Ransomware and Cyber Insurance: delving into the legality issue

Lucas Nascimento*

Introduction

In an era where digital landscapes dominate global economies, the battle against cyber threats has taken centre stage. Among these threats, ransomware has emerged as a formidable adversary, locking down businesses, institutions, and even critical infrastructure with ever-increasing frequency. As organizations struggle with the decision of whether to pay ransoms to regain control of their digital assets, a complex dilemma regarding the legality of these payments has arisen. Simultaneously, the rising popularity of cyber insurance further muddies the waters, bringing a new dimension to the debate surrounding the legality of ransomware payments and the existence of insurance cover against it.

On the one hand, there are arguments supporting that paying ransom demands and taking out insurance to support these payments should be illegal, as they may fuel cybercriminal activity and the ransomware business. On the other hand, paying ransom demands may sometimes be a more cost-effective and safer option to end the attack and cyber insurance has the potential to work as a feature to mitigate losses of victims and to promote better cyber security standards.

This paper delves into the intricate web of considerations that surround the legality issue of paying ransoms to cybercriminals and the presence of cyber insurance. Exploring the tensions between legality and practicality, it presents the reasons why this issue holds critical relevance in today's digital age. From examining the potential implications of ransomware attacks to understanding the evolving role of cyber insurance in mitigating financial risk, this analysis aims to shed light on a topic that impacts not only individual organizations but the broader security fabric of our interconnected world, and to explore possible initiatives that could strengthen the weapons against ransomware.

Given this context, the purpose of this paper is to answer whether it should be illegal in the United Kingdom to pay ransom demands arising from cybercrime and to have insurance coverage for them. Additionally, this paper intends to assess possible alternatives to making ransom payments illegal.

In terms of methodology, the study is a desk-top doctrinal analysis of case law and a review of secondary sources, including books, academic articles, journals, government reports, insurance and cyber security industry reports, media reports, and online forum discussions.

The central part of this paper is divided into three sections: section 1 defines ransomware attacks based on information technology sources, aiming to introduce the subject and explain the characteristics of this kind of cybercrime, as well as some statistics to demonstrate the magnitude of such a threat. Section 2 outlines

* Master of Laws (LL.M.) in Insurance Law, Queen Mary University of London. Specialist in Civil Procedure Law, Universidade Presbiteriana Mackenzie. Bachelor of Laws (LL.B.), Centro Universitário das Faculdades Metropolitanas Unidas (FMU). Associate at the Insurance, Reinsurance, Private Pensions and Supplementary Health team of Demarest Advogados (Sao Paulo, Brazil). Email lcnascimento@demarest.com.br.

the background of cyber insurance and the development of underwriting practices, as well as examines the role it performs against the risk of ransomware. Section 3 starts with an overview of the relevant issue regarding the legality of paying ransom demands arising from cyberattacks and the existence of insurance cover for them. Then, it examines both the arguments of the cases against and for the legality. Finally, it presents alternatives to banning ransomware payments and insurance from a legal perspective. The paper finishes with a summary of the proposed alternatives for insurers and the UK Government.

1. Defining Ransomware Attacks

Ransomware is a type of malware that infects a computer system and locks the user's access to data, typically by encrypting it.[1] The attackers then demand the victim to pay a ransom to regain access to their computer and data, usually demanded in cryptocurrencies due to their ability to provide cybercriminals with anonymity, as they are harder to trace.[2]

There are different types and ways in which a ransomware attack can be executed. The most common ones are known as *"Locker"*, which blocks access to computers until a payment to unlock is made, and *"Crypto"*, that encrypts files until a payment is made to receive a decryption key.[3] Seeking to earn even more money from these attacks, hackers are progressively using a tactic known as *"Double extortion"*, whereby not only they encrypt the data, but also demand a higher ransom to not make them public. This tactic can be very effective because, even if the victim has a backup of their files, they can still be coerced to pay the ransom to avoid having all of their information leaked.[4] Finally, there is another type known as *"Ransomware as a Service (RaaS)",* a business model that allows subscribers to carry out ransomware attacks by using a pre-developed ransomware software and paying a percentage of each successful ransom to the malware creator.[5]

Hackers usually obtain access to systems and files through three common vectors: *phishing*, whereby the attacker pretends to be someone else in a genuine looking email hoping that the victim click on a malicious link or open a malicious attachment[6]; brute force attacks, a trial-and-error method used by software to

---

[1] Sandra Gittlen, 'The Complete Guide to Ransomware' (*TechTarget*, 27 June 2023) <www.techtarget.com/searchsecurity/Guide-to-preventing-phishing-and-ransomware> accessed 23 August 2023.

[2] Jake Moore, 'The Rising Cybersecurity Concerns of Cryptocurrencies' (*TechRadar*, 2 December 2021) <www.techradar.com/features/the-rising-cybersecurity-concerns-of-cryptocurrencies> accessed 23 August 2023.

[3] Gittlen (n 1).

[4] Nicholas Fearn, 'Double extortion ransomware attacks and how to stop them' (*ComputerWeekly.com*, 27 August 2020) <www.computerweekly.com/feature/Double-extortion-ransomware-attacks-and-how-to-stop-them?_gl=1*i6k3wx*_ga*NjU2OTgxODUuMTY5MjE5MDU2MQ..*_ga_TQKE4GS5P9*MTY5MjE5MDU2MS4xLjEuMTY5MjE5NTA2MC4wLjAuMA..&_ga=2.213519632.52293748.1692190567-65698185.1692190561> accessed 23 August 2023.

[5] Kinza Yasar and Sean Michael Kerner, 'What is Ransomware as a Service (RaaS)?' (*TechTarget*, 7 July 2023) <www.techtarget.com/whatis/definition/ransomware-as-a-service-RaaS> accessed 23 August 2023.

[6] Alexander S Gillis, 'What is Phishing and How Does It Work?' (*TechTarget*, 21 June 2023) <www.techtarget.com/searchsecurity/definition/phishing> accessed 23 August 2023.

decode login information to gain unauthorized access to systems[7]; or by taking advantage of security vulnerabilities in systems or digital devices.[8]

These kinds of attacks usually come with short deadlines that must be met to avoid the increase of the ransom demand.[9] Moreover, it must be noted that there is no guarantee that the hackers will decrypt the files after the ransom has been paid. In fact, statistics show that victims only recover around 65% of the encrypted data after paying the ransom demand.[10] There is also no guarantee whether the malware has been left behind by the hackers and if the victim is still exposed to further attacks. "Ransomware like ZCryptor act as worms that can be left behind and reinfect your network."[11]

The impacts of a ransomware attack can be catastrophic, and the recovery process can be long and costly.[12] Not only does the victim suffer a direct loss if they decide to pay the ransom demand, but it also bears other indirect losses that can arise from the attack.[13] The most common consequence suffered by a ransomware attack is that a company suffers losses due the interruption of its business. During the time when computers are locked and files are encrypted, the company is not able to fully operate, which can result in a massive loss of revenue that in many cases can be even greater than the ransom demand itself.[14] Depending on the nature of the victim's business, the losses can even go beyond finances. In attacks against healthcare organizations, for example, shutting down operations can represent a threat to patient's lives.[15]

The victim also bears costs with the necessary measures to restore the organization's temporary or permanent lost data – for example, with IT forensics, specialist service providers and internal personnel to carry out the recovery work –, which sometimes can happen even if the ransom has been paid.

