European Journal of Risk Regulation (2023), **14**, 382–398
doi:10.1017/err.2022.45

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

The Uneasy Case for a Ransom Tax

Bernold Nieuwesteeg[1]* and Michael Faure[1,2]

[1]Erasmus Universiteit Rotterdam, School of Law, School of Law, Burgemeester Oudlaan 50, Rotterdam, 3062 PA, The Netherlands and [2]Maastricht University, METRO, Bouillonstraat 1-3, Maastricht, 6211 LH, The Netherlands
*Corresponding author. Email: nieuwesteeg@law.eur.nl

Abstract

The goal of our paper is to demonstrate the potential effects of a tax on paying a ransom on the incentives of stakeholders involved: both the perpetrators (the attackers placing the ransomware) as well as the potential victim. We do think that there is a case for a ransom tax, but we do also realise that it is not easy to make that case, and hence we express this doubt in our title. A tax could stimulate ex ante cybersecurity and also (when price elasticity is not too low) reduce ex post ransom payments. In addition, a tax in combination with a smartly designed subsidy could have benefits.

Keywords: cyber insurance; cyber risk; cybersecurity; ransomware; taxation

I. Introduction

Over the past few years, we have seen a surge in ransomware attacks with an increasing economic impact.[1] Organisations confronted with a ransom demand can either pay, negotiate a lower price or refrain from paying.[2] Currently, organisations compare the private costs and benefits of these three options.[3] The cost of paying obviously concerns the price of the ransom demand.[4] In this case, organisations can often use tax deduction because ransomware is considered as a cost of doing business.[5] The cost of negotiation concerns invested time and possibly also an incident response service that manages the negotiation. After negotiation, the result will still be either a payment of a ransom (but potentially a

[1] DW Woods and R Bohme, "How Cyber Insurance Shapes Incidents Response: A Mixed Methods Study" (20th Workshop on the Economics of Information Security (WEIS) 2021).

[2] R Monroe, "How to Negotiate with Ransomware Hackers" (*The New Yorker, Annals of Technology*, 31 May 2021) <https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers> (last accessed 21 December 2022); B Nieuwesteeg, "To Negotiate or Not to Negotiate" (2021) 9 Data, Cybersecurity & Privacy 10.

[3] In this paper, we distinguish private cost and benefits from social costs and benefits in the sense that private costs and benefits are the costs and benefits for the actor that makes the payment decision and the social costs and benefits are the costs and benefits for society as a result of this decision.

[4] There may obviously be other costs, such as legislative compliance and reputation management, which will probably also slightly differ between the options.

[5] A Barber, "The Real Price of Paying Ransoms: The Australian Legal Position Concerning Ransom Payments to Terrorist Organisations" (2016) 41 The University of Western Australian Law Review 119. The discussion regarding tax deduction could also help to clarify the exact taxable status of ransomware payments, which we will further discuss in Section VI.

lower amount if the victim could bargain successfully) or not paying.[6] The cost of not paying concerns the cost of restoring the IT system to its previous state, which has a correlation with the ex ante security level of the organisation, such as the existence and age of backups.[7] In this paper, we will use the term "reparation cost" for all of the costs an organisation makes when it decides not to pay ransomware; this also includes, for instance, revenue loss and communication costs.

This paper focuses on this decision-making process. How can we ensure that an individual actor (either an organisation or an insurer), which now takes into account the repercussions of this decision for itself, makes a socially optimal decision? It is clear that negative externalities exist.[8] Paying a ransom demand reinforces the criminal business model, which increases the likelihood of future ransomware attacks.[9] Within the options to align the private optimum with the social optimum, we analyse the relatively unexplored territory of taxation. Does a tax on ransom payments align the private optimum of the payer with the social optimum? The goal of our paper is therefore to demonstrate the potential effects of a tax on paying ransom on the incentives of stakeholders involved: both the perpetrators (the attackers placing the ransomware) as well as the potential victim when an attack has occurred. The most important point is that the ex post reaction (eg the payment of the ransom) should not adversely affect incentives ex ante more particularly of the perpetrator. In this paper, we will focus on the professional hacker that executes ransomware attacks within a business model framework because the policy options we present (primarily taxation) are aimed at eroding this very business model.[10] We want to contribute to the literature and connect different fields of discussion regarding a ransom tax, including: the negative externalities of ransom payments; the relation of tax with regard to other policy options; the effect a tax can have on payment activity; and the interplay between a tax and a subsidy. We use a rational choice model and hence assume that perpetrators act rationally. We realise that the literature on this topic is scarce and therefore we will allow ourselves to touch upon a broad range of subtopics that, without doubt, need further research. We do think that there is a case for a ransom tax, but we do also realise that it is not easy to make that case, hence we express such doubt in our title.[11]

In order to answer these questions, we first need to establish what is best for society in the long term when organisations are confronted with a ransom demand. In order to do so, we first discuss the negative externalities ransomware payments create (Section II).

[6] In the remainder, we therefore only consider two options: either paying the ransom or the refusal to pay the ransom and so solving the consequences of the ransom oneself (or obviously with the help of third parties). After bargaining, there will therefore de facto only be two options: paying the ransom or refusing.

[7] When an organisation has purchased cyber insurance, which also covers the ransom, the cyber insurer will make the payment decision based on the private cost–benefit analysis of the cyber insurer. The cyber insurer incurs other costs and benefits from negotiation and not paying. The cyber insurer has probably easier access to incident response (less transaction costs), which makes it more likely that it will opt for negotiation instead of direct payment. In addition, the insurer can take into account the remainder of its insurance pool, which we will discuss later on in this paper.

[8] For a broader discussion on market failures in cybersecurity (externalities and information asymmetries), we refer to B Nieuwesteeg, "The Law and Economics of Cyber Security" (dissertation, Erasmus University 2018) and RJ Anderson, "Why Information Security Is Hard – An Economic Perspective" (Seventeenth Annual Computer Security Applications Conference 2001).

[9] Indication: "Law Enforcement Pressure Forces Ransomware Groups to Refine Tactics in Q4 2021" (*Coveware*, 3 February 2022) <https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021> (last accessed 13 October 2022).

[10] The occasional hackers that simply place the ransomware for fun or media attention (eg a script kiddie) or state actors that hack for disruptions fall outside the scope of this paper, for the simple reasons that these hackers usually do not have a business model and do not demand ransom.

[11] Following WJ Blum and H Kalven, "The Uneasy Case for Progressive Taxation" (1952) 3 University of Chicago Law Review 417.

