Management Science

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

The Impact of Cryptocurrency on Cybersecurity

Terrence August, Duy Dao, Kihoon Kim, Marius Florin Niculescu

To cite this article:
Terrence August, Duy Dao, Kihoon Kim, Marius Florin Niculescu (2025) The Impact of Cryptocurrency on Cybersecurity. Management Science 71(11):9606-9627. https://doi.org/10.1287/mnsc.2023.00969

https://pubsonline.informs.org/journal/mnsc

MANAGEMENT SCIENCE
Vol. 71, No. 11, November 2025, pp. 9606–9627
ISSN 0025-1909 (print), ISSN 1526-5501 (online)

The Impact of Cryptocurrency on Cybersecurity

Terrence August,[a,*] Duy Dao,[b] Kihoon Kim,[c] Marius Florin Niculescu[d]

[a] Rady School of Management, University of California, San Diego, La Jolla, California 92093; [b] Haskayne School of Business, University of Calgary, Calgary, Alberta T2N 1N4, Canada; [c] Korea University Business School, Seoul 136-701, Korea; [d] Scheller College of Business, Georgia Institute of Technology, Atlanta, Georgia 30308

*Corresponding author

Contact: taugust@ucsd.edu, https://orcid.org/0000-0002-4085-1147 (TA); duy.dao@ucalgary.ca (DD); kihoon@korea.ac.kr, https://orcid.org/0009-0000-7977-062X (KK); marius.niculescu@scheller.gatech.edu, https://orcid.org/0000-0002-4330-662X (MFN)

Received: March 30, 2023
Revised: September 8, 2024; December 20, 2024; January 3, 2025
Accepted: January 16, 2025
Published Online in Articles in Advance: March 27, 2025

https://doi.org/10.1287/mnsc.2023.00969

Abstract. Cryptocurrencies have prompted a shift away from classic security attacks toward ransomware-based extortion. To better understand the impact of cryptocurrencies on the cybersecurity landscape, we conduct a comparative analysis of cybersecurity metrics prior to and after the adoption of cryptocurrency using a series of connected software-use models in the presence of security externalities. In this framework, we endogenize the actions of both heterogeneous consumers and attackers, with entry of the latter being driven by both the size of the unpatched consumer population and, as a subset of it, the size of the ransom-paying consumer population. We first examine users' adoption and patching behavior under both security scenarios. We explore how changes in attacker entry costs impact outcomes under both conventional and post-crypto ransomware threat landscapes. We show that ransomware scenarios may be more desirable than conventional ones when attacker entry costs are low, provided that the gains from entering with standard attacks under the ransomware scenario are not too high. However, under such scenarios, social welfare can increase under the same conditions that lead to larger ransoms being demanded and a higher expected total ransom being paid, which presents a conundrum to policymakers. We also examine the impact of market parameters associated with security losses from conventional attacks and residual losses when victims pay in ransomware attacks.

History: Accepted by Kay Giesecke, finance.

Funding: This work was partially supported by Insung Research Grant of KUBS, the LG Yonam Foundation (of Korea), and an award from the Georgia Institute of Technology Center of International Business Education and Research as part of its funded research program.

Supplemental Material: The online appendices are available at https://doi.org/10.1287/mnsc.2023.00969.

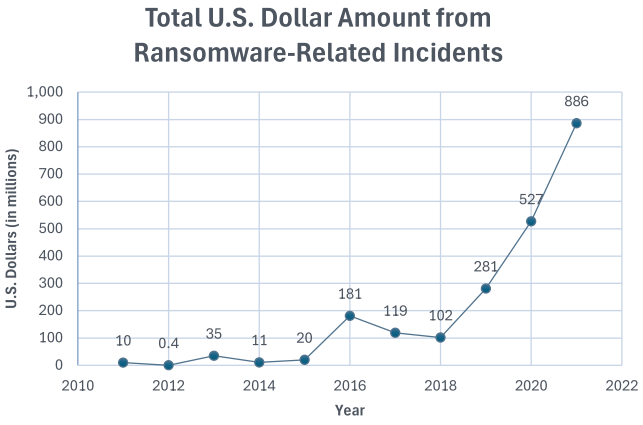
Keywords: ransomware • cryptocurrency • cybersecurity • open source • interdependent risk