Other losses can continue to happen even after the victim has restored the lost data and has the business up and running again.[16] For example, the cost of reputational damage, which perhaps is the most durable one and the hardest to measure. As the CEO of a security platform stated, "It could take years for businesses to recover their customers as a result of a damaged reputation. Public admission to a ransomware attack can

---

[7] Katie Terrell Hanna, 'What Is a Brute-Force Attack?' (*TechTarget*, 27 September 2021) <www.techtarget.com/searchsecurity/definition/brute-force-cracking> accessed 23 August 2023.
[8] Gittlen (n 1).
[9] Ron Cadwell, 'Ransomware Examples: 25 Most Famous Ransomware Attacks' (*phoenixNAP Blog*, 27 June 2023) <https://phoenixnap.com/blog/ransomware-examples> accessed 23 August 2023.
[10] Vanson Bourne, *The State of Ransomware 2021* (Sophos News 2021) 11 <https://assets.sophos.com/X24WTUEQ/at/k4qjqs73jk9256hffhqsmf/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469> accessed 23 August 2023.
[11] Mike Wilson, 'Why Paying Ransomware Is Typically A Bad Idea And What You Can Do Instead' (*Forbes*, 12 July 2021) <www.forbes.com/sites/forbestechcouncil/2021/07/12/why-paying-ransomware-is-typically-a-bad-idea-and-what-you-can-do-instead/?sh=3c3ef24c1503> accessed 23 August 2023.
[12] Harun Oz and others, 'A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions' [2022] ACM Computing Surveys 7, 8 <http://dx.doi.org/10.1145/3514229> accessed 23 August 2023.
[13] ibid 8.
[14] *Datto's Global State of the Channel Ransomware Report* (Datto 2020) 13 <www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf> accessed 23 August 2023.
[15] Kari Paul, ''Lives Are at Stake': Hacking of US Hospitals Highlights Deadly Risk of Ransomware' (*the Guardian*, 14 July 2022) <www.theguardian.com/technology/2022/jul/14/ransomware-attacks-cybersecurity-targeting-us-hospitals> accessed 23 August 2023.
[16] Jason Blosil, 'Ransomware Cost: Measuring the True Cost of a Ransomware Attack' (*NetApp*, 24 October 2022) <www.netapp.com/blog/ransomware-cost/#:~:text=The%20lion's%20share%20of%20costs%20from%20a%20ransomware,be%2050%20times%20greater%20than%20the%20ransom%20demand.> accessed 23 August 2023.

severely impact investor confidence and strain relations with valued stakeholders."[17] On a recent case tried by the High Court[18], the claimant, which had been a victim of ransomware, was allowed to remain anonymous should they bring a legal case because of the attack – for instance, if it eventually decided to seek for injunctions to try to avoid the disclosure of illegally obtained data. As the Court granted the anonymity, it acknowledged that the nature of the business of the claimant was a sensitive one and that a "very great deal of harm" could be done if their identity were disclosed[19], which supports the idea that this kind of attack can be extremely harmful to the reputation of victims.

A ransomware attack will also trigger the obligations provided for in The Data Protection Act 2018, mainly the ones from Section 67 (1) and (8), by which the victim must notify the attack and any data breach to the Information Commissioner's Office (ICO) and eventually to the affected individuals, which will also have a cost. Likewise, the victim might be exposed to liability for damages to third parties, for example, if the business interruption has prevented it from fulfilling any contractual obligations or in case the cybercriminals decide to expose personal data that may involve those third parties.

In addition to all that, it is not unusual for victims of a ransomware attack to incur in costs with attorney fees, insurance deductibles, loss of intellectual property, hiring a public relations agency to handle the crisis, etc. The list of losses that can arise from this kind of incident is not an exhaustive one and they may vary from one victim to another.

According to a recent IBM study[20], the global average cost of a ransomware attack in 2023 is USD 5.13 million, which represents a 13% increase over the previous year. The same report identified that the average time that organizations take to identify and contain a ransomware attack is 273 days with law enforcement involved, compared to 306 days without[21], which reveals the importance of victims of cyberattacks notifying law enforcement agencies, not only for the purpose of helping to combat cybercrime, but also because it may result in significant time and cost savings.

Although the official statistics on cyber security breaches recently shared by the UK Government show that there was a decrease in the number of identified ransomware attacks compared to previous years (from 17% to 4%)[22], the UK is still the second most attacked country in the world, placing only behind the United

[17] Stu Sjouwerman, 'Seven Factors Analyzing Ransomware's Cost to Business' (*Forbes*, 29 July 2021) <www.forbes.com/sites/forbestechcouncil/2021/07/29/seven-factors-analyzing-ransomwares-cost-to-business/?sh=1738581b2e98> accessed 23 August 2023.
[18] XXX v Persons Unknown [2022] EWHC 2776 (KB).
[19] ibid [28].
[20] *Cost of a Data Breach Report 2023* (IBM 2023) 32 <www.ibm.com/reports/data-breach> accessed 23 August 2023.
[21] ibid 34.
[22] UK Government, 'Cyber Security Breaches Survey 2023' (*GOV.UK*, 19 April 2023) <www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023#summary> accessed 23 August 2023.