Secondly, we discuss some policy options mentioned in the literature to provide incentives to parties to make more socially optimal choices when confronted with a ransom demand (Section III). Thereafter, we more elaborately discuss the option of a ransom tax by providing a brief review of the current literature regarding taxation in general and ransom taxation in particular (Section IV). Afterwards, we discuss price elasticity (Section V), practical and unique challenges (Section VI), present several scenarios (Section VII) and conclude (Section VIII).

II. Do ransom payments create negative externalities?

The starting point for our analysis is that a distinction has to be made between the private cost–benefit analysis executed by a victim of ransomware versus the analysis of the social costs and benefits. We will argue that there is a fundamental divergence between the private and the social motive to pay the ransom.[12] There are many other examples discussed in the law and economics literature where, because of a collective action problem (everyone enjoying the benefit but individuals not taking sufficient individual action), inefficiencies occur. This is the case, for example, with the installation of a LoJack security system in cars,[13] and it is also an explanation for the low demand for legal expenses insurance.[14] There are, in other words, also other situations where victims may abide with a criminal request, optimising private benefits but creating social costs.[15] If individual ransomware payments have no further impact on society, such as the security levels of other companies, criminal activity and future payments, the private optimum would equal the social optimum. The victim of the ransom attack would then weigh their private costs of not paying (repairing the damage caused by the ransomware itself or with the help of a third party) against the ransom demanded by the attackers. In that case, no policy interventions would be needed.[16] So, it is important to establish whether ransom payments create externalities (ie effects on others than the decision-maker; in this case, the victim of the ransomware).

It makes sense that paying ransom to cybercriminals reinforces their business model. If there were no payments at all, criminals would have no income and no incentive to carry out further attacks.[17] The payment of the ransom could be a negative externality (subsidising the criminal network), so refraining from payment could be considered as a positive externality (the beneficial effect for society of endangering the business model of the criminal network).

[12] Compare: S Shavell, "The Fundamental Divergence between the Private and the Social Motive to Use the Legal System" (1971) 26 Journal of Legal Studies 575.

[13] This is a small radio transmitter that is hidden in one of many possible locations within a car. In case of theft it can be activated in order to track the precise location and movement of the stolen vehicle. A decrease in the aggregate crime rate (positive externality) due to LoJack will not lead to sufficient benefits for the individuals who install LoJack, causing LoJack to be undersupplied in the market (I Ayres and SD Levitt, "Measuring Positive Externalities for Unobservable Victim Precaution: An Empirical Analysis of Lojack" (1998) 113 Quarterly Journal of Economics 43).

[14] See J De Mot, B Depoorter and M Faure, "The Multiplication Effect of Legal Insurance" (2016) 13(1) New York University Journal of Law & Business 1–31.

[15] It is a point also made, for example, by O Ben-Shahar and A Harel, "Blaming the Victim: Optimal Incentives for Private Precautions against Crime" (1995) 11(2) Journal of Law and Economic Organization 434.

[16] A Laszka, S Farhang and J Grossklags, "On the Economics of Ransomware" in S Rass, B An, C Kiekintveld, F Fang and S Schauer (eds), *Decision and Game Theory for Security, 8th International Conference, GameSec 2017, Vienna, Austria, October 23–25, 2017, Proceedings* (Berlin, Springer 2017) p 397.

[17] Assuming for a moment that these attacks are only carried out to extract a ransom from the targeted company or individual (there could of course be other non-directly economic motives such as the intention to create a disruption in the targeted company or agency). Those motives we do, however, disregard.

The mere existence of an external effect would, in our opinion, not be sufficient to justify significant policy interventions such as a prohibition or a tax. For this, the externalities of paying ransom need to be significant. What would be the size of the external effect in an individual case? In other words, what would be the impact of a single decision not to support the criminal business model?

We argue that the impact of not paying the fee demanded by the attackers depends on whether the attack is tailor-made or scattered.[18] Some cyberattacks are tailor-made, such as the targeted attack on Colonial Pipeline where apparently a compromised password was used.[19] Some cyberattacks are not directed at a single organisation but at vulnerabilities that are present in many organisations.[20] These attacks spread among organisations all over the world and will therefore not respond to particular ransomware policies in particular countries or sectors.[21] It would be fair to assume that there will be no collective worldwide decision to stop paying ransom and that there will always be ransomware payments in some sectors or some parts of the world. Therefore, for scattered cyberattacks, the decision of a single organisation, sector, insurer or even country not to pay could have a negligible impact on the total revenue of the attack. As an example of a scattered cyberattack, in the summer of 2021, Kaseya and its customers and the customers of its customers became victims of a ransomware attack executed by the REvil group. This caused disruption for many organisations, as Kaseya provided software that enabled its customers to enter the systems of their customers. Hence, the Kaseya hack is sometimes referred to as a "double supply chain" hack. The impact on refraining from a single ransomware payment on the criminal business model will only be high if a very significant portion of the victims decides not to pay.[22] Hence, the marginal social cost of ransomware payments differs according to the type of attack:

- A targeted attack on a single organisation (such as Colonial Pipeline): the positive externalities of not paying are high, since this eliminates the criminal revenue of a costly tailor-made attack.
- A scattered cyberattack such as supply-chain hacks (as in the Kaseya case): the impact of a single decision not to pay is relatively low because there are many victims.

Although the link between refraining from paying and eroding the criminal business model is not crystal-clear and may depend upon various elements such as the type of attack, we for now conclude that reducing the payment activity reduces the criminal activity by eroding the business model, But, as we discuss in the next section, even if there are limited externalities of paying ransom ex post (in some cases of scattered attacks), policy measures can have a positive impact on the ex ante security.

[18] KD Logue and AB Shniderman, "The Case for Banning (and Mandating) Ransomware Insurance" (2021) University of Michigan Law & Economics Working Papers 207 <http://hdl.handle.net/20.500.12424/4156072> (last accessed 4 July 2022).

[19] W Turton and K Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Password" (*Bloomberg*, 4 June 2021) <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password> (last accessed 4 July2022).

[20] B Barrett, "A New Kind of Ransomware Tsunami Hits Hundreds of Companies" (*Wired*, 2 July 2021) <https://www.wired.com/story/kaseya-supply-chain-ransomware-attack-msps/> (last accessed 4 July 2022).

[21] For instance, popular supply chain hacks have these consequences.

[22] In that way, not paying is different from the hostage analogy where a "not paying" statement/policy of a certain country/sector can indeed be very effective.

Table 1. Summary of the policy options (this scheme has the purpose to provide a brief overview, not to provide exact answers on the impact of the measures).