1. Introduction

Cryptocurrencies (crypto), the most prominent type of blockchain-based digital asset, have been heralded as a game changer for the payments industry, marking the beginning of an era of decentralized finance (DeFI), with the promise of near-instant secure transactions, storage of funds in secure digital wallets, and accessibility via Internet from anywhere (Levy 2024). But for all the sung praise and promise, it is undeniable that there is a real dark side related to the adoption of crypto; namely, cryptocurrencies have become the go-to instrument for transactions associated with cybercriminal extortion-type activity due to the pseudonymity of crypto transactions (Black 2022). Such extortion-based cyberattacks, commonly referred to as *ransomware* attacks, have rapidly grown in frequency and impact as seen in the Financial Crimes Enforcement Network (FinCEN) 2011–2021 data reproduced in Figure 1.

Ransomware did exist prior to the introduction of Bitcoin in 2009 (even going back to 1989), but its financial impact in earlier decades was negligible.[1] Once Bitcoin adoption gathered steam and crypto transaction tools and exchanges evolved into the mainstream, the stage was set for malicious actors to take ransomware to a higher impact level, which occurred in 2013 when CryptoLocker became the first major ransomware strain combining advanced encryption locking with ransom demands in cryptocurrency (Crowdstrike 2022). Going beyond FinCEN's 2011–2021 data, researchers estimate that ransom payments reached $1.1 billion in 2023 (Chainalysis 2024).

Figure 1. (Color online) Data Sourced from FinCEN Ransomware Trends Report (FinCEN 2022)



Note. Values are computed as of "incident date" that reflects the date associated with payments.

Although modern crypto-fueled ransomware attacks initially targeted proprietary software, we also see a large volume of these attacks on open-source software (OSS), particularly after 2021.[2] More broadly, cybercriminals are attacking OSS across industries using a variety of attack vectors and payloads even going beyond ransomware (Statista 2024). In fact, according to a 2024 study by Sonatype, 704,102 malicious packages targeting OSS have been identified since 2019 (Maudrill 2024). The reason for malicious hackers' interest in exploiting OSS vulnerabilities is simple: Nowadays, leveraging OSS is a critical aspect of most firms' information technology (IT) strategies. With OSS, a firm maintains significant flexibility with regard to customization, less lock-in with software vendors, lower software costs, and more. What is particularly noteworthy is the extent to which OSS components are being leveraged. The number of OSS contributions to GitHub (one of the most prominent repositories of OSS projects) reached 301 million in 2023 alone, and nearly 30% of Fortune 100 companies started their own open-source program offices to coordinate OSS strategies (GitHub 2024). RedHat's *The State of Enterprise Open Source* reports that 90% of surveyed IT leaders already use enterprise OSS (Red Hat 2021). According to Black Duck (2024), 96% of commercial codebases leverage to some extent OSS code (with 77% of the total code originating from OSS). Among surveyed codebases, 84% contained OSS security vulnerabilities (with 74% of the codebases including high-risk vulnerabilities), and no less than 91% contained components that were at least ten versions behind the current version of the component. This current industry reality presents hackers with opportunities to land widely disruptive attacks on OSS vulnerabilities, with substantial associated losses.

