the study. Others requested cash cards, like Moneypak, Paysafe, or UKash. Of those using bitcoin, almost three-quarters used a bitcoin address for only two transactions (the incoming transaction to receive payment, then an outgoing one to move the funds) [12]. From there, attackers split the outgoing funds into multiple accounts (or cryptocurrency wallets) to obscure traceability. They laundered the extorted funds by mixing them with funds in other wallets accumulated from various sources. The 'clean' funds were later recombined and dispersed back to the attacker in a 'clean wallet'. Most of the accounts and aliases associated with these wallets were active for fewer than five days. Following this period of time, they were often discarded and never used again.

4.2. Component Costs and Value Creation of Ransomware Tools

The darkweb marketplace for the different components of a ransomware attack is opaque but not impossible to survey. Huang and colleagues offer clues on how value can be exchanged and disrupted. They document entire pharmacy databases of customers' personal information available for less than $1000 [31]. There are groups (or so-called bot-nets) of compromised devices with pre-installed bitcoin mining software for an average price of €2.25. Phishing services, managed by professional cybercriminals and operating on a criminal customer's behalf, cost approximately $100 per month [31].

Although their research into the value chain of ransomware transactions was limited to a single example, it provides some evidence that warrants broader study. Huang et al. note that the darkweb purchase of the Neutreno ransomware payload, corresponding tool kit, and related services to execute a ransomware attack end-to-end would cost approximately $13,000 per/month plus an aggregate commission of 40% on gains. Based on reports by the Cisco cyber research team, conservative estimates of return on investment by a skilled hacker gang would exceed 500% or $81,000 per/month [31]. This could be accomplished by a criminal with minimal technical skill or prior experience in cybercrime.

This analysis is based on a review of one tool kit and one exploit. Although it does not necessarily represent the broader population of ransomware tool kits and actors, it supports the idea that the rapid growth of ransomware can be explained by its ability to generate value more easily, elusively, and profitably than other cybercrime-related activities. The authors also suggest several areas for further study that could alter ransomware returns on investment to the detriment of attackers. We return to this topic in the Conclusion.

4.3. Absence of Direct or Deferred Consequences

A significant financial component common in crime prevention, but absent in the fight against ransomware, is the imposition of costs after the crime. After a bank heist, for example, criminals are forced to abandon vehicles and technology. They often cannot reuse aliases that took time and money to create. They might have sunk costs in safe houses and equipment. This is often not the case in cybercrime, particularly ransomware crime. It significantly affects the cost side of the ledger when criminals know that their tools, networks, and well-being will be harmed because of their crimes [32].

In his Nobel Prize winning research into the economic framing of critical motivation, Gary Becker theorised that criminal decisions are made under a paradigm of *marginalism* which only takes into account the proximate costs and perceived benefits of the crime, with little regard given for the costs and benefits already experienced [33]. Further, Nagin and coauthors build on this premise and suggest that criminal motivations will be higher where they risks associated with the marginal decision are opaque [34]. From the criminal perspective, this likely makes ransomware especially lucrative.

We investigated this hypothesis, searching the literature on ransomware to determine if any research capable of determining the impact of *marginalism* on ransomware actors' perceptions of the value created by a cyberattack. Laszka and colleagues have developed a novel approach for pricing the optimum ransom demand to ensure profitability for the attacker. It highlights the lucrative opportunities for attacker revenue creation, given the current constraints of the system [35]. That said, revenue represents only one side of the equation. Profit requires the subtraction of expenses and other costs from gross revenues. Laszka et al. suggest a formulation for calculating the execution cost of ransomware attacks. The entire analysis merits consideration, but the core function posits a straightforward calculation of the unit cost of the attack, consisting of a valuation of the attacker's time plus the cost of developing or acquiring the attack software. The authors concede, however, that this issue is understudied, and while they do arrive at some interesting methods for estimating the value of the attacker's time, there was insufficient data to calculate the overall attack cost using this method at the time of the article's publication.