Policy option	Ex ante impact on security level?	Ex post impact on reducing ransom payments?	Feasibility
Ex ante subsidy	Yes	No	In principle feasible, but free-riding and moral hazard risks are present
Fostering cyber insurance	Yes, if insurers require this at a tailor-made level	Depends on the insurer policy and the size of the insurance pool	Cyber insurance is already present and some policies do not provide coverage for ransom payments, but the market is still developing
Prohibition	Yes	Yes	High evasion risk and practical enforcement challenges
Tax	Yes	Yes	Practical challenges, evasion and enforcement costs
Subsidies for ex post relief	Possibly negative, depending on the design of the subsidy	Yes	Free-riding and moral hazard risks are present, but potentially less than with ex ante security investment

III. Policy options to reduce ransom payments

In this section, we will review some known policy options to reduce the amount of ransom payments (Table 1). The assumption that comes with every policy option to reduce ransomware is that the payment increases the criminal activity. We will assume that the policy option to reduce ransomware payments at least leads to some of those positive externalities as discussed in the previous section. We discuss both the effect of the policy option on ex ante security levels (putting the organisation in such a position that it will have on average a lower reparation cost as a result of not paying) and on the ex post payment decision (influencing the payment decision after an attack happens). We use a rational choice model and hence assume that perpetrators act rationally.[23] Of course, a behavioural approach might provide additional explanations. It could be that the tendency, for example, to pay the ransom could also be based on particular biases. Within the scope of this paper we stick, for reasons of simplicity, to the rational actor model. Many of the stakeholders involved, both the perpetrators (ransomware gangs) as well as the victims, are often professionals. For those it can be assumed that they generally act as rational actors.[24]

1. Ex ante subsidies for technical preventative solutions

There is a large body of literature that focuses on technical solutions to mitigate the consequences of a ransomware attack.[25] We refer here to ex ante incentives in cybersecurity and, for example, preventing the damage from an attack by making additional backups. We are well aware that the reparation costs of a ransomware attack depend on many more

[23] Similar to Gary S. Becker in his analysis on irrational behaviour: GS Becker, "Irrational Behavior and Economic Theory" (1962) 70 Journal of Political Economy 1.

[24] See for instance: RS van Wegberg, BJ Klievink and MJG van Eeten, "Discerning Novel Value Chains in Financial Malware on the Economic Incentives and Criminal Business Models in Financial Malware Schemes" (2017) 23 European Journal on Criminal Policy and Research 574.

[25] AM Maigida et al, "Systematic Literature Review and Metadata Analysis of Ransomware Attacks and Detection Mechanisms" (2019) 5 Journal of Reliable Intelligent Environments 67.

factors, but we use the backup example throughout this paper. In this way, the cost of not paying a ransom can be reduced.[26] The mere existence of these solutions is often not enough because companies may lack information, have bounded rationality or have insufficient incentives due to the negative externality problem to invest in these ex ante security measures. Hence, there is ongoing discussion regarding subsidising technical cybersecurity.[27] The economic reasoning would be that the subsidy can constitute a nice "carrot"[28] and can generate positive externalities as society could generally benefit from the reduced risk of a cyberattack. The private costs of prevention could, however, be high, which may constitute an argument to subsidise this positive externality.

The potential danger of this subsidy is obviously (especially in the case of prevention costs being fully compensated) that it might create a free ride for the potential target company, which would then have its private cybersecurity financed by the taxpayer. That could equally create a moral hazard and reduce the incentive to consider the cost-effectiveness of the investments in cybersecurity. An overgenerous subsidisation of preventative technical solutions could create incentives for inefficient overinvestment. The argument in favour of ex ante preventative technical solutions is that they put the organisation in a better position when confronted with a ransom demand.[29] However, when an organisation is confronted with a ransomware attack and a ransomware payment is requested, which is the focal point of this paper, there is no time to implement technical solutions because they should have been implemented at a much earlier stage.[30]

2. *Fostering cyber insurance*

Insurers can internalise a part of the externality through their insurance pool and bear the higher cost of not paying because in the long term there will be lower ransomware activity in the entire insurance pool. However, often the pool is too small to fully internalise the externality. With multiple insurers in the market, the effect of not paying ransom would be a small reduction of ransomware attacks within one single insurance pool. And even if insurers reinsured cyber insurance or made a collective decision not to pay ransom, then there would still be many organisations that are not insured and would free ride on the costly decision not to pay ransom. This would result in underinvestment of the insurer. In practice, some insurers still pay ransom, although it is a measure of last resort.[31]

Would compulsory insurance then be an option? If there would be compulsory insurance and insurers would still be allowed to pay ransom, it would only partially internalise the externality, although there will be an information advantage in the negotiation phase. If there would be compulsory insurance and insurers would not be allowed to pay, this would potentially greatly increase premiums (as the costs for the insurer would obviously increase) and, moreover, organisations that "stand with their backs against the wall"

[26] E Cartwright, JH Castro and A Cartwright, "To Pay or Not: Game Theoretic Models of Ransomware" (2019) 5(1) Journal of Cybersecurity tyz009.

[27] X Wang, B An and H Chan, "Who Should Pay the Cost: A Game-Theoretic Model for Government Subsidised Investments to Improve National Cybersecurity" (Twenty-Eighth International Joint Conference on Artificial Intelligence, 2019) <https://personal.ntu.edu.sg/boan/papers/IJCAI19_Cyber.pdf> (last accessed 13 October 2022).

[28] G de Geest and G Dari-Mattiacci, "The Rise of Carrots and the Decline of Sticks" (2013) 80 University of Chicago Law Review 341.

[29] See for instance: J Thomas and G Galligher, "Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware" (2018) 11 Computer and Information Science 14.

[30] Compare in this respect the difference between ex ante precautions, ex post relief and ex post recovery in case of disasters: G Dari-Mattiacci and MG Faure, "The Economics of Disaster Relief" (2015) 37(3) Law & Policy 180.

[31] B de Waard, B Nieuwesteeg and L Visscher, "The Law and Economics of Cyber Insurance Contracts" (2018) 26 European Review of Private Law 371.

would arguably still privately pay ransom because the maximum pay-out of the insurer (the cap) would be lower than the reparation cost when not paying the ransom. Another major objection against compulsory insurance in an underdeveloped market is the high moral hazard risk when the transaction costs for the insurer to assess the cybersecurity level of the insured are high. This is the case regarding cyber insurance, but it equally applies to compulsory insurance for artificial intelligence.[32]

Insurers are also better able to lower the ransomware price by negotiation and thereby reduce the externality. They can assemble more expertise in ransomware payment negotiation because they are repeat players.[33] In connection with the prevision argument, insurers have access to better incident-response knowledge to assess the cost of paying relative to not paying ransom. This could potentially lead to relatively more frequent decisions not to pay. Lastly, cyber insurance can foster the implementation of ex ante security measures, which could increase the resilience of organisations in terms of cybersecurity.