When examining the economics of open source as it relates to security, certain attributes are particularly salient. OSS is typically available for free and therefore can engender significantly larger user populations than its commercially available counterparts. Increased usage often goes hand-in-hand with increased *risky* usage in that a sizeable portion of the user population will find it incentive compatible to remain unpatched. Thus, historically with traditional (nonransomware) attacks, risk management has centered on mitigation via policies to improve patching behavior (August and Tunca 2006). However, in the face of ransomware, this calculus gets shifted because users have an additional opportunity to contain losses by paying out ransoms instead. To be sure, a user with intent to pay ransom as part of its strategic defense clearly has dampened incentives to patch. Ceteris paribus, possessing an option to pay ransom instead of incurring larger losses can be good for consumer surplus. At the same time, attackers' strategies are shifting as they consider both ransomware and standard attacks. Ransomware can certainly streamline the monetization process by extracting payments directly from victims. However, aggressive attacks, larger payouts, and publicized successes can actually lead to higher attack volumes and ultimately deter unpatched consumption (Jeffery and Ramachandran 2021).

A common presumption in the economics of cybercrime is that raising hacker costs and risks would be beneficial to cybersecurity. For example, national security strategy in the United Kingdom dictates that "we need to *raise the cost*, raise the risk, and reduce the reward of cyber criminals' activity" and, similarly in the United States, aims to "disrupt and dismantle threat actors" and has an approach that specifically includes "targeting the illicit cryptocurrency exchanges on which ransomware operators rely and improving international implementation of standards for combatting virtual asset illicit finance" (United Kingdom 2016, p. 47; White House 2023, pp. 14 and 17). Attacker costs are critical in that they can significantly sway attacker entry behavior. However, the shifting of attacker entry costs can have a significant, *differential* impact when examining a pre-crypto environment versus a post-crypto one characterized by the presence of ransomware. Moreover, the presumption that raising costs will be helpful needs further consideration in that the strategic interaction between user behavior (adoption, protection, and ransom-paying strategies) and attacker behavior (entry and attack strategy) is highly complex.

Against this backdrop, in this paper, we perform a comparative analysis of the security landscapes and market outcomes under both a pre-crypto context characterized by traditional attacks and a post-crypto context where ransomware becomes a possibility. Given the enabling role that crypto plays in the execution of digital extortion attacks, this comparison allows us to identify the impact of cryptocurrency on cybersecurity.

As part of our research agenda, we aim to shed light on the role of attacker entry costs in shaping cybersecurity market outcomes while particularly highlighting that increased costs can unexpectedly be detrimental in the post-crypto ecosystem. Thus, reducing attacker entry costs may possibly lead to superior post-crypto outcomes in comparison with pre-crypto ones.

To the best of our knowledge, this is the first study to execute such a comparison while endogenizing the actions of both (a continuum of) heterogeneous consumers and (a continuum of) heterogeneous attackers, with the entry of the latter being driven by both the size of the unpatched consumer population and, as a subset of it, the size of the ransom-paying consumer population. Moreover, by focusing on a relatively new warfront in ransomware attacks, namely attacks on OSS, we further extend the research agenda on the economics of ransomware.

Specifically, we study how attackers are drawn differently to vulnerable software across pre-crypto and post-crypto scenarios. Post-crypto, we characterize how ransomware-specific metrics such as the ransom-paying population size and expected total ransom paid are impacted by attacker entry costs, a relevant moderating variable for our comparative analysis as discussed above. We examine how the strategic behaviors of consumers and attackers affect social welfare, and we compare the impact before and after cryptocurrencies transformed the landscape. There are multiple economic forces at work. Under both settings, lowered entry barriers for attackers can increase pressure on consumers from a security risk perspective but can also dilute attacker returns due to crowding out effects. However, in the post-crypto ransomware setting, entering attackers also strategically choose the attack mode (with or without ransomware payload) and the ransom amount. This provides them with greater flexibility to manage the crowding out effect. Moreover, when some attackers choose ransomware, a portion of the unpatched consumers are able to mitigate, to some degree, the attack losses through ransom payments in the post-crypto setting. These forces shape the equilibrium segmentation of consumers and attackers, with the overall net effect on outcomes hinging on the extent of each segment's presence. Because, in equilibrium, unprotected consumers segment into ransom payers and nonpayers, and attackers segment into those who enter with conventional attacks and those who enter with ransomware attacks, there are significantly more complex dynamics under post-crypto ransomware setting relative to the pre-crypto one. A key contribution of our study is that we formally demonstrate that the presence of ransomware can be socially beneficial, even in the presence of strategic attackers making self-interested entry decisions. We show that a *decrease* in attacker entry costs can unexpectedly shift post-crypto welfare outcomes higher relative to the pre-crypto scenario. Moreover, we also highlight that welfare can be increasing in the attacker entry costs on the same region where ransomware-specific metrics (expected ransom paying population, expected ransom demand, and expected total ransom paid) are also increasing. For example, in that one might expect that decreasing expected total ransom paid would be helpful, rather than harmful (which we establish is a possibility), to social welfare, our results can help policymakers better understand how to approach the security problem in this domain and avoid policies that might focus in the wrong direction on certain metrics. We also conduct a numerical analysis that includes additional layers of attacker heterogeneity to demonstrate the robustness of our findings. Finally, we discuss how our exploration can help inform policymakers working in this space.