During our review of the topical literature, we did not identify any method that can suitably model costs and the breakeven point where commercially motivated ransomware attacks stop being profitable. There are, however, some interesting results from the private sector. Published in 2011, Martin's 'Cyber kill chain' whitepaper identified seven steps that cyber actors must take to complete an attack [36]. Briefly summarised, the steps are: (1) 'reconnaissance' to identify an exploitable target; (2) 'weaponisation' of a payload capable of exploiting the vulnerable system; (3) 'delivery' of the payload via some mechanism, i.e. phishing; (4) successfully bypassing installed controls, such as anti-virus, and 'exploiting' the victim system; (5) 'installation' of a second-stage malware with the ability to conduct the intended activity of those data without being blocked; (6) 'command and control' of the victim system by the attacker; and (7) 'actions on intent', such as key exchange and encryption for a ransomware attack. The article articulated a method for modelling an attack that allows defenders to target each step of the attacker's actions. Although some of the terminology may seem obscure, it allowed for much more complex attack vectors to be grouped for analysis and countermeasure. This led to an approach in cybersecurity, known as 'intelligence-driven defence', which has been used as the basis for numerous cybersecurity innovations. The result has increased not only the defence efficacy but also the cost of performing attacks significantly.

In a recent interview, Mike Poddo (one of the coauthors of the original 'Cyber kill chain' article) explained the results of a career spent applying intelligence-driven defence to deter attacks:

> 'Even well-funded, professional cyber actors operate with limited resources, this includes financial resources, but also includes time, patience, and rare zero-day exploits'.[4]

Poddo goes on to explain that, by analysing an attack at all seven stages of the kill chain, he was able to prioritise controls focused on each stage. This was done to maximise protection, but there are further benefits. For example, an attack might successfully bypass controls at the first four stages only to be caught at the fifth stage. However, the attacker is often blind to where the failure occurred. They know only that the attack failed and that there was no response from the device they were attempting to infect. They would then often replace every element of the attack infrastructure used in the first five stages. Poddo speaks of regularly seeing attackers discard perfectly good command and control infrastructure (which was unknown to defenders and was not being blocked) out of fear that it may have been detected. There were also times when his team discovered rare zero-day exploits, not through research or complex modelling but because they detected the attack using conventional controls at a subsequent stage and then reverse-engineered the initial exploit. Over time, even the most well funded attackers would tire of burning resources. Poddo had the following to say about the impact of this method of defence on attacker morale:

> It's hard to know anyone's precise motivations, but we have KPIs [key performance indicators] associated with our jobs. If you were a hacker and your job was to successfully target companies in the defense and security sectors, wouldn't you get tired of showing reports that indicated you spent lots of hours, burned through lots of vulnerabilities and malware that were painstakingly developed, and had no successful compromises to show for it? [37]

The question is obviously rhetorical; we would likely answer it in the affirmative. The cyberworld includes endless potential targets. The experiences Poddo recounts indicate that cyber attackers are motivated to maximise the return on their investments of time and energy. It also suggests that the incentive to engage in the attack decreases as both actual and opportunity costs for an attack increase.

4——'Zero-day vulnerability' is an industry term used to describe vulnerabilities discovered by an attacker before the manufacturer of the software discovers them. There are then no developed patches or countermeasures in place. Once used, the vulnerability is traceable and the software manufacturer can develop fixes. The day the fixes are released is counted as day 1 of the vulnerability's life.

5. How Should Society Respond: Effective Ethical, Social, and Legal Constraints on Ransomware

Perspectives on the ethical implications of preventing cybercrime vary. According to Hollis and Ohlin, ethical actions concerning cybercrime should align with 'self-defense, economic interests in protecting intellectual property, and public health' [38]. Much scrutiny has been applied to regulatory interventions targeted at cybercriminals but impacting citizen privacy as collateral damage. Critiques of these actions are numerous and are outside the scope of this article. More relevant to this review is the efficacy of these interventions at cybercrime deterrence. Here, the evidence suggests attempts to control cybercrime through purely punitive means have largely failed to keep up with the forces compelling its growth.

Law enforcement has mostly been slow to adapt rules of evidence and patterns of investigation to digital crimes [39]. Governments also struggle to deal with the transnational nature of most cybercrimes and the methodological process of international adjudication. Cyberspace facilitates borderless digital theft and hacktivism unmoored from standard constraints of proximity in the physical world. The crimes occur in a new domain of competition where there are no established norms for social pressures to act as restraints on bad behaviour [40]. Governance structures still observe Westphalian boundaries that do not apply to the digital contours of cyberspace [41].