Insurance of ransom payments is, however, debated for the simple reason – which is at the core of our paper – that the private benefits of insurance can obviously be high, but the social costs can be high as well because ransom payments are still being made. This is precisely the reason why policymakers now often take a position against such an insurance of ransom payments.

3. Prohibition of ransom payments and its insurance

Lately, there is increasing debate regarding the prohibition of ransom payments.[34] The prohibition includes either solely payments by insurers or payments by any organisation affected by a ransomware attack.[35] De facto, ransom payments are prohibited to some areas in the USA because they are considered enemies of the state.[36] In other jurisdictions there is a debate on prohibiting the insurance of ransom payments for the precise reason that this would feed the lifeline of criminal organisations. However, some consider banning ransomware payments to be unrealistic.[37] One problem is that enforcement of a prohibition of ransom payments (either by the attacked operator or by an insurer) may be extremely difficult, as it often happens "in the dark". It may be extremely difficult to discover that such a ransom payment was made. Moreover, the prohibition could also provide incentives not to disclose the ransom attack, whereas full disclosure might be

[32] M Faure and S Li, "Artificial Intelligence and (Compulsory) Insurance" (2022) 13 Journal of European Tort Law 1.

[33] M Galanter, "Why the 'Haves' Come Out Ahead: Speculations on the Limits of Legal Change" (1974) 9 Law and Society 95.

[34] B Nieuwesteeg et al, "Betaal geen losgeld bij een Ransomware aanval" (*FD*, 3 July 2021) <https://fd.nl/opinie/1390205/betaal-geen-losgeld-bij-een-ransomware-aanval-onl1cakh6F7i> (last accessed 4 July 2022); J Blaney and J Weiss, "Federal Legislation Considers Banning Ransom Payments to Hackers" (*JDSupra*, 17 June 2021) <https://www.jdsupra.com/legalnews/federal-legislation-considers-banning-5827069/> (last accessed 4 July 2022); J Breslow, "How to Stop Ransomware Attacks? 1 Proposal Would Prohibit Victims From Paying Up" (*NPR*, 13 May 2021) <https://www.npr.org/2021/05/13/996299367/how-to-stop-ransomware-attacks-1-proposal-would-prohibit-victims-from-paying-up?t=1645695847094> (last accessed 4 July 2022).

[35] Logue and Shniderman, supra, note 18.

[36] T Anscombe, "To Pay or Not to Pay? Legal or Illegal? These Are the Questions" (*Welivesecurity*, 8 July 2021) <https://www.welivesecurity.com/2021/07/08/ransomware-pay-not-pay-legal-illegal-these-are-questions/> (last accessed 4 July 2022). There are similar discussions when observing ransom payments for kidnapping, but here "there is a major disconnect between public statements on the policy of paying ransoms, the legality of paying ransoms, and what is actually done in practice". S Kazmir, "The Law, Policy, and Practice of Kidnapping for Ransom in a Terrorism Context" (2015) 48 International Law and Politics 325.

[37] I Bryan, "Verzekeraars verbieden om losgeld te vergoeden is slecht voor cyberveiligheid" (*FD*, 24 September 2021) <https://fd.nl/opinie/1413644/verzekeraar-verbieden-om-losgeld-te-vergoeden-is-slecht-voor-cyberveiligheid-kol1cakh6F7i> (last accessed 4 July 2022).

important to prevent others from falling victim to the same ransomware attack – in other words, in order to reduce social costs.[38] Moreover, the cost of not paying ransom could be too high for some organisations because they might not have adequate cybersecurity such as backups. The organisation has no option but to pay to retrieve their data, which makes the prohibition option less feasible. In cases where the private cost of non-payment would be so high that it would de facto lead to a complete shutdown of operations, this could lead to high, potentially even unacceptable socio-economic costs, which may make this option politically very difficult. One of the reasons a ransom tax can be proposed is because a prohibition is deemed not feasible for these reasons.[39] Normally it is the other way around. One often first starts with taxation and sometimes ends with a prohibition.[40] The reason to start with taxation is that it is, according to the pyramid of regulation, considered as a market solution. After all, a taxation does not prohibit the particular activity (ie the payment of the ransom), but simply allocates a price to the behaviour.[41] It is for that reason that a tax is considered a market-based system as it simply taxes the externality but leaves it to the market to internalise it.[42]

4. A ransom tax

A tax is therefore considered as a milder alternative than a prohibition (ie a ban). A tax poses an additional price on the harmful activity of paying ransom. It would shift the balance from paying ransom to not paying by internalising the negative externalities that come with paying the ransom as an additional cost. A tax is a classic remedy that has been advanced as the solution to internalise externalities (eg in the environmental area). The idea is that the externality can be reduced to socially desirable levels by increasing a firm's marginal private costs by means of a tax to reflect the marginal costs to society.[43] Since we are not, as such, looking at the social optimum that internalises the marginal social cost of paying ransom but rather are trying to find a suitable way to deter organisations from paying ransom, the goal of the tax is clearly deterrence. In the next section we will further develop this point.

5. Subsidies for ex post relief

We have already indicated that a subsidy could be provided for ex ante investments in preventing an attack (increased cybersecurity) or in mitigating the damages in case of an attack (investing in adequate backups). We indicated that this solution has particular benefits (of generating positive externalities) but substantial disadvantages of free-riding and moral hazard. The argument for a subsidy for ex post relief (assistance in kind or cash for not paying the ransom) is much stronger: the problem is that the attacked operator needs, under the pressure of having to resume its activities, to make a decision on whether

[38] This could be mitigated by making disclosure mandatory, possibly similar to the data breach notification system. However, enforcement of these notification schemes is not an easy task; see for instance: B Nieuwesteeg and M Faure, "An Analysis of the Effectiveness of the EU Data Breach Notification Obligation" (2018) 34(6) Computer Law & Security Review 1232.

[39] Compare the analysis of Kazmir into the prohibition of paying ransom in the case of "offline" kidnapping, although it is often unclear whether these laws are enforced. Kazmir, supra, note 36.

[40] "New Zealand to Ban Cigarettes for Future Generations" (*BBC News*, 9 December 2021) <https://www.bbc.com/news/world-asia-59589775> (last accessed 4 July 2022).