States.[23] In fact, as noted by the UK Government, "ransomware is a tier 1 national security threat, with attacks against businesses and public sector organizations increasingly common".[24]

Another relevant point is that, at the moment, the UK legal framework does not mandate the report of ransom payments arising from cyberattacks, which might hold back law enforcement efforts to capture cybercriminals.[25]

Research conducted by the Royal United Services Institute (RUSI)[26], a UK's leading defence and security think tank, highlights the drivers and enablers of ransomware, which helps to summarize how ransomware is an important threat in the present days. The first driver is that ransomware is a 'highly profitable and efficient business model', which is enabled by three features: the growth of ransom payments, as cybercriminals have found effective ways to extort their victims; the emergence of the cryptocurrency industry, which has made hackers to be unconcerned with being caught, as it is an untraceable payment method; and the professionalization of the ransomware ecosystem, as it has become a system with dedicated employees, along with the fact that Ransomware as a Service is widely available.[27]

The second driver is the 'poor security practices among organizations', which is enabled by the current difficulties of securing modern IT infrastructures and to keep up to date with the development of cybercriminals' tactics, and the commercial and informational barriers to invest in cyber security, which primarily affects SMEs, among which there is a sense that ransomware attacks only happen to large companies and that they do not need to protect themselves.[28]

Finally, the third driver is 'the low-cost nature of the cybercriminal ecosystem', which is enabled by the permissive law enforcement environments, mainly in Russia, a country that provides safe harbour for cybercriminals to sustain a highly developed domestic cyber ecosystem it can draw on if needed.[29]

2. The Role of Cyber Insurance Against Ransomware

The first cyber insurance plans started to appear in the 1990s, aiming to address gaps in the existing insurance lines. At that time, new regulations related to the protection of personal data were emerging in the United States, which gave rise to concerns about possible liability that could arise from it and contributed to the development of cyber insurance. Initially, cyber products included coverage for: first-

[23] Threat Intelligence Team, 'Global Ransomware Attacks at an All-Time High, Shows Latest 2023 State of Ransomware Report' (*MalwarebytesLabs*, 3 August 2023) <www.malwarebytes.com/blog/threat-intelligence/2023/08/global-ransomware-attacks-at-an-all-time-high-shows-latest-2023-state-of-ransomware-report> accessed 23 August 2023.
[24] Foreign, Commonwealth & Development Office, 'UK cracks down on ransomware actors' (*GOV.UK*, 9 February 2023) <www.gov.uk/government/news/uk-cracks-down-on-ransomware-actors> accessed 23 August 2023.
[25] Jamie MacColl and others, 'Cyber Insurance and the Ransomware Challenge' [2023] 71, Royal United Services Institute for Defence and Security Studies, <https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-ransomware-challenge> accessed 24 August 2023.
[26] ibid 15-17.
[27] ibid 16.
[28] ibid 17.
[29] ibid 17.

and third-party exposures; business interruption; data and software loss; and regulatory notification expenses.[30]

Originally, cyber extortion and ransomware used to be covered under kidnap and ransom (K&R) policies, but that stopped being the usual practice in the 2010s.[31] Then, such risks began to be covered under standalone policies with specific limits until broader cyber insurance products started to be developed, offering coverage for most kinds of risks as a package.[32]

Taking out a cyber insurance policy may be a bit harder than it used to not long ago. Until 2019, "ransomware was not a major problem for the cyber insurance market".[33] The risk appetite was significantly larger, and the underwriting process did not require high standards of cyber security for a company to be insured.[34] This changed between 2020 and 2021 – with a fair share of blame given to the COVID-19 pandemic that demanded remote working across the world and contributed to lower cyber security standards[35] –, when the number of ransomware attacks increased, and the criminals started to cause alarming business interruptions.[36] Since then, whilst some insurers backed out from underwriting cyber, others completely changed their approach on how to do it. This resulted in higher premiums, more limited coverages, specific security requirements, and exclusions that did not exist before.[37]

It could be argued that this new approach made the purchase of cyber insurance harder, especially for small and medium businesses, but it also reflects the intention of the market to reduce the risk of ransomware and to create a sort of self-governance process for companies buying cyber insurance, so that they can be aware of their cyber security practices and take the necessary measures to improve it.[38]

From a practical perspective, cyber insurance policies are said to play a critical role in incident response during a ransomware attack, helping the insured recover compromised data and resume operations as quickly as possible – which is one of its main purposes. That is because many cyber products require that incident response plans be set out even before coverage attaches.[39] Such a plan includes access to pre-approved service providers, for instance, of data forensics to investigate the cause of the attack, crisis management, ransomware negotiation, specialist attorneys, public relations agencies, and other types of services that might be needed to guarantee an effective incident response. This is said to be a very attractive

[30] ibid 18.
[31] Tom Baker and Anja Shortland, 'Insurance and Enterprise: Cyber Insurance for Ransomware' [2022] The Geneva Papers on Risk and Insurance - Issues and Practice 283, <http://dx.doi.org/10.1057/s41288-022-00281-7> accessed 24 August 2023.
[32] MacColl and others (n 25) 18.
[33] ibid 19.
[34] ibid 20.
[35] *Cyber Threat Report: UK Legal Sector* (National Cyber Security Center 2023) 8 <www.ncsc.gov.uk/report/cyber-threat-report-uk-legal-sector> accessed 24 August 2023.
[36] MacColl and others (n 25) 21.
[37] ibid 21.
[38] ibid 21.
[39] ISG Tech, 'Cyber Insurance. And the War on Ransomware. - ISG Technology' (*ISG Technology*, 27 September 2022) <www.isgtech.com/cyber-insurance-and-the-war-on-ransomware/> accessed 24 August 2023.

feature of this kind of insurance, especially for small and medium businesses, that perhaps could find some difficulties in responding to an incident without proper support.[40]

Normally, upon becoming aware of a ransomware attack, the insured is advised to notify the Incident Response Manager (IRM) named in the policy – usually a third-party law firm that operates a "24/7 hotline" to receive those kinds of notifications –, which will then triage the incident and suggest hiring the necessary companies from the pre-approved panel of service providers to deal with the incident.[41] From the earliest moments after the attack is noticed and notified, the IRM appointed by the insurer will coordinate the necessary actions to make sure that the incident is properly dealt with and that the insured is supported. It is important that the insured is fully aware of all coverages and services that a cyber policy can offer, in order to allow a quick response. On that note, research has revealed that policyholders tend not to properly utilise the loss prevention services offered by their policies[42], which is why it could be valuable for insurers to invest on educating their clients as to the benefits that their product provides. If, in turn, the insured decides to appoint their own vendors and not use the pre-approved panel, they might need to seek for prior approval of the insurer, which might delay the response.

Another key purpose of cyber insurance policies, as can be expected, is to cover the losses borne by the insured in result of the incident. Normally, these policies offer coverage for first-party risks, being the costs incurred directly by the insured (in restoring the lost data, IT forensics, notifications to third-parties, as well as the loss of revenue due to business interruption, for example), and third-party risks, being the damages that the insured might have to pay as compensation to customers who might have had their data exposed by the hackers.