In addition to the ambiguous and inadequate governance of cyberspace, the growth of ransomware also benefits disproportionally from advances in anonymous cryptocurrency payment mechanisms [41]. Paquet-Clouston and colleagues argue that the widespread popularity of cryptocurrencies, such as bitcoin, has made a once fraught exchange of value low-risk and largely seamless. This is somewhat unique in the exchange of stolen goods. Usually, stolen property – art objects, for example – trade at a significantly reduced value owing to potential forfeiture and penalties for trading in stolen goods. A conventional ransom exchange is especially fraught because the currency can be traced, and both the kidnappers and victims are physically vulnerable. Current governance structures and ethical pressures do not allow the imposition of the same constraints on cyber ransom.

Moreover, corporate shareholder interests are often misaligned with those of stakeholders. As Etzioni argues, a range of factors misalign the interests of corporations – typically the most

significant victims of ransomware – with societal aspirations (whether individual or collective) [42]. Etzioni states four reasons for this: concerns about cost, regulatory burden, consumer pressure, and efficacy. He illustrates with an analogy to historical self-regulation challenges regarding environmental pollution. Quoting a cybersecurity expert at the Security and Exchange Commission, Etzioni writes:

> Cybersecurity resembles environmental law in that both fields are primarily concerned with negative externalities. Just as firms tend to underinvest in pollution controls because some of the costs of their emissions are borne by those who are downwind, they also tend to underinvest in cyber defenses because some costs of intrusions are externalised onto others. [42]

To address this imbalance, a combination of social pressure, criminal penalties, public policy, and financial disincentives is required. To be done with the highest degree of efficacy, a policy should align corporate, individual, and societal interests.

5.1. Relevant Literature in the Field of Criminology

Cybercrime occurs in a digital but not invisible marketplace. Many criminal cyber transactions market illicit goods deniably on the dark web and the exchange of value occurs online based on fictitious and deniable personas. Many crimes, ranging from illegal distribution of narcotics to wildlife trafficking, were once primarily confined to the terrestrial domain but now leverage the discretion of deniable cyberspace. This is especially well documented in literature on criminology as catalogued by Sebagh in *Policing illegal drug and wildlife trades* [43]. Yet, although the research demonstrates that it is possible to observe the illicit trade on the dark web and apply specialised policing techniques, these have had limited affect owing considerably to the complexity of the jurisdictional environment and the lacking specialisation of law enforcement in digital forensics. Still, cybercrime is overwhelmingly conducted for profit, and law enforcement actions resulting in judicial penalty are only one means of affecting actor motivations. A range of law enforcement and adjacent organisations (some state-sanctioned and others not) have demonstrated their ability to affect criminal behaviour by raising real and perceived costs to the criminals. As Button demonstrated in *Private Policing*, the critical factor is for law enforcement actions to align with the public's perceived and real interests, not only to align against the interests of criminals [44].

We examine this through analysis of a conventional variant of a similar crime in the following section.

5.2. Conventional Kidnapping and Ransom Case Study

As mentioned, the ethical implications of ransomware-related crimes are understudied. However, analyses and evaluations of more conventional ransom-related crimes are quite robust. Consider the rise of kidnappings for ransom in Latin America in the late 20th century. Studies adopting the GELSI approach to conventional kidnapping could illuminate the ransomware problem. The National Defense University's Marks notes that the Revolutionary Armed Forces of Colombia's (FARC) use of kidnapping as a tool to generate ransom-related revenues in the 1980s and 1990s progressed from a source of minor revenue to the primary means of operational finance [45]. From a governmental and ethical perspective, this was considered far more benign than FARC's narcotics activity or its violent campaign against the government. It also furthered the local perception of FARC members as freedom fighters. Funds were extracted from wealthy foreign corporations, many of which were viewed by working-class locals as exploiting the country. Violence was also generally directed at foreigners, and most kidnappees were eventually returned alive.