[41] Compare: R Cooter, "Prices and Sanctions" (1984) 84 Columbia Law Review 1343.

[42] J Freeman and C Kolstad, *Moving to Markets in Environmental Regulation: Lessons from 20 Years of Experience* (Oxford, Oxford University Press 2007).

[43] MG Faure and RA Partain, *Environmental Law and Economic. Theory and Practice* (Cambridge, Cambridge University Press 2019) p 132.

to pay the ransom or to fund the private costs of restoring its systems. If its private costs are higher than the ransom demanded, the operator might tend to pay the ransom, which precisely creates the negative externalities that are the focus of our paper. Subsidising ex post relief can therefore make a lot of sense as it shifts the balance for the private operator towards a refusal to pay the ransom becoming more attractive. As most of the benefits of a refusal are positive externalities for society (attacking the lifeline of the criminal network), it does make sense to use taxpayers' money to pay for (part of) this ex post relief. Moreover, as these costs often cannot be foreseen and have to be made ad hoc (after the attack has occurred), there is less of a problem of free-riding or moral hazard, which occur in the case of subsidies for ex ante preventative solutions.[44] The potential risk of a negative impact on ex ante security levels remains, however, which needs to be taken into account when drafting the design of such a subsidy. In Section VII, we will therefore further discuss several scenarios in which we take into account such a subsidy in combination with a tax.

IV. Current literature regarding ransom taxation

In this section, we discuss the literature regarding ransom taxation. There are only a few authors who briefly describe the idea to tax ransom payments. DeMuro discusses the ransomware tax from the perspective of the healthcare industry.[45] The tax would reduce both the incentives to pay the ransom for companies and the incentive for hackers to attack with ransomware, as the hackers would know that the possibility of the company paying is lower due to the tax. The tax revenue can be used to combat the ransomware problem. DeMuro observes the drawback that companies (in this case healthcare organisations) are less likely to report ransomware attacks because if nobody knows about the attack the organisation can refrain from paying the tax. Dey and Lahiri discuss the ransomware tax as well.[46] They also observe practical challenges in terms of the collection of such a tax and discuss the need for a ransomware notification duty. They also mention a combination of the ransomware tax with providing aid to firms that refuse to pay ransom demands. In this way, the firms who pay the ransom are punished and the firms who do not pay are subsidised. This mix of a tax and a subsidy can be done in a somewhat revenue-neutral way. The tax revenue can be used to pay for the subsidies.[47] The literature and public debate regarding ransomware taxation are relatively scarce. For instance, to the best of our knowledge, the UK ransomware task force has not published anything about ransom taxation, and we did not find any other discussions in our research of the literature and public debate. The scarce literature on ransomware taxation sees a ransomware tax as a means to internalise externalities. They do not discuss the extent of the externality which we covered in the previous section. They stress some practical issues with collecting taxes. In addition, they mention using the revenue to foster ransomware prevention by providing aid to organisations who refuse to pay or to combat the ransomware problem more broadly.

[44] A similar argument is made in the literature on ex post disaster relief, where it is equally argued that government intervention for ex post disaster relief is not problematic as these payments will not negatively affect the incentives for disaster risk reduction. See G Dari-Mattiacci and MG Faure, "The Economics of Disaster Relief" (2015) 37 Law & Policy 180.

[45] PR DeMuro, "Keeping Internet Pirates at Bay: Ransomware Negotiations in the Health Care industry" (2018) 41 Nova Law Review 350.

[46] D Dey and A Lahiri, "Should We Outlaw Ransomware Payments?" (2021) 54 Hawaii International Conference on System Sciences 6609.

[47] Cartwright et al, supra, note 26.

The current literature does not explicitly discuss the benefits of taxation regarding the incentives to increase the ex ante cybersecurity level. If ransom amounts are low, companies have fewer incentives to increase their cybersecurity level. When a ransom payment is higher due to a tax, this incentive increases. The literature does address that the revenue of a ransomware tax can be used to contribute to the mitigation of ex ante insufficient protection against ransomware by subsidising cybersecurity.

V. Price elasticity of "demand"

In this section, we will discuss the extent to which an increase in the price of ransomware actually leads to differences in payment activity: the price elasticity of a ransom. Our goal is not to extensively model price elasticity, but rather to explore the effect of imposing an additional cost for paying ransomware on the decision either to pay or not to pay ransom. Under circumstances of high elasticity, an increase in the price of ransom (eg by means of a tax) has a larger effect on the number of payments (which create negative externalities) than under circumstances of low price elasticity. In this section, we will use the simplified example of backups to illustrate price elasticity. As has been said, we are well aware that the reparation costs of a ransomware attack depend on many more factors, but we use the backup example to discuss various perspectives on price elasticity.

Suppose the possibility for an organisation to refrain from paying a reasonable price depends on whether the company has a backup or not. Organisations with no backups stand "with their backs against the wall". Organisations with backups have the possibility to quickly recover from a ransomware attack. In this situation, price elasticity is low. A higher price of the ransom payment (because of a tax) would not deter an organisation without backups from paying a ransom demand if the cost of repairing the system is a multiple of the ransom price. Hence, price elasticity is low, and if one wants to lower the payment activity, the tax must be very high (almost equalling the very high reparation cost). The tax will de facto equal a prohibition.[48]

In reality, the distribution of the amount of cybersecurity resilience among organisations is likely to be less dichotomic than illustrated in the case above. Organisations do not simply have either backups or no backups. They might have backups, but they might not all have been made at the same time. If an organisation has older backups, more data would be lost and the cost of reparation would be higher. When the ex ante level of cybersecurity is distributed more widely, a tax would indeed reduce the payment activity, especially for those organisations where the ransom demand is slightly lower than the reparation cost.[49] If there is price elasticity in paying a ransom and if not paying hurts the criminal business model, then a tax may induce organisations not to pay ransom and to internalise the externality.

When one follows the logic of this perspective, policy options focused on ex ante cybersecurity could increase the price elasticity of demand. If one invests in ex ante cybersecurity, more organisations will have more security measures in place. This leads to fewer organisations that have very high repair costs because they have no backups ("stand with their backs against the wall"). Hence, according to this argument, a policy that stimulates ex ante security also improves the effect of measures targeted at changing the payment

[48] In that sense, a ransom tax may look like a tax on gasoline, which is also an inelastic good. "Imposing environmental surcharges on gasoline will result in only a small reduction in driving and thus only a small improvement in the environment": KN Sipes and R Mendelsohn, "The Effectiveness of Gasoline Taxation to Manage Air Pollution" (2001) 36(2) Ecological Economics 299.