2. Literature Review

This study builds on several streams of research: (i) economic impact of cryptocurrencies, (ii) IT security, and (iii) economics of ransomware.

A lot of the recent literature on cryptocurrencies focuses on their technical aspects (as a direct application of blockchains). Only recently are we starting to see an emerging body of work on the economic impact of this type of digital money while the vast majority of extant work focuses on financial aspects of cryptocurrencies, as is summarized in recent research literature surveys by Halaburda et al. (2020), Bariviera and Merediz-Solà (2021), and Yue et al. (2021). Although there is palpable excitement about the potential of cryptocurrencies (and decentralized finance in general) to bring significant change to the financial sector, there are some problematic effects of the adoption of cryptocurrencies that warrant closer scrutiny. First, the impact of mining for cryptocurrencies has been examined from an energy sustainability and environmental perspective in several studies, with particular focus on the Bitcoin protocol, which relies on a computationally intensive proof-of-work implementation (Badea and Mungiu-Pupazan 2021). Also, because of various degrees of pseudonymity, cryptocurrencies became the preferred go-to payment tools for illegal and criminal activities (Foley et al. 2019). It is within this latter category that our study makes a novel contribution, by focusing on the impact of adoption of cryptocurrencies on the cybersecurity landscape.

As cryptocurrency payments represent the main enabler of ransomware attacks at such unprecedented scale, in order to assess the role cryptocurrencies have in shaping software adoption, security losses, and overall social welfare, it is insightful to compare security outcomes across scenarios in the absence of ransomware threats (pre-crypto) and in the presence of ransomware

threats (post-crypto). The extant literature on the economics of IT security has explored at depth pre-crypto (traditional) cyberthreat landscapes, tackling a wide spectrum of research questions on topics including interdependent network security risks (Gal-Or and Ghose 2005, August and Tunca 2011, Zhao et al. 2013), patching incentives and management (Ioannidis et al. 2012, Dey et al. 2015, August et al. 2019), management of vulnerability disclosure (Cavusoglu et al. 2007, Choi et al. 2010, Mitra and Ransbotham 2015), open-source software security (Witten et al. 2001, Swire 2005, Schryen and Rich 2010), and cyber insurance (Böhme and Schwartz 2010).