On another note, it pays to point out that although insurers might engage in the incident response alongside their insureds, the decision on whether to pay out a ransom demand is not made by them.[43] This is important because, as it will be seen in the sections below, some critics suggest that, during a ransomware incident, insurers tend to conduct a cost-benefit analysis and recommend paying the ransom rather than supporting the recovery of data, which could potentially be a more costly resolution – therefore, arguing that the insurance industry is fuelling ransomware.[44] However, even though insurers might sometimes opt for more cost-effective outcomes – as they are part of a "for-profit industry" –, research has shown that the decision on whether to pay or not is ultimately of the insured.[45]

In addition, although insurers are less subject to the Financial Conduct Authority's (FCA) anti-money laundering rules than other entities[46], they still need to implement measures to avoid financial crime, as the

[40] MacColl and others (n 25) 18.
[41] ibid 19.
[42] Baker and Shortland (n 31) 293.
[43] ibid 24.
[44] Renee Dudley, 'The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks' [2019] ProPublica <www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks> accessed 24 August 2023; and MacColl and others (n 25) 24.
[45] MacColl and others (n 25) 25.
[46] FCA Handbook, Financial Crime Guide, 3.1.3: This guidance is less relevant for those who have more limited anti-money laundering (AML) responsibilities, such as mortgage brokers, general insurers and

Proceeds of Crime Act 2002 is still applicable and mandates the reporting of suspicious activities. This is an important remark because, just like victims of ransomware, insurers are not currently obliged to report ransomware payments to authorities unless they know or suspect, or they have reasonable grounds for suspecting that money laundering is taking place.[47]

In this regard, section 330 of the Proceeds of Crime Act 2002 establishes that a person working in a regulated sector, such as the insurance market, commits an offence where (i) they know, suspect or have reasonable grounds for knowing or suspecting that another person is engaged in money laundering; (ii) the related information came to them in the course of a business in the regulated sector; (iii) they can identify the person or laundered property involved; and (iv) they do not properly disclose it as soon as is practicable after they become aware of it.

As it was seen in this section, the dynamics of how a cyber insurance policy should work upon the occurrence of a ransomware attack demonstrates that it performs a highly important role in the incident response and, consequently, in the extent of losses, given that, the faster the response facilitated by the policy's features, the lower the potential exposure to damages for both the insured and third parties.[48]

3. The Legality of Ransomware Payments and its Insurance Coverage

As seen in the previous sections, ransomware attacks are currently an important threat that is haunting public and private sectors across the globe.[49] Currently, insurance cover is available for the risk of such incidents, including cover for ransom demands, which has attracted critiques from academics and market commentators in the sense that cyber insurance against ransomware is serving as an incentive for criminals, and that the insurance industry is benefiting from the growth in such cybercriminal activity.[50]

As Logue and Shniderman point out, "[t]he concern is that the presence of insurance is making the ransomware problem worse", and it is what is making the number of attacks increase[51], which is why they propose that this kind of coverage should be prohibited by law. Lubin, on a similar note, remarks that "Each of these payments helps fuel the criminal enterprise behind ransomware, thereby inviting further attacks."[52]

This leads to the following set of questions: are cyber insurance policies that cover ransomware demands incentivizing criminal activity? If so, how should the law and insurance companies work to address this

---

general insurance intermediaries. But it may still be of use, for example, to assist them in establishing and maintaining systems and controls to reduce the risk that they may be used to handle the proceeds from crime; and to meet the requirements of the Proceeds of Crime Act 2002 to which they are subject.

[47] MacColl and others (n 25) 71.

[48] ibid 19.

[49] MacColl and others (n 27, 28 and 29).

[50] Dudley (n 44); and Victoria Hudgins, 'Rising Ransomware Attacks Spur Debate Over Whether Cyber Insurance Is to Blame | Legaltech News' (*Legaltech News*, 4 December 2020) <www.law.com/legaltechnews/2020/12/04/rising-ransomware-attacks-spur-debate-over-whether-cyber-insurance-is-to-blame/?slreturn=20230724061143> accessed 24 August 2023.

[51] Kyle D Logue and Adam B Shniderman, 'The Case for Banning (And Mandating) Ransomware Insurance' [2021] SSRN Electronic Journal 251, <http://dx.doi.org/10.2139/ssrn.3907373> accessed 24 August 2023.

[52] Asaf Lubin, 'The Law and Politics of Ransomware' [2022] 55 Vanderbilt Journal of Transnational Law 1185, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4181964> accessed 24 August 2023.

unintended effect? Or, instead, should it be illegal to pay ransoms to cyber criminals, and, consequently, to provide insurance cover for such a risk?

The subsequent section will present an overview in relation to the current legality status of ransomware payments and its insurance cover, followed by arguments that support the cases against and for the legality. In the end, this section concludes with alternatives to making ransom payments by victims and insurers illegal.

3.1 Are ransomware payments and insurance illegal?

Currently, there are no precedents in English case law which have expressly considered whether it is legal to pay a ransom demand arising from a cyberattack. Nonetheless, it is possible to draw an analogy from maritime cases involving the payment of ransom requests arising from piracy, as the element of extortion is present in both situations, as well as other characteristics.

In *Masefield AG v Amlin Corporate Member Ltd (The Bunga Melati Dua)* [53], for example, Lord Justice Rix confirmed that '[t]here is no legislation against the payment of ransoms, which is therefore not illegal'. To support such a conclusion, he referred to Arnould[54] and the Royal Boskalis[55] appellate judgment:

> "There appears to be little doubt that where a payment which is not illegal itself under any relevant law is made to secure the release of property, this can be recovered even though the persons demanding the payment are not acting lawfully in so doing. Thus, for example, payment to recover property from pirates or hijackers must, it is submitted, in general be recoverable."[56]

It is also worth noting that UK Courts have not questioned the legality of ransomware payments and the relevant insurance cover when they came across the subject. For example, in AA v Persons unknown[57], an English insurer requested a proprietary injunction in respect of the Bitcoins used by said insurer to pay a ransom demand received by its insured, who had been a victim of a ransomware attack. Not only the Court did not question the legality of such payment, but it also recognized that the insurer was subrogated on the rights of the insured because of it.[58] It is true that the legality of the payment was not the central issue of the case, but the fact that it was not disputed by the Court allows us to conclude that, so far, English courts may recognize that it is not against the law.

From a governmental and regulatory perspective, the conclusion is the same. In a joint letter from 2022, the UK's National Cyber Security Centre (NCSC) and the Information Commissioner's Office (ICO)

---

[53] [2011] EWCA Civ 24; [2011] 1 WLR [63-64].
[54] Arnould's Law of Marine Insurance and Average (17th edn, Sweet & Maxwell, 2008) para. 25-21
[55] [1999] QB 674
[56] Gotthard Gauci, 'Total Losses and the Peril of Piracy in English Law of Marine Insurance' (2012) 11(1) WMU Journal of Maritime Affairs 118-119, <http://dx.doi.org/10.1007/s13437-012-0024-3> accessed 24 August 2023.
[57] [2020] 4 WLR 35
[58] AA v Persons unknown [2020] 4 WLR 35 [51].

confirmed that the payment of ransom demands is not unlawful, but also stated that law enforcement does not encourage nor endorse it.[59]

But there are some exceptions. Paying a ransom could constitute a criminal offence if it violated the provisions of the Terrorism Act 2000, the Proceeds of Crime Act 2002, or the Sanctions Act 2018.