[49] Either because their reparation cost is relatively low compared to those "who stand with their backs against the wall" as, for instance, they might have older backups that results in some work to restore the system, but not so much that it is unsurmountable, or because of a very high ransom demand.

decision ex post, because the policy focused on ex ante security on average reduces victims' willingness to pay and increases price elasticity.

Would there be a case for a tax when price elasticity turns out the be very low? A tax can induce ex ante security measures and can shift the private optimum from paying to not paying and increase price elasticity. Ex post, such a tax will have limited effect on the actual ransom payment activity and merely punishes organisations "standing with their backs against the wall".

VI. Challenges when implementing a ransom tax

This section describes challenges when implementing a ransom tax. We will compare the ransom tax with excise taxes on fast-moving consumer goods such as tobacco, cannabis, alcohol and petrol,[50] and with environmental taxes for companies[51] to distinguish the "cyber dimension" of a ransom tax that leads to specific challenges when implementing such a tax.

1. Taxing whom?

One could, for instance, either tax the insurer (who would pay the ransom) or the individual organisation that is the victim of a ransomware attack.[52] The former has lower administrative costs but creates additional incentives for evasion – namely, to pay the ransom privately and possibly also to refrain from insurance. One of the parties engaging in the transaction that is taxed is a criminal. However, it is hard to tax the "seller" of ransom. In many excise taxes, the seller is responsible for the taxation because this lowers transaction costs.

2. Public resistance

A tax can lead to the public opinion that the victims of a ransomware attack are being punished instead of the criminals, and this is analogous to the public resistance towards a prohibition of the payment of ransom.

3. Legality of a tax on (sometimes) forbidden transactions

When the payment of a ransom is taxed, it could be argued that this de facto implies that the state legalises or at least tolerates this activity. That is of course not necessarily the case. A distinction should be made between, on the one hand, the legality of the ransomware, which obviously remains illegal, and on the other, the payment of the ransom, which does not become legal (or illegal) just by subjecting it to a tax. Those are two different issues. Moreover, there are many other examples in the law where illegal activities are also taxed. Albeit in some countries the sale of soft drugs (eg marijuana) first had to be legalised in order to be able to tax it, this is not always the case.[53] However, currently, as mentioned in the introduction to this paper, a ransomware payment can often be

[50] Sipes Mendelsohn, supra, note 48.

[51] Perhaps taxes on physical ransom payments? To the best of our knowledge, this has not been discussed in the literature.

[52] What might be a workable idea is a mix between the two. A pre-tax is levied on the organisation. If this organisation is not insured, the tax is levied on the organisation. If it is insured, that tax is deductible from the tax that is included in the price of the insurance. This can also stimulate insurance depending on the tax rate.

[53] P Messino, "Taxing Illegal Drugs: How States Dabble in Drugs and Why They Shouldn't" (2007) Reason Foundation Policy Study 357.

deducted as the cost of doing business. If this is the case, it is likely that ransom can be part of "normal" financial operations. In other words, if a cost can be deducted from corporate tax, it can probably also be taxed.

4. Tax evasion

Whenever a tax is imposed, the question always arises as to whether it can be enforced in an effective and cheap manner. The point is that with a tax, victims of a ransom attack will also receive incentives to conceal the fact that a ransom payment has been made. Moreover, if criminal networks become aware of the fact that ransom payments are taxed (thus making non-payment more attractive for the victim), they could change their strategy. They could, for example, require a payment of monthly instalments for "security monitoring" instead of demanding a lump sum ransom. In addition, there is a danger that victims would conceal the cyber incident, which also has the perverse effect of reducing information diffusion regarding the incident, thus reducing cybersecurity generally. Greater excise taxes are levied on fast-moving consumer goods such as tobacco, petrol and alcohol, among others. Ransomware is not a very fast-moving (consumer) good. It is a one-time experience in which you have to make a dichotomous decision and you are a "one-shotter". The implication might be that not every company knows about the tax and hence that administrative costs might be relatively high. This would be less of a problem if the tax only focuses on insurers, but it also creates evasion incentives. An insurer might ask the insured to pay the tax directly if only insurers have to pay the tax.

5. Inequality

A tax can cause inequality. To a certain extent, a ransomware attack is random (and, of course, to an important extent, the success of it has a correlation with one's cyber defence). The tax would therefore specifically target victims, whereas it is not always clear that they are to blame for becoming a victim of a ransomware attack. The attack could have been random and not necessarily related to too little investment in cybersecurity. Hitting victims of a criminal attack additionally with a tax could therefore be considered as unfair.

6. Administrative costs of enforcement

Administrative costs can be high when enforcement is difficult and if there are evasion possibilities. The ransom paid by the victim of the attack can generally be tax deductible. That implies that as long as the ransom tax is lower than the tax advantage (of reducing the payment), there would be an incentive to pay the tax in order to obtain the tax deduction. In the opposite case (the tax being higher than the benefit of tax deduction), the victim would have an incentive not to report the ransomware payments.

7. Determining the tax rate

Determining the tax rate can be difficult, especially when one wants to make it adjustable to the amount of the externality. One can opt for a flat rate, but also for a regressive, proportional or progressive tax rate. As has been said, there has been some media attention regarding the possibility of deducting the payment as a business expense. One could therefore consider the prohibition of the deduction of ransomware payments as a tax-deductible cost. In this paper, we will not further go into the topic of tax deduction of ransomware payments, but instead we will suggest in the next section some scenarios for a tax that is adopted independently from the possibility of whether or not the payment

may be deductible. This has the disadvantage that this "tax" depends on the corporate tax rate of the company. In the next section, we sketch some scenarios in which we adjust the tax rate and also introduce the alternative of a subsidy.