On the other hand, the literature on economics of IT security in the presence of ransomware (post-crypto) has just recently gained traction. Ransomware attacks differ from conventional attacks in that, in the wake of the attack, some of the victims may be able to moderate the magnitude of the loss through the payment of a ransom. Laszka et al. (2017), Cartwright et al. (2019), and Ryan et al. (2022) explore interactions between ransomware attackers and victims in the context of bargaining games, a setup fitting the realities of targeted, sparse attacks. Vakilinia et al. (2021) propose a smart-contract solution to implement a mechanism to ensure attackers share the decryption keys after a ransomware attack. Galinkin (2021) explores options to decrease ransomware attacker incentives. Fang et al. (2022) study the decision to pay ransom from the perspective of a Bayesian game with incomplete information for both the hacker and victim. Cartwright and Cartwright (2019) and Li and Liao (2020) explore the role of attacker reputation in the context of multiple-period repeated ransomware attacks. Dey and Lahiri (2021) analyze how banning ransom payments or executing corporate bailouts would affect welfare in a steady-state multiperiod market with two participants. Balasubramanian (2021) and Yin et al. (2023) explore how cyber insurance impacts the frequency and severity of ransomware attacks, as well as defender efforts. Hernandez-Castro et al. (2020) study how consumer market and ransomware attack parameters affect welfare in targeted attacks without interdependent risk. Ahnert et al. (2022) explore the impact of ransomware in financial markets. Zhao et al. (2021), August et al. (2022), and Cartwright and Cartwright (2023) explore ransomware in the context of interdependent security risks in networked environments.

The aforementioned ransomware studies consider either a single, endogenous attacker or an exogenously modeled threat. Although there exists an established literature within the more general attacker-defender modeling domain accounting for multiple, endogenous attackers (Hausken and Bier 2011, Garcia et al. 2019, Xu and Zhuang 2019, DuBois et al. 2023), considerably less exploration has been done on this front in the ransomware threat context (which, as mentioned above, is different from the conventional threats context). In a related work in the context of economics of kidnapping, Selten (1988) propose a model of multiple attackers who contemplate perpetrating at most one attack per period and update their attack pattern over time. In their model, the size of the attacker population is exogenously determined (all attackers are active). Li and Whinston (2020) propose a multiperiod Bayesian game with multiple attackers who strategically build reputation over time. In their study, the attackers' ransom choice is exogenous but the choice of attacking (entering) at each period is endogenized. We make a significant contribution to this line of work by constructing a model with multiple heterogeneous ransomware attackers who strategically decide whether to enter the market, which attack mode to employ, as well as set their ransom demand. Raising the complexity but better capturing their interaction, we incorporate indirect network externalities between attackers and victims such that users' patching and ransom-paying decisions affect attackers' incentives, and attackers' entry decisions affect users' incentives. In addition, we capture direct crowding-out effect that attackers have on one another.

Importantly, there is a dearth of research *directly comparing* and *contrasting* traditional (pre-crypto) versus ransomware (post-crypto) cybersecurity outcomes. This is where our main contribution lies. As discussed in the Introduction, there is a direct connection between the adoption of cryptocurrencies as payment methods and the proliferation of significant ransomware attacks. Thus, through a comparison of traditional cybersecurity scenarios and cybersecurity scenarios with ransomware, we capture the nuanced impact of cryptocurrencies on cybersecurity. August et al. (2022) compare and contrast traditional and ransomware risk scenarios in the context of proprietary software and strategic software vendors. Their model includes an exogenous ransomware threat and does not account for the role of the ransom-paying population on the attack rate. However, in this work, we endogenize both consumer and attacker decisions, and consider a multi-attacker setting with strategic entry driven by expectations of both the size of the unpatched consumer population and, as a subset of it, the size of the ransom-paying consumer population. Moreover, we extend that exploration by focusing on a relatively new area in ransomware attacks, namely attacks on OSS. Ahnert et al. (2022) also compare traditional versus ransomware attacks, but their model considers a single malicious actor attacking multiple homogeneous platforms, each serving multiple homogeneous clients (with assumed symmetric multihoming). The security investment decision is delegated to the platforms. The authors show how ransomware changes the relationship between client and platform. In contrast, we consider both multiple heterogeneous

attackers and multiple heterogeneous consumers whose strategic decisions are endogenized. This allows us to model explicitly one of the anecdotal observations in the ransomware landscape, that more unpatched or paying consumers encourage more attackers to join the landscape, and the ensuing market effects associated with such dynamics.