This coincided with the mainstreaming of Kidnap and Ransom (K&R) insurance, offered primarily to expatriate executives from the United States and Europe. Ransom payment generally resulted in favourable outcomes. Nonetheless, some evidence suggests that this also created a moral hazard. The presence of insurance contracts and the likelihood of seamless high-value payouts caused what is known in the insurance industry as *adverse selection*: being insured increases the risk of kidnapping [46]. Kidnappings in Colombia rose from 42 in 1982 to 3572 per year by the end of the century, an increase of more than 8000% [47]. By the early 1990s, Colombia had grown to lead the world in kidnappings. K&R insurers were quick to recognise this trend. They responded with a series of requirements for new insurance policies that effectively reduced adverse selection effects. Payouts to groups, such as FARC, also decreased because the US Office of Foreign Asset Control (OFAC) employed an international governance approach focused on terrorist financing. Partner nations adopted similar methods [48]. Other political and social factors likely co-contributed to reducing kidnappings in Colombia. These are addressed by Pires et al. and it is informative to read their conclusion in its entirety [47]. However, there appears to be a clear correlation between measures taken by

insurers and regulators on the one hand and decreasing kidnappings on the other. By 2010, the overall frequency of kidnapping for ransom in Colombia had dropped by 91% [47].

5.3. Adverse Selection and Moral Hazard in Responses to Ransomware

The cautionary tale of the K&R insurance market is illustrative of the present-day dynamics in cyber and ransomware insurance. We see a similar adverse selection bias in ransomware activities. The present cyber insurance market appears to be driven by the rise in ransomware targeting commercial enterprises. However, cyber insurance also contributes to the sharp ransomware growth curve. Baker and Shortland, reflecting on the previously mentioned ransomware incident at Colonial Pipeline, noted that insurance may have contributed to a double failure, first failing to incent Colonial to achieve a security posture capable of limiting the damage of the hack and then by paying a large and public ransom that likely incented other bad actors [49]. According to Manky from cybersecurity company Fortinet, ransomware attackers will search a victim network for evidence of ransomware insurance contracts [50]. The attackers often take a particular interest in the deductible and maximum payouts guaranteed by a policy. We also see a trend in pricing related to the requested ransom that closely tracks conventional kidnapping and ransom. Attackers frequently align the ransom amount with their understanding of typical ransomware coverage to maximise returns and expedite payment [41].

There are then evident similarities between the two ransom- and extortion-based insurance markets. Just as abuse of K&R insurance led to hardening of industry standards for security, Mott et al. demonstrate the sharp increase in ransomware crimes led to the insurance industry putting significant pressure on companies to improve internal security controls before they would be deemed 'insurable' [51]. There also appear to be similarities between the decision calculus of those paying the ransom. Connolly and Hervé reflect on more than 40 specific ransomware cases and document that, even when benefit of payment appears clear, the victims considered a range of views about ethics of rewarding the attacker or the degree to which they could trust their guarantees, each making their decision far more complex [52]. However, it remains unclear whether governance measures targeted at reducing incentives for payment will result in similar reductions in ransomware attack frequency. This area demands further study, as the point is less obvious than it may seem. On the one hand, it is reasonable to expect

that governance of payout mechanisms and checks on adverse selection effects will drive ransomware attack numbers down. On the other hand, there are notable dissimilarities between the two cases that may directly affect the efficacy of such controls and require careful investigation.

For example, efforts have been made to reduce payments to ransomware actors through governance actions, such as OFAC. Some ransomware cartels have been labelled terrorist organisations, and ransom payments compared to terrorist financing. This mirrors the designation given to FARC in Colombia. However, unlike the Colombian example, the actor-and-victim relationship is not geographically bound when it comes to cybercrime. In Colombia, the actors were members of a known group that physically congregated, organised in camps within FARC-controlled territory, and considered themselves members of an organisation with rank and hierarchy. Such a group can be designated an identifiable terrorist organisation and/or added to a banned list [46]. However, in the case of cybercrimes, attribution is non-geographical and often beyond the technical means of the victims. Cartel members may be distributed worldwide, and group affiliation may be discrete. Misattribution of attacks by ransomware syndicates known to be on a banned list will likely diminish the effect of these measures. A detailed investigation of the mechanisms that would disincentivise ransomware attacks is sorely needed but would be far from simple.