The Terrorism Act makes it an offence for a person to provide money or other property if that person knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism (Section 15 (3)).[60] Although the threat of cyberterrorism is a real one, not every cyberattack is made with terrorism purposes, so as to be caught by this provision. In general, the nature of most of the attacks seen so far seems to be related to criminals acting purely for personal gain – given that ransomware has become a very profitable business, as demonstrated earlier[61] –, rather than to intimidate or coerce a government or its people for political or social objectives.[62] For this reason, unless a victim of cyber extortion has clear indications that an attack is related to terrorism, paying the ransom demand would not constitute a breach of this law. Considering that, in most cases, the identity of the cybercriminals is unknown, there may be no actual knowledge or "reasonable cause to suspect" that the extortion is being brought by someone related to terrorism. Therefore, it could be safe to presume that there is no link to terrorism in the absence of evidence to the contrary.[63]

The Proceeds of Crime Act considers it a money laundering offence for a person to engage in an arrangement that they know or suspect to facilitate (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person (Section 328 (1)).[64] However, money used for the payment of a ransom demand will only become criminal property when it reaches the hands of the attackers. Before that, if the money was not the proceeds of crime[65], the person using that money would not be in breach of the Proceeds of Crime Act.[66] Therefore, it is rather unlikely that a company which is a victim

---

[59] John Edwards and Lindy Cameron, *The Legal Profession and Its Role in Supporting a Safer UK Online* (Information Commissioner's Office and National Cyber Security Centre 2022) <https://ico.org.uk/media/about-the-ico/documents/4020874/ico-ncsc-joint-letter-ransomware-202207.pdf> accessed 24 August 2023.

[60] European Union Committee, 'The Law in the UK on Ransom Payments (Money Laundering and The Financing of Terrorism)' (*UK Parliament*, May 2009) [7], <https://publications.parliament.uk/pa/ld200809/ldselect/ldeucom/132/9031112.htm#:~:text=The%20person%20or%20group%20of,terrorist%20financing%20offence%20being%20committed> accessed 24 August 2023.

[61] MacColl and others (n 27).

[62] Gabriel Weimann, *Cyberterrorism How Real Is the Threat?* (United States Institute of Peace 2004) 5, <www.usip.org/publications/2004/05/cyberterrorism-how-real-threat> accessed 24 August 2023.

[63] Felix Zimmermann and Kirsty Oliver, 'The Legality of Cyber Extortion Payments' (*Simmons & Simmons*, 14 December 2018) <www.simmons-simmons.com/en/publications/ck0ahwpb0ncm30b369kyk8e7o/131218-the-legality-of-cyber-extortion-payments> accessed 24 August 2023.

[64] European Union Committee (n 57) [3].

[65] Criminal property is defined by Section 340 (3) of the Proceeds of Crime Act 2002 in the situations where "(a) it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly), and (b) the alleged offender knows or suspects that it constitutes or represents such a benefit.".

[66] 'Ransomware: To Pay or Not to Pay?' (*Osborne Clarke International Legal Practice*, 16 February 2021) <www.osborneclarke.com/insights/ransomware-pay-not-pay> accessed 24 August 2023.

of cyber extortion paying a ransom demand would be in breach of those provisions, unless proven that the origin of the money to pay the ransom was illegal in the first place.

Finally, a ransom payment could also constitute an offence if it were made to an individual that is included on the lists published by the OFSI – Office of Financial Sanctions Implementations, which can be easily avoided by conducting reasonable due diligence and checking those lists in advance.[67] On this note, the Lloyd's Market Association has published the 'Guidance for handling a ransomware incident' which provides for recommendations of the steps that should be taken by insurers in the due diligence process if payment is requested in a ransomware incident[68], which should contribute to avoiding payments to sanctioned individuals or entities.

There are plenty of arguments to support different views on the legality of ransomware payments and the presence of insurance for it, as the literature highlights both benefits and drawbacks of both scenarios. In order to answer the proposed questions, the following topics will assess some of those arguments and evaluate workable solutions to existing gaps in regulation and/or law enforcement.

3.2 The case against the legality

There is a theory that the availability of insurance for ransom payments in cyber incidents makes the number of attacks increase and, therefore, that it should be illegal.[69] Moreover, that the existence of insurance makes ransomware attacks a victimless crime, as the loss that arises from it would be covered by an insurer. In truth, this argument is supported by the fact that cybercriminals are even asking for their victim's cyber insurance policies details, to make sure that their ransom demands are met.[70]

Another argument against ransomware payments is the uncertainty related to the decryption and recovery of the locked data, even after the payment is made, as sometimes files can get corrupted, and the information might be lost.[71] As priorly mentioned, statistics reveal that despite paying the ransom demand, victims only recover about 65% of the encrypted data.[72]

This is currently being discussed by many commentators[73], but specifically by Logue and Shniderman, in their article "The Case for Banning (and Mandating) Ransomware Insurance", whose arguments are going to be considered for the purposes of this part of the paper, in order to evaluate the basis of this theory and some of the proposed suggestions to address the issue.

---

[67] ibid.
[68] 'Guidance for Handling a Ransomware Incident' (*Lloyd's Market Association*, 10 December 2021) <www.lmalloyds.com/LMA/News/Blog/guidance_101221.aspx> accessed 24 August 2023.
[69] As previously quoted from Logue and Shniderman (n 51).
[70] Graham Cluley, 'HardBit Ransomware Tells Corporate Victims to Share Their Cyber Insurance Details' (*Tripwire | Security and Integrity Management Solutions*, 22 February 2023) <www.tripwire.com/state-of-security/hardbit-ransomware-tells-corporate-victims-share-their-cyber-insurance-details> accessed 24 August 2023.
[71] Aleksandar Kochovski, 'Ransomware Statistics, Trends and Facts for 2022 and Beyond' (*Cloudwards*, 23 April 2023) <www.cloudwards.net/ransomware-statistics/> accessed 24 August 2023.
[72] Bourne (n 10) 11.
[73] Such as Logue and Shniderman (n 51) 247; Dudley (n 44); Hudgins (n 50); and Lubin (n 52) 1185.