VII. Several scenarios

In this section, we will discuss several scenarios in which we adjust the amount of the ransom tax. In two scenarios, we also introduce a subsidy on not paying ransom to investigate whether this has a mitigating effect on the drawbacks of a tax. In each scenario, we will review the potential effect of the instrument on the private and social optimum. For the moment, we assume that there is no tax evasion and that there is indeed some price elasticity of "demand" in paying ransom.[54]

1. Scenario 1: low tax, no subsidy

In this scenario, we consider a relatively low tax.[55] Such a tax rate could, for instance, be 25%, which is lower than the advantage of entering the ransom amount paid in the bookkeeping for tax-deduction purposes,[56] but it is still an amount that substantially increases the ransom amount (in order to have any effect on the decision of this one-time event).

a. Private cost and benefits

i. Effect on ex ante security. The tax will induce organisations to invest more ex ante in cybersecurity because the cost of cybercrime will be higher, and hence the revenues of investing in cybersecurity will be higher as well. Since the tax is low, there will be relatively minor incentives.

ii. Effect on ex post payment decision. Organisations for which the total cost of paying the ransom is increased by the tax such that this will now be higher than the cost of not paying will opt to refrain from paying.[57] For organisations for which the total ransom cost is still lower than the cost of not paying, they will still pay ransom and thus the tax. The change in incentive to negotiate a lower ransom price depends on the type of tax. If the tax is a fixed amount, then this will not change the expected revenue of negotiating. However, if the tax is a percentage of the ransomware demand, there will be an increased return on investment of negotiation since the absolute tax will also be lower.

b. Social cost and benefits

i. Effect on social losses through ransomware attacks. Organisations will invest slightly more in cybersecurity, which reduces the impact cybercriminals can have. These investments can also benefit combatting other types of cybercrime.[58] Secondly, slightly greater numbers of

[54] For reasons of space and simplicity, we only deal with the four scenarios that will be developed below. But other scenarios could also be examined that we do not further discuss, such as the scenarios with a low tax and a high subsidy, or even no tax and a high subsidy. The effects of those could in fact simply be deduced from the analysis of the four other scenarios we do analyse in further detail.

[55] With this percentage, the tax is lower than the advantage gained by treating the ransom payment as a business expense.

[56] In the situations/jurisdictions where a tax may be deductible.

[57] Cartwright et al, supra, note 26.

[58] If the level of investment becomes too high, this can have negative externalities due to overinvestment. This risk is low because there is a low tax and consequently a low incentive to invest. In addition, the private cybersecurity optimum is normally lower than the social cybersecurity optimum due to positive externalities of cybersecurity investments.

organisations will refrain from paying ransom, which hurts the criminal business model. Thirdly, organisations will have increased incentives to negotiate, which impacts the criminal business model. Fourthly, criminals will possibly anticipate the tax and lower their ransom price to avoid the previous effect, but this still will have an impact on their revenue.

2. Scenario 2: low tax, low subsidy

In this case, there is a subsidy for those organisations that refrain from paying; this equals the tax on paying ransom (in this case 25%), but it is not higher than the actual cost of the reparation costs as a consequence of not paying ransom.

a. Private cost and benefits

i. Effect on ex ante security. At first sight, the tax and the subsidy would cancel out the net incentives to invest in ex ante cybersecurity. But for those organisations for which after the imposition of the tax paying is still cheaper than not paying (and they will likewise still pay), there is still an incentive to increase their security as in the previous scenario because they will not have the benefits of the subsidy. In that sense, the subsidy has no negative incentives on poor performers relative to the first scenario and, together with the tax, creates additional incentives for those poor performers to ex ante invest in cybersecurity.

On the other end, the subsidy has slight negative incentives for organisations with decent cybersecurity if this would imply that organisations would decrease their investments in cybersecurity knowing that they would be provided with a subsidy every time they are confronted with a ransom demand. As we argued above, the danger of this moral hazard is substantial if investments in ex ante cybersecurity investments were to be fully subsidised. However, the problem is less significant in the case where the (partial) subsidy targets the costs of not paying the ransom and restoring one's own systems. As a ransom attack is often random and can ex ante hardly be predicted (assuming adequate cybersecurity), ex post relief does not necessarily create a serious moral hazard problem, provided that the subsidy is designed in a smart manner (ie with a financial cap on the subsidy that, on the one hand, still makes it attractive to refuse the payment instead, but on the other hand preserves incentives to ex ante invest in cybersecurity). In addition, one could think of certain baseline cybersecurity conditions that form a prerequisite for providing the subsidy. One could also distinguish between in-kind and cash subsidies. The exact definition of such a subsidy could be a subject for future research.

In addition, a relatively low subsidy will be targeted at those companies that do not "have their backs against the wall" (which arguably is often the result of poor ex ante cybersecurity, as we have discussed in Section V) but possibly have backups that are slightly older or are simply unlucky. A low subsidy will not induce companies that have poor ex ante cybersecurity to refrain from paying because for these companies the cost of not paying, even when a low subsidy is included, will still be larger than the cost of paying.

ii. Effect on ex post payment decision. The subsidy would generate an additional incentive to refrain from paying, which would also reach those organisations that would not pay in the current situation without a tax.

b. Social cost and benefits

The introduction of the subsidy may reduce the incentives to invest ex ante in some areas (mainly the organisations that already have good cybersecurity levels), but it may reduce the amount of ransom payments further. As a consequence, criminals could respond by

lowering the price of ransom even further than in Scenario 1. Some part of the subsidy may be directed at organisations that do not need it since they would have never have paid in the first place.

3. Scenario 3: high tax, no subsidy

A tax is "high" if it ensures that in most scenarios not paying will be cheaper than paying. For this, we assume that the tax should be in the order of magnitude of a minimum of ten times the ransom payment.[59] The magnitude of the tax might indicate lower feasibility when executing the tax.

a. Private cost and benefits

i. Effect on ex ante security. A high tax would increase the incentives for investing in improving ex ante security levels.

ii. Effect on ex post payment decision. The high tax would create an additional incentive not to pay. However, the companies with high reparation costs would face bankruptcy if they had to either choose between a ransom payment with a high tax or reinstalment of their systems. They would not pay and instead go bankrupt. In addition, the tax would create an additional incentive to negotiate a lower price if the tax is a percentage of the ransom demand.

b. Social cost and benefits

This option has a positive social impact on ex ante security levels and ex post payment decisions. When the tax is high enough, theoretically there would be no ransom payments anymore and, in fear of bankruptcy, companies would either invest in cybersecurity or shift the risk to an insurer (or do both).

However, poor performers (and companies that are victims of a sophisticated cybersecurity attack that could not be avoided) that did not manage the ransom risk properly are punished severely by this option. When the tax is very high, it is effectively a ban, as companies would have no other option than to go bankrupt if they fail to negotiate a lower price. This obviously has a high social cost because this destroys economic activity. Criminals might anticipate the high tax and reduce their ransom demand considerably.

4. Scenario 4: high tax, high subsidy

In this case, there is a subsidy for those organisations who refrain from paying, which equals the tax on paying but is not higher than the actual cost of not paying. The subsidy is implemented together with a high tax.

a. Private cost and benefits

i. Effect on ex ante security. The subsidy would cancel out the net incentives to invest in ex ante cybersecurity of the tax for those who would have paid in the original situation without a tax if the price of not paying (including the subsidy) equals the original ransom price (without a tax). For those companies for which the price of not paying after the subsidy is still higher than the original ransom price, there is an additional incentive to invest in cybersecurity because the measure increases the private cost of a ransomware attack.