6. Conclusion

The frequency and extent of the damage continue to grow. The actor rationale behind this growth is straightforward: ransomware simplifies the attacker value chain. It commoditises the victim's data, selling access to such data back to the victim. It exploits vulnerabilities that are abundantly available in software and computing systems. The illicit market for ransomware tool kits and exploits operates efficiently, where the most powerful malware and prolific actors rise to the top. This market is widely accessible to parties with a range of technical skills. It offers attack building blocks and raw materials to the technologically adept; it offers 'ransomware as a service' for the technophobe. The barriers to entry are low, and the return is high (and growing higher). What further conclusions can be drawn from this realisation? Are there areas of investment or study that could alter the current incentive model, thus forcing the curve of ransomware growth downward?

It is clear that ransomware actors operate with motivations similar to those of other more conventional criminal actors. As a result, it stands to reason that policies targeted at their motivations would likely have a limiting effect. This was demonstrated by Waldrop in 2016, chronicling a series of punitive efforts directed at cybercriminals. They found that a law enforcement takedown of one group might have a 'creative destruction' affect similar to the failure of a business in the conventional economy, but also that punitive efforts that raised the cost of a material need by criminals did impact their behaviour, driving it away from the cost increase and towards an alternative [53]. Yet, it remains true that the overwhelming majority of the academic literature focuses on the technical nature of ransomware crimes. Our research found that the majority of hard data on attacker activity, motivations, and transactions comes from industry. Only a handful of sources addressed the multi-disciplinary *who* and *why* questions that were our scope for this review.

Still, from the literature that does exist, it seems clear that reducing the financial benefits would significantly reduce the frequency of ransomware crimes, given that ransomware actors are primarily motivated by monetary gain. Given Schneier's observation that the majority of cybercriminals are low skill and low focus, combined with Hill's [24] observation of the low average individual return, simply raising the real or opportunity costs of carrying out ransomware attacks could significantly reduce the frequency of ransomware crimes. Furthermore, concentrated social and legal pressure applied against the comparatively small number of criminal cartels generating disproportionate harm could have an outsized impact on the value realised by these organised ransomware actors owing to the concentration of the ransomware market (as measured by HHI). The economic impact on corporations and the life-threatening implications for individuals should motivate further innovations to reduce ransomware incentives. If properly understood, this could have the effect of leading to a greater convergence between societal norms and social values in cyberspace that might disincentivise criminal behaviour and lead to a greater degree of public diligence and corporate compliance. They could drive general acceptance of business models for technology products that impose a modest amount of friction for consumers, but with the benefit of rendering criminal technology business models obsolete.

There are many examples of similar parallels emerging in society and governance. Consumers first sought optional safety features in vehicles, many of which became standards enshrined in transportation regulations. Were the standards and governance removed,

it is unlikely that consumers would readily go back to driving vehicles without seat belts, airbags, or anti-lock brakes – suggesting that the features provide value that exceeds the mandated compliance. Individuals also readily accept a slight delay in access to their funds from the banking system to allow for transactions to clear, so as to reduce the risk of fraudulent transactions. It is certainly conceivable that similar concessions could be made in cyberspace if it was clearly demonstrated that the cost to society was well below the cost imposed on criminal actors. It stands to reason that such innovations would fundamentally reduce the real and perceived value of financially motivated cybercrime.

It is the conclusion of this review that cyber governance strategies that address the growth of cybercrime in general, and ransomware specifically, are understudied and badly needed. Further research needs to be done on how to provide potential victims and societies with significant leverage against attackers. Some limited work in this direction has begun [54], providing an excellent starting point. However, if society is to successfully combat cybercrime, effective governance must consider the social and financial costs of remedies and ensure that the costs are aligned with societal norms and values with the costs primarily allocated to the bad actors. A detailed study of these costs, both allocated to society and to cybercriminal, is necessary. It should engage the domains of economics and criminology to the same or greater degree than that of computer science, and should focus on demonstrating specifically the point at which social, legal, and financial pressures can bring the cost of conducting ransomware attacks equal to the value likely to be achieved by the cybercriminal. Such a study lies beyond the scope of this review article, but is planned as the topic of forthcoming research.

References

[1] VirusTotal Blog. (2021). *Ransomware in a global context.* [Online]. Available: https://blog.virustotal.com/2021/10/ransomware-in-global-context.html [Accessed: Feb. 03, 2024].

[2] Verizon Business. (2021). *DBIR results & analysis.* [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/ [Accessed: Apr. 01, 2023].