Logue and Shniderman argue that, because there is insurance for ransom payments and because paying those demands is usually cheaper than bearing the costs of business interruption and restoration of the encrypted data, victims often prefer to simply pay the ransom, in amounts that are increasing as the time goes by because the existence of insurance is known by the hackers, which creates an incentive to engage in ransomware attacks and, consequently, an increase in the demand for insurance, driving insurers to charge higher premiums.[74]

In response to that, the idea proposed by the authors is, first, to implement a ban on insurance coverage for ransomware payments, with the exception for situations that could involve substantial threat to human health or life. They justify this proposal by arguing that, if it were illegal to pay ransom demands, under the penalty of heavy fines, the amounts asked by cybercriminals would diminish and so would their incentive to engage in ransomware activities in the first place.[75]

Second, they suggest the creation of a government subsidy to encourage the purchase of cyber insurance by means of a mandate that all cyber insurers offer coverage in standalone policies with reasonable amount of coverage (higher than what is currently offered) related to the other costs of ransomware attacks, such as the costs for recovering the encrypted data, and the losses related to business interruption and liability to third parties.[76]

The logic behind their proposal is that both the ban on ransomware insurance and the government subsidy could work together to reduce the profitability of ransomware attacks, as from one side, the ban on insurance would reduce the resources of those who would be inclined to pay the ransom demand, and from the other side the subsidy would increase the resources of those who would refuse to pay it.[77] As a result, cybercriminals would not profit as much as they do with ransomware activities, which would lead to reducing the number of attacks, and, consequently, the costs for the proposed program.[78]

Even though the proposals seem reasonable and are well-supported from both legal and economical perspectives, some obstacles still exist in making them work as intended. First, because hackers commonly adopt double extortion strategies, and this is an important thing to consider.[79] The proposed ban on ransom payments and insurance would not eliminate the civil and administrative liability that could arise to the victim (i.e. the insured) from the exposure of the stolen data that belongs to third parties. In these cases, the ransom payment could be the only way to prevent the data being leaked.

At the same time, it is fair to say that there is no guarantee that the hackers would refrain from exposing the data just because paying the ransom demand is illegal. In fact, it could be argued that, because of the huge exposure faced by victims of ransomware in relation to the leakage of data, they would consider paying the ransom even under the risk of being heavily penalized for it, to minimize the overall loss.

[74] Logue and Shniderman (n 51) 247.
[75] ibid 255 and 304.
[76] ibid 258 and 305.
[77] ibid 305.
[78] ibid 305.
[79] Fearn (n 4).

For example, in relation to the civil liability exposure, any individual who believes that their rights under the UK's Data Protection Act have been breached is entitled to claim compensation for any damage suffered, pursuant to Section 168 of said Act.[80] Research has shown that the amounts of compensation can get from £2,000 up to £42,900, depending on the seriousness of the breach and the nature of the exposed data.[81] Depending on the number of victims of the data breach, the financial exposure of the insured could be significant.

The insured could also face an administrative penalty for infringing the provisions of the Data Protection Act, which, pursuant to Section 157 (5), can get to the higher maximum amount of £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year of the company, whichever is higher.[82]

Second, from a more practical point of view, without the possibility to pay the ransom, the insured could be exposed to even longer business interruptions, and, consequently, higher amounts of losses arising from it. Even if the coverage for recovery costs turned out to be higher than what is currently offered, truth is that no insurance policy is unlimited, which could still leave a gap of coverage, especially considering that the recovery costs and losses from business interruptions are already said to be a lot higher than the ransom demand.[83]

3.3 The case for the continued legality

While it is completely possible to understand the case against the legality of ransomware payments and its insurance coverage, on balance, it is submitted that no change to the law is required, as it will be explained in further detail below.

The defence of the continued legality of ransomware payments and insurance is supported by many points, to begin with the argument that making it illegal would not automatically solve the problem and discourage ransomware attacks. In fact, considering the commonly adopted tactic of "double extortion", victims are

[80] 168 Compensation for contravention of the GDPR (1) In Article 82 of the GDPR (right to compensation for material or non-material damage), "non-material damage" includes distress. (2) Subsection (3) applies where— (a) in accordance with rules of court, proceedings under Article 82 of the GDPR are brought by a representative body on behalf of a person, and (b) a court orders the payment of compensation. (3) The court may make an order providing for the compensation to be paid on behalf of the person to— (a) the representative body, or (b) such other person as the court thinks fit. In combination with the provision of Article 82 of the General Data Protection Regulation.

[81] 'UK GDPR and Data Breach Compensation: What You Need to Know.' (DataGuard, 2 March 2022) <https://www.dataguard.co.uk/blog/gdpr-and-data-breach-compensation-in-the-uk#:~:text=You%20have%20the%20right%20to%20file%20a%20data%20breach%20claim,hacked%2C%20misappropriated%2C%20or%20lost> accessed 24 August 2023

[82] (5) The "higher maximum amount" is— (a) in the case of an undertaking, 20 million Euros or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or (b) in any other case, 20 million Euros. Although the provision says 20 million Euros, the ICO has clarified the maximum amount in the UK currency, which is £17.5 million. (see 'Penalties' (ICO) <https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/penalties/> accessed 24 August 2023).

[83] Datto (n 14).

still going to be compelled to pay the ransom demand to avoid having their data exposed, even if it means using their own funds.[84]

Another relevant point is that many attacks target critical sectors, such as healthcare, water, energy, oil and gas, and public services in general (such as the judiciary). In these cases, being prohibited to pay a ransom demand not only would not be the answer, but it is possible that the government would even step-in and make the payment in order to avoid bigger losses or threats to human life or society's well-being if necessary.[85]

Even if there were an exception to the ban in relation to the situations where health and safety of individuals might be compromised because of the attack, as suggested by Logue and Shniderman[86], the practicalities of such an exception would seem to complicate more than resolve the issue. As suggested by said authors, having this exception would put a target on hospitals and other sensitive services' backs, as they would be the only entities allowed to pay the ransom without any concerns. Their proposed solution to this is that the ban should be a general one, with no explicit exceptions, except when priorly approved by the competent regulatory agency.[87] However, to impose the need for prior approval of the regulator appears to be an unnecessary obstacle in a life-threatening situation, as there would have to exist a proper procedure for obtaining the green light for payment, which could take time that probably would not exist in those kinds of scenarios.

A similar logic is applicable to businesses, especially SMEs, in the situation where the ransomware attack has caused a major disruption in the company's operation. In these cases, managers would not be able to afford extended periods of business interruption while they are trying to decrypt their data and would rather pay the ransom to avoid going bankrupt.[88] On that note, criminalizing ransom payments could be seen as a further punishment to businesses that only have that as the main alternative to recover their data and to avoid the exposure of third-party data.[89]

Additionally, it is worth remembering that cyber insurance plays an important role in the incident response. Specifically in relation to ransomware, the provision of specialized services by the insurer, such as the access to ransom negotiators or intermediaries, can be a valuable asset to the insured during the turbulence of a cyberattack.[90]

---

[84] Jon Hunt, Lisa Fitzgerald and Melissa Tan, 'Ransomware and Insurance: Is Cyber Insurance for Ransomware Problematic?' (*Lander & Rogers*, October 2021) <www.landers.com.au/legal-insights-news/ransomware-and-insurance-is-cyber-insurance-really-problematic> accessed 24 August 2023.
[85] Tom Baker and Anja Shortland, 'The Government Behind Insurance Governance: Lessons for Ransomware' [2022] Regulation & Governance 31, <http://dx.doi.org/10.1111/rego.12505> accessed 24 August 2023.
[86] Logue and Shniderman (n 51) 306.
[87] ibid 307.
[88] Baker and Shortland (n 81) 31.
[89] Laurie Clarke, 'Is Legislation the Best Defence Against Ransomware Attacks?' (*Raconteur*, 2 May 2023) <www.raconteur.net/risk-regulation/is-legislation-the-best-defence-against-ransomware-attacks#:~:text=A%20major%20argument%20against%20companies,recover%20all%20of%20their%20data> accessed 24 August 2023.
[90] MacColl and others (n 25) 18.