[59] Indirect costs are much higher than direct costs; see R Anderson et al, "Measuring the Changing Cost of Cybercrime" (18th Annual Workshop on the Economics of Information Security, Boston, 2019) <https://www.repository.cam.ac.uk/handle/1810/294492> (last accessed 13 October 2022).

However, for those companies that would not even pay a ransom in the first place because they have relatively good cybersecurity, a high subsidy could lower incentives to invest in cybersecurity, as the private marginal benefits of investing in cybersecurity will be lowered by the subsidy.

ii. Effect on ex post payment decision. The vast majority of the organisations would not pay a ransom because the high tax raises the price of paying significantly, while, on the other side, the high subsidy lowers the price of not paying.

b. Social cost and benefits

A high tax–high subsidy mix could reduce the risk of companies going bankrupt when facing ransomware attacks while still effectively eliminating most ransom payments. However, it increases the risk for companies with bad ex ante cybersecurity to free ride if the subsidised price of not paying is equal to or lower than the ransom demand without the tax.

This can be mitigated, as is illustrated by the following example: an organisation faces a ransom demand of 100,000 euros with a cost of not paying of 800,000 euros. The ransom tax is 1,000,000 euros and the subsidy is 600,000 euros. In this situation, the net cost of not paying is still 200,000 euros, which is higher than the original ransom demand (100,000 euros) and hence generates incentives to invest in cybersecurity ex ante because it has private benefits for reducing these costs. The high tax–high subsidy scenario reduces the incentive to negotiate because in this situation one has to reduce the ransom demand (100,000 euros plus 1,000,000 euros in tax) much more strongly to achieve a scenario in which paying is still more profitable than not paying. For instance, a reduction of 90% would lead to a total price of 10,000 euros in ransom plus 100,000 euros in tax, which is lower than 200,000 euros. Hence, this leads to the conclusion that it would be best in a high tax–high subsidy scenario if the net cost of not paying (after the subsidy) always remains higher than the original ransom demand to maximise incentives for ex ante cybersecurity and still reduce payment activity.

The high subsidy also leaves open an opportunity to tie the subsidy to the externalities of the ransom payment in an individual case. A high tax–high subsidy scenario could, for instance, be used in the case of targeted attacks, where the negative external effect is higher, as we argued in Section II. A high subsidy–high tax scenario could therefore be used to provide deterrence for targeted attacks such as the Colonial Pipeline hack, while similarly leaving room for the organisation to operate and keep the incentive to invest in ex ante cybersecurity.

If the high tax–high subsidy scenario leads to the conclusion that no one would pay ransom and consequently the ransom tax (given the combination of a high tax and high subsidy), there would be no revenue-neutral way to do this, and hence there is a social cost of the subsidy in the short term. However, if this leads to the elimination of ransom demand and subsequently ransomware attacks, the subsidy is never invoked, and so it can be revenue neutral. This depends on global ransomware policy and the distribution between scattered (worldwide) and tailor-made (regional) attacks. When the latter prevail, criminals would bypass countries that have a high-subsidy policy, but when there are still scattered attacks, an organisation in a country with a high subsidy still risks being part of a scattered (eg supply chain) cyberattack.

VIII. Conclusion

This paper explored the uneasy case for a tax on ransomware. We first discussed whether ransom payments create negative externalities. Secondly, we discussed the policy options

in the literature to provide incentives to parties to make more socially optimal choices when confronted with a ransom demand. We provided a brief review of the current literature regarding taxation in general and ransom taxation in particular. In addition, we discussed price elasticity, unique characteristics and practical challenges, and we presented several scenarios. Our goal was to contribute to the literature and connect different fields of discussion regarding a ransom tax, amongst others: the negative externalities of ransom payments; the relationship of tax with regards to other policy options; the effect that a tax can have on payment activity; and the interplay between a tax and a subsidy. We realise that the literature on this topic is scarce and therefore we allowed ourselves to touch upon a broad range of subtopics that, without doubt, need further research.

The case for a ransom tax remains uneasy, perhaps in the first place because public resistance is expected. A tax can lead to the public opinion that the victims of a ransomware attack are punished instead of the criminals. There are numerous other practical challenges, such as the risk of tax evasion. Nevertheless, our analysis has provided three key insights that can be used to facilitate policymaking.

First, a tax could have two benefits. It could stimulate ex ante cybersecurity and reduce (when price elasticity is not very low) ex post payment activity. A stimulation of ex ante cybersecurity could also increase price elasticity.

Second, a tax in combination with a smartly designed subsidy could possibly be more effective than a tax alone. A low tax–low subsidy scenario could provide an incentive for organisations to invest in ex ante cybersecurity and reduce payment activity, while still giving organisations that have very high reparation costs the possibility to pay a ransom. A high tax–high subsidy scenario could potentially strongly reduce ransom attacks while still keeping an incentive for organisations to invest in cybersecurity ex ante. In addition, this option avoids bankruptcy for organisations that "stand with their backs against the wall". However, if the measure is effective and no ransom is being paid anymore, there is no revenue-neutral way to adopt such a policy.

Third, we argued that some ransom payments create more negative externalities than others. The tax–subsidy mix could be tailored to the specific nature of the ransom attack. One could argue, for instance, that in the case of a scattered ransomware attack, a low tax–low subsidy mix is appropriate because it can change a portion of the victims of such attacks from having to pay to not paying while simultaneously providing additional incentives for investing in ex ante cybersecurity. In the case of a targeted ransomware attack, a high tax–high subsidy mix could possibly respond better to the stronger negative external effect of paying ransom in the individual case.

Further research could study the rate of the tax, the conditions for the subsidy and substantiate other challenges that will arguably differ between jurisdictions. We hope that our exploration of the uneasy case for a ransom tax aids the further development of policy options aimed at providing ex ante incentives for cybersecurity and ex post incentives to refrain from paying ransom in the case of a ransomware attack.

Acknowledgments. We are very grateful to Goran Dominioni, Daniel Woods, Willem Kuijken and Rens Hoogerwaard for their feedback on earlier versions of this paper and, in the case of Willem Kuijken and Rens Hoogerwaard, for their research assistance as well.

Competing interests. The authors declare none.

Cite this article: B Nieuwesteeg and M Faure (2023). "The Uneasy Case for a Ransom Tax". *European Journal of Risk Regulation* **14**, 382–398. https://doi.org/10.1017/err.2022.45