[3] Businesswire. (Aug. 12, 2021). *IDC survey finds more than one third of organizations worldwide have experienced a ransomware attack or breach.* [Online]. Available: https://www.businesswire.com/news/home/20210812005739/en/IDC-Survey-Finds-More-Than-One-Third-of-Organizations-Worldwide-Have-Experienced-a-Ransomware-Attack-or-Breach [Accessed: Apr. 01, 2023].

[4] TechTarget. (2023). *Ransomware trends, statistics and facts in 2023*, Security. [Online]. Available: https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts [Accessed: Apr. 01, 2023].

[5] C. Radu, N. Smaili, "Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure," *Journal of Business Ethics*, vol. 177, no. 2, pp. 351–374, 2021, doi: 10.1007/s10551-020-04717-9.

[6] K. Farahbod, C. Shayo, J. Varzandeh, "Cybersecurity indices and cybercrime annual loss and economic impacts," *Journal of Business and Behavioral Sciences*, vol. 32, no. 1, pp. 63–71, 2020.

[7] GlobeNewswire Inc. (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025.* [Online]. Available: https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html [Accessed: Oct. 09, 2023].

[8] R. Anderson, C. Barton, R. Bohme, R. Clayton, C. Gañán, T. Grasso, M. Levi, T. Moore, M. Vasek, "Measuring the changing cost of cybercrime," in Proceedings of the 18th Workshop on the Economics of Information Security (WEIS), Dec. 2018.

[9] T. Seals. (2020). "FIN11 cybercrime gang shifts tactics to double-extortion ransomware," *The Cybersecurity Review.* [Online]. Available: https://www.cybersecurity-review.com/news-october-2020/fin11-cybercrime-gang-shifts-tactics-to-double-extortion-ransomware/ [Accessed: Apr. 01, 2023].

[10] M. Novinson. (Dec. 23, 2021). "The 10 biggest cyber and ransomware attacks of 2021," *CRN.com.* [Online]. Available: https://www.crn.com/slide-shows/security/the-10-biggest-cyber-and-ransomware-attacks-of-2021 [Accessed: Aug. 27, 2024].

[11] M.J. Grant, A. Booth, "A typology of reviews: an analysis of 14 review types and associated methodologies," *Health Information & Libraries Journal*, vol. 26, no. 2, pp. 91–108, 2009, doi: 10.1111/j.1471-1842.2009.00848.x.

[12] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda, "Cutting the Gordian knot: A look under the hood of ransomware attacks," in *Detection of intrusions and malware, and vulnerability assessment*, DIMVA 2015. Lecture Notes in Computer Science, vol. 9148, M. Almgren, V. Gulisano, F. Maggi, Editors. Cham: Sringer, 2015, doi: 10.1007/978-3-319-20550-2_1.

[13] T. McIntosh, A.S.M. Kayes, Y.-P.P. Chen, A. Ng, P. Watters, "Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions," *ACM Computing Surveys*, vol. 54, no. 9, pp. 1–36, 2022, doi: 10.1145/3479393.

[14] R. Richardson, M. North, "Ransomware: Evolution, mitigation and prevention," *International Management Review*, vol. 13, `no. 1, pp. 10–21, 2017.

[15] J. Lee, "State of Security 2024," (2024). Splunk. [Online]. Available: https://www.splunk.com/en_us/pdfs/gated/ebooks/state-of-security-2024.pdf [Accessed: Jun. 10, 2024].

[16] Verizon Business. (2022). *DBIR report 2022 – Summary of findings.* [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/ [Accessed: Jun. 10, 2024].

[17] I. Yaqoob, E. Ahmed, M.H. Rehman, et al. "The rise of ransomware and emerging security challenges in the Internet of things," *Computer Networks*, vol. 129, no. 2, pp. 444–458, 2017, doi: 10.1016/j.comnet.2017.09.003.

[18] T. Mulhall "Computer-related fraud and its evolution within telephony," *Computers & Security,* vol. 16, no. 6, pp. 521–521, 1997, doi: 10.1016/S0167-4048(97)84676-7.