Hence, there seems to exist a number of reasons why making ransomware payments and their insurance coverage illegal would be quite a troubled measure, that could result in even more complications than solutions.

3.4 Alternatives to banning ransomware payments and insurance

Rather than simply establishing a ban, the UK Government could implement new measures intended to reduce the number of attacks and disincentivize this significant present-day criminal activity. This section will address some of these alternatives that have been suggested by academics and commentators on the subject.

Strengthen Cyber Security Regulations. There is no greater disincentive to cybercrime than being prepared for it and being able to avoid it from happening. It is certain that no enterprise is cybercrime-proof, but the more prepared they are, the lower the chances of suffering an attack. And cyber insurers play a key role in this regard, by incentivizing their insureds to invest in self-protection, which is often stimulated by premium reductions or imposing security-related conditions on the underwriting process[91], that is, if the insureds do not comply with specific cybersecurity requirements, they would not be eligible for cover.

Instead of banning insurance cover for ransom payments, the government could intervene to strengthen the regulation related to cybersecurity.[92] In the UK, there is plenty of legislation governing cybersecurity and data protection (such as the Data Protection Act 2018, the UK-GDPR and the Network and Information Security Regulations 2018)[93], as well as significant guidance from the NCSC on cyber resilience.

Nevertheless, although the provisions on those acts do impose some obligations requiring the implementation of technical measures to ensure an appropriate level of security[94] and the possibility of being certified for compliance with those obligations[95], there is still room for improvement in cybersecurity regulation to require the adoption of minimum cybersecurity standards by actually demanding the implementation of specific features[96] (such as multifactor authenticators, for example) and this could be done based on the size of the business – the bigger the company, the more security features they would have

[91] Tom Baker and Anja Shortland, 'How Crime Shapes Insurance and Insurance Shapes Crime' [2023] Journal of Legal Analysis 4, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4390802> accessed 24 August 2023.
[92] ibid 18.
[93] Kyle Chin, 'List of Cybersecurity Laws and Regulations in the UK' (*UpGuard*, 11 August 2023) <www.upguard.com/blog/cybersecurity-laws-regulations-uk> accessed 24 August 2023.
[94] For example, Section 66 of the Data Protection Act 2018 and Chapter 4, Section 2, Article 32 of the UK-GDPR.
[95] Chapter 4, Section 5, Article 42 of the UK-GDPR.
[96] Baker and Shortland (n 31) 290.

to adopt. The United States[97] and the European Union[98], for example, are both adopting measures in the field of cybersecurity, as the subject is becoming a matter of national security.

With more cyber security regulations in place, insurers could insist on the implementation of certain security measures and require evidence of compliance during the entire policy period as a condition of coverage or charge a higher premium and remedial action where this is not the case.[99] Such provision could be included in the policy in the form of a warranty, as it would be related to the insured undertaking to comply with certain security standards. In case of breach by the insured, coverage would be suspended until the breach has been remedied, but the insurer would not be able to avoid claims in circumstances where the breach was unrelated to the loss, pursuant to Sections 10 (2) and 11 of the Insurance Act 2015.

By acting this way, cyber insurers are, to some extent, turning the process of buying insurance into a process of self-governance to insurance buyers, and ultimately contributing to combating cybercrime, rather than fueling it.

Furthermore, insurers often offer limited cover to ransom demands.[100] This way, the insured will also have some skin in the game and, in a certain way, is incentivized to increase its own cybersecurity standards instead of simply relying on the existence of insurance in case an incident happens.

Strengthen Law Enforcement. Another approach to disincentivize cybercrime as opposed to simply banning ransomware payments and insurance would be by strengthening law enforcement against cybercriminals. The UK Government, through the National Crime Agency (NCA), promotes enforcement against ransomware threat actors, including the use of financial sanctions.[101]

The problem with bringing ransomware criminals to justice, however, is that more often than not they are not based in the UK and working from a different jurisdiction than their victims, and, usually, those jurisdictions might be less cooperative with cybercrime control, which compromises law enforcement in significant levels.[102] The question, then, is: how to make law enforcement more effective in order to disincentivize ransomware attacks?

An initial proposal would be for UK lawmakers to enact an obligation to report to the competent agencies any ransomware payments knowingly made by entities based in the UK, under the risk of financial penalties

---

[97] Felicia Jafferies and Amanda Brazinski, "Navigating the Patchwork of U.S. Privacy and Cybersecurity Laws: Key Regulatory Updates From Summer 2023" (Reuters, 09 October 2023) <www.reuters.com/legal/litigation/navigating-patchwork-us-privacy-cybersecurity-laws-key-regulatory-updates-summer-2023-10-09/#:~:text=On%20July%2026,%202023,%20the,cybersecurity%20risk%20management%20procedures%20and> accessed 21 October 2023.

[98] European Union, "Commission Welcomes Political Agreement on New Rules to Boost Cybersecurity in EU Institutions, Bodies, Offices and Agencies" (*European Commission*, 26 June 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3483> accessed 21 October 2023.

[99] Baker and Shortland (n 31) 290.

[100] Baker and Shortland (n 31) 291-292.

[101] Office of Financial Sanctions Implementation (HM Treasury), "Ransomware and Sanctions: Guidance on Ransomware and Financial Sanctions" (2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1135587/Ransomware___Sanctions_guidance__Feb_2023_.pdf> accessed 24 August 2023.

[102] Baker and Shortland (n 31) 286-287.

being applied in case of non-compliance.[103] Because it is currently not mandatory, victims of cybercrime are less likely to report incidents and ransom payments to authorities[104] (probably for reputational reasons), which prevents law enforcement agencies from carrying out the necessary investigation in many cases. By making it mandatory, agencies would be able to develop more expertise and eventually start bringing those criminals to justice more often.

It would be important that such a duty includes insurance companies based in the UK that either pay ransom demands on behalf of their insureds or reimburses a ransom payment under the respective coverage. That is because sometimes the insured is not located in the UK, but the insurer is. This way, law enforcement agencies would be more certain about the compliance with the proposed duty.