[19] A. Pawlicka, M. Choraś, Pawlicki, "The stray sheep of cyberspace a.k.a. the actors who claim they break the law for the greater good," *Personal and Ubiquitous Computing*, vol. 25, no. 5, pp. 843–852, 2021, doi: 10.1007/s00779-021-01568-7.

[20] I. Harford. (Oct. 2021). "The history and evolution of ransomware," *Tech Target.* [Online]. Available: https://www.techtarget.com/searchsecurity/feature/The-history-and-evolution-of-ransomware [Accessed: Sep. 26, 2022].

[21] M. Egan. (2021). "Gasoline demand spikes in several states after pipeline hack," *CNN Business.* [Online]. Available: https://www.cnn.com/2021/05/11/business/gas-shortage-demand-pipeline-hack/index.html [Accessed: Jun. 12, 2024].

[22] Homeland Security Newswire. (Apr. 21, 2010). *World's youngest known hacker caught.* [Online]. Available: https://www.homelandsecuritynewswire.com/worlds-youngest-known-hacker-caught [Accessed: Jun. 12, 2024].

[23] B. Gilbert. (2019). "Lamborghinis, baby lions, and stacks of cash: The Russian hackers in charge of 'Evil Corp' are living an absurdly lavish lifestyle," *Business Insider.* [Online]. Available: https://www.businessinsider.com/millionaire-russian-hackers-evil-corp-car-pictures-video-2019-12. [Accessed: Jun. 12, 2024].

[24] M. Hill. (2016). "'Flipping the economics of attacks' – A report," *Infosecurity Magazine.* [Online]. Available: https://www.infosecurity-magazine.com/blogs/flipping-the-economics-of-attacks/ [Accessed: Sep. 26, 2022].

[25] CSO Online. (2016). *A booming business: The rise of cybergangs* [Online]. Available: https://www.csoonline.com/article/559369/a-booming-business-the-rise-of-cybergangs.html [Accessed: Feb. 01, 2024].

[26] I. Thornton-Trump, "Malicious Attacks and Actors: An Examination of the Modern Cyber Criminal," *EDPACS*, vol. 57, no. 1, pp. 17–23, 2018, doi: 10.1080/07366981.2018.1432180.

[27] W. Gragido, *Blackhatonomics an inside look at the economics of cybercrime*, 1st ed. Amsterdam: Syngress, 2013.

[28] D. Freeze. (2021). "Cybercrime to cost the world $10.5 trillion annually by 2025," *Cybercrime Magazine* [Online]. Available: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ [Accessed: Jun. 12, 2024].

[29] Verizon Business. (2024). *DBIR report 2024 - Summary of findings.* [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings/ [Accessed: Jun. 12, 2024].

[30] D.B. Cornish, R.V. Clarke, "Understanding crime displacement: An application of rational choice theory," *Criminology*, vol. 25, no. 4, pp. 933–948, 1987, doi: 10.1111/j.1745-9125.1987.tb00826.x.

[31] K. Huang, M. Siegel, K. Pearlson, S. Madnick, "Casting the dark web in a new light," *MIT Sloan Management Review*, vol. 61, no. 1, pp. 84–85, 2019.

[32] The Azure Forum. (2022). *Deterring ransomware attacks: Treat ransomware as criminality* [Online]. Available: https://www.azureforum.org/deterring-ransomware-attacks-as-an-international-security-priority-treat-ransomware-as-criminality/ [Accessed: Jun. 12, 2024].

[33] G.S. Becker, "Crime and punishment: An economic approach," *Journal of Political Economy*, vol. 76, no. 2, p. 169, 1968, doi: 10.1086/259394.

[34] D.S. Nagin, F.T. Cullen, C.L. Jonson, Eds., *Deterrence, choice, and crime, vol. 23: Contemporary perspectives*. New York: Routledge, 2018. doi: 10.4324/9781351112710.

[35] A. Laszka, S. Farhang, J. Grossklags, "On the economics of ransomware," *arXiv.org*, 2017, doi: 10.48550/arxiv.1707.06247.

[36] Martin L. (2015). *Cyber kill chain®* [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html [Accessed: Jun. 12, 2024].

[37] M. Poddo, "Cyber killchain interview," Jun. 2021. Interview by J. Jaffe.