In this regard, it would be key that insurers have the necessary means to conduct the ransomware reports. This is relevant because the research conducted by RUSI revealed that,

> "At present, the UK does not have a comprehensive framework for reporting and, significantly, tracking ransomware payments. One potential approach is to expand existing financial crime reporting mechanisms to generate insights on ransomware and more actively involve insurers in reporting. Intelligence about ransom payments could be provided through suspicious activity reports (SARs) to the NCA's Financial Intelligence Unit. However, while regulated institutions are required to file a SAR if they detect suspicious behaviour, it is currently not possible to 'code' the SAR as money laundering related to ransomware (although it is possible to code a SAR as relating to virtual assets).280 Moreover, insurers are not currently covered by existing FATF recommendations and UK money laundering regulations, and so may not feel obliged to report. In view of this, the government should explore modifying SARs to incorporate ransomware and find ways to integrate insurers and specialist ransomware response services into financial crime reporting mechanisms."[105]

The same RUSI report indicates that, currently, only two UK cyber insurers require that the insured notifies law enforcement prior to making a ransom payment.[106] Therefore, in addition to making the report mandatory, it should be legally established that coverage for a ransomware payment claim under a cyber insurance policy should be conditional on the insured notifying the incident to the competent agency (i.e. the NCA) and cooperating with law enforcement.

This could have the potential to enhance the number of reports from ransomware victims to law enforcement, specially from those who have purchased cyber insurance and would like to seek coverage, and ultimately increase intelligence around ransom payments and the operation of cybercriminals which could contribute to the success of law enforcement in bringing those criminals to justice.

---

[103] Baker and Shortland (n 31) 294.
[104] Joanna Curtis and Gavin Oxburgh, "Understanding Cybercrime in 'Real World' Policing and Law Enforcement" [2022] The Police Journal <https://doi.org/10.1177/0032258X221107584> accessed 24 August 2023.
[105] MacColl and others (n 25) 71-72.
[106] ibid 58.

Regulate Cryptocurrencies. As Trautman and Ormerod point out, "The anonymity of cryptocurrencies provides obvious benefits to those seeking to mask payments for such things as armaments, ransom, or bribes to officials of foreign governments."[107] In this context, another way of making the pursuit of criminals more effective would be by regulating cryptocurrencies to disrupt the payment process and make it traceable.[108]

Despite the challenge that cybercrimes being committed from different jurisdictions pose to law enforcement, making payments less secure to criminals by de-anonymizing cryptocurrency transactions could increase the success rate in identifying those criminals, and it could work as a compelling disincentive to ransomware attacks without the need to ban payments of ransom demands and cyber insurance.

Similar to the proposed obligation of reporting ransomware attacks, this approach to de-anonymize cryptocurrency transactions would have to apply to the transactions made by entities in the UK, including insurers that might eventually pay ransoms on behalf of their insureds using cryptocurrencies – as previously seen in *AA v Persons unknown*, for instance –, as well as any specialized company appointed by the insurer to assist the insured in the negotiations with the hackers and/or the intermediation of the ransom payment.

Ideally, this measure would follow the same steps as the ones recently adopted by the European Union, that implemented new rules requiring crypto asset service providers to collect and make accessible certain information about the sender and the beneficiary of transfers with cryptocurrencies, aiming to better identify suspicious transactions.[109]

Conclusions

There is no question that the law should work in a way that it does not promote or incentivize crime. However, as is evident from the above discussion, serious doubts have been raised on whether banning the payment of ransom demands and the existence of insurance for it would actually reduce the number of attacks, let alone put an end to ransom requests. In fact, Shortland and Baker suggest that "The overall effect of a ban is thus questionable: the crime would continue and become more damaging. Companies that fail after (unresolvable and uninsurable) ransomware incidents would likely lobby for bail-outs (…)".[110]

As it was argued in this paper, ransomware payments and insurance should not be made illegal. Instead, it is possible to address the issue relative to cyber insurance allegedly acting as an incentive to ransomware by imposing new duties on insurers when they are involved in a ransom payment, which could have the potential to reduce the number of attacks and improve the results of law enforcement.

---

[107] Lawrence J. Trautman and Peter C. Ormerod, "Wannacry, Ransomware, and the Emerging Threat to Corporations" [2019] 86 Tennessee Law Review 540 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3238293> accessed 24 August 2023.
[108] Baker and Shortland (n 81) 31.
[109] Council of the European Union, 'Anti-Money Laundering: Council Adopts Rules Which Will Make Crypto-Asset Transfers Traceable' (16 May 2023) <https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/anti-money-laundering-council-adopts-rules-which-will-make-crypto-asset-transfers-traceable/> accessed 24 August 2023.
[110] Baker and Shortland (n 81) 31.

In reality, cyber insurance should be used as a weapon against ransomware attacks, as it allows not only a faster recovery of the insured's operation, but also the development of intelligence, for example, on how these cyberattacks are perpetrated, how the negotiations with criminals are carried out, or what sort of cybersecurity features are working to stop the attacks, which could be used to cooperate with law enforcement. The knowledge base that insurance companies can develop by working on these kinds of incidents can be unbelievably valuable to lawmakers and law enforcement agencies in their efforts to achieve better results.

As it was suggested, cyber insurers, together with lawmakers, could draw upon this expertise to develop and establish stronger cybersecurity standards, in order to reduce vulnerability to attacks in the first place.

Currently, ransomware attacks are successful not only because there are no specific and mandatory cybersecurity standards, but because there is a very low risk of criminals being caught by enforcement agencies. In response to that, the law needs improvement to disincentivize cybercriminals, as suggested, by mandating the reports of incidents and ransom payments made by any UK entity, which would increase the number of investigations, as well as by regulating cryptocurrencies and making transactions involving UK entities more easily traceable.

It is also important to note that a law that bans ransomware payments and the existence of insurance against it would not be completely effective, mainly for three reasons. One, because a victim of a ransomware attack in danger of going bankrupt due to business interruption would find the necessary way to pay the ransom demand in order to save their business, even if it means acting illegally or suffering financial penalties. Two, because a local ban on insurance coverage for cyber extortion would not prevent companies from seeking and contracting cover in other jurisdictions that are more accommodating to this issue. And three, because making ransom payments illegal would not eliminate the threat to expose stolen data, which could represent significant liability to the victim of the attack as the controller of such data.

Thus, the arguments in favour of the legality of ransom payments and the existence of insurance cover for it seem to be more persuasive than the arguments against it. Whether the UK Government should make any changes to the law in this regard would require further research and even further data and statistics. Nevertheless, this paper summarized a few suggestions that have been made by other academics and entities researching the subject, which could be adopted by the UK Government to improve the current situation around the legality of ransomware payments and the respective insurance.