[38] D.B. Hollis, J.D. Ohlin. (2018). *What if cyberspace were for fighting?* [Online]. Available: https://solo.bodleian.ox.ac.uk/discovery/fulldisplay?docid=cdi_gale_infotracmisc_A570532983&context=PC&vid=44OXF_INST:SOLO&lang=en&search_scope=MyInst_and_CI&adaptor=Primo%20Central&tab=Everything&query=any,contains,what%20if%20cyberspace%20was%20for%20fighting&offset=0 [Accessed: Jan. 31, 2024].

[39] G. Gogolin, J. Jones, "Law enforcement's ability to deal with digital crime and the implications for business," *Information Security Journal*, vol. 19, no. 3, pp. 109–117, 2010, doi: 10.1080/19393555.2010.483931.

[40] P. McGuiness, "Interview with Paddy McGuiness," Jan. 2022. Interview by J. Jaffe.

[41] M. Paquet-Clouston, B. Haslhofer, B. Dupont, "Ransomware payments in the Bitcoin ecosystem," *Journal of Cybersecurity*, vol. 5, no. 1, pp. 1–11, 2019, doi: 10.1093/cybsec/tyz003.

[42] A. Etzioni. "Cybersecurity in the private sector," *Issues in Science and Technology*, vol. 28, no. 1, pp. 58–62, 2011.

[43] L. Sebagh, *Policing illegal drug and wildlife trades – The role of the police, legal online platforms, private organisations and individuals, and cybercriminal traders*. PhD thesis, Oxford: University of Oxford, 2021.

[44] M. Button, "Voluntary policing," in *Private policing*, 2nd ed. London: Routledge, 2019, pp. 128–151. doi: 10.4324/9781351240772-8.

[45] T.A. Marks, "FARC, 1982–2002: Criminal foundation for insurgent defeat," *Small Wars & Insurgencies*, vol. 28, no. 3, pp. 488–523, 2017, doi: 10.1080/09592318.2017.1307612.

[46] P.L. Brockett, L.L. Golden, S. Zaparolli, J.M. Lum, "Kidnap and ransom insurance: A strategically useful, often undiscussed, marketplace tool for international operations," *Risk Management and Insurance Review*, vol. 22, no. 4, pp. 421–440, 2019, doi: 10.1111/rmir.12134.

[47] S.F. Pires, R.T. Guerette, C.H. Stubbert, "The crime triangle of kidnapping for ransom incidents in Colombia, South America: A 'Litmus' test for situational crime prevention," *British Journal of Criminology*, vol. 54, no. 5, pp. 784–808, 2014, doi: 10.1093/bjc/azu044.

[48] US Department of the Treasury. (Apr. 22, 2008). *Treasury targets FARC financial network in Colombia.* [Online]. Available: https://home.treasury.gov/news/press-releases/hp938 [Accessed: Jun. 12, 2024].

[49] T. Baker, A. Shortland, "Insurance and enterprise: Cyber insurance for ransomware," *Geneva Papers on Risk and Insurance – Issues and Practice* , vol. 48, no. 2, pp. 275–299, 2023, doi: 10.1057/s41288-022-00281-7.

[50] D. Manky, J. Richberg (Feb. 17, 2022). *Ransomware cyber insurance & settlements Q&A*, Fortinet Blog. [Online]. Available: https://www.fortinet.com/blog/industry-trends/qa-ransomware-settlements-and-cyber-insurance [Accessed: Jun. 12, 2024].

[51] G. Mott, S. Turner, J.R.C. Nurse, J. MacColl, J. Sullivan, A. Cartwright, E. Cartwright, "Between a rock and a hard(ening) place: Cyber insurance in the ransomware era," Computers & Security, vol. 128, 2023, doi: 10.1016/j.cose.2023.103162.

[52] A. Yuryna Connolly, H. Borrion, "Reducing ransomware crime: Analysis of victims' payment decisions," *Computers and Security*, vol. 119, no. C, 2022. doi: 10.1016/j.cose.2022.102760.

[53] M.M. Waldrop, "How to hack the hackers: The human side of cybercrime," *Nature*, vol. 533, no. 7602, pp. 164–167, 2016, doi: 10.1038/533164a.

[54] Verizon Business. (2023). *DBIR report 2023 – Summary of findings.* [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/ [Accessed: Jun. 12, 2024].