3. Model Description and Consumer Market Equilibrium

In order to highlight the impact cryptocurrencies have on the software security ecosystem, we develop a unifying modeling framework that facilitates a comparative analysis across two scenarios. The initial specification centers on the state of affairs prior to the cryptocurrency-fueled ransomware problem of today. We refer to this modeling context as *pre-crypto benchmark* (*BM*) setting. The second specification focuses on the context of the current times and it incorporates the characteristics of extortion attacks. We refer to this modeling context as *post-crypto ransomware setting* (*RW*).[3] First, we introduce a primary model that captures core interdependencies at play (in Section 3), and we explore equilibrium market behavior across these settings, as well as the potential harm and benefit of ransomware attacks on society. Subsequently, in Online Appendices C and D, we examine a generalized model with additional attacker heterogeneity to explore robustness of our results.

Our study centers on open-source software but the applicability of the model extends to a broader range of technologies that are offered for zero price and possess similar protective action opportunities and risk interdependence characteristics. Moreover, through a reframing of the setup, our model and results can also be used to generate insights in a more general context inclusive of other types of software.[4]

3.1. Pre-Crypto Benchmark Model (*BM*)

There is a unit mass continuum of consumers whose valuations of the software lie uniformly in $\mathcal{V} = [0,1]$.[5] Users incur an adoption cost of $\kappa > 0$ if they choose to use the software.[6] Moreover, the software is used in a network setting, thus exposing consumers to security risks associated with its use. A security vulnerability can arise in the software in which case the provider makes a patch available. Users who do not apply the security patch are at risk. If a user decides to patch the software, the user will incur an expected cost of patching denoted $c_p > 0$ to immunize against the attack.[7] If the user decides not to patch the software, the probability that the user is randomly hit by a security attack depends on the number of attackers who choose to enter the market, which we discuss next after introducing attacker agents. Ultimately, each user makes a decision to either *adopt*, A, or *not adopt*, NA. Similarly, the patching decision is either *patch*, P, or *not patch*, NP. The consumer action space is then given by $S^c_{BM} = \{(A,P), (A,NP), (NA,NP)\}$.

There is a unit mass continuum of attackers, each characterized by their skill θ distributed uniformly on $\Theta = [0,1]$. In particular, an attacker with skill θ will incur a fixed cost of $\tau(1-\theta)$, with $\tau > 0$, to enter the threat landscape, configure attack tools, initiate attack campaigns, risk being caught, and so on. Thus, attackers with greater skill incur lower costs. The parameter τ captures the state of technology available to facilitate attacks and evade prosecution and hence the cost burden for hackers.[8] Each attacker decides whether to *enter* the market, E, or *not enter*, NE. The attacker action space is then given by $S^a_{BM} = \{E, NE\}$.

Let $\gamma : \Theta \to S^a_{BM}$ and $\sigma : \mathcal{V} \to S^c_{BM}$ denote the strategy functions of the attackers and the consumers, respectively, based on the heterogeneity of each group. Moreover, $\Phi = <\gamma, \sigma>$, denotes an *attacker-consumer strategy profile*.[9] Next, we lay out how attacker and consumer decisions are interdependent. For example, attackers' entry decisions affect consumer losses, and consumer patching behavior affects attackers' entry decisions. Under a candidate Φ, the size of the entering attacker population is given by

$$a(\Phi) \triangleq \int_{\Theta} \mathbb{1}_{\{\gamma(\theta)=E\}}\, d\theta. \tag{1}$$

We denote the probability that a consumer is randomly hit by a security attack by $q(a(\Phi))$, where $a(\Phi)$ is endogenously determined in equilibrium. The function $q(\cdot)$ is assumed to be smooth, increasing, and concave, with $q(0) = 0$, $q(1) \leq 1$, $q'(0) < \infty$, and the attacker elasticity of risk is decreasing, that is, $\eta'_q(a) < 0$, where $\eta_q(a) = (dq/q)/(da/a)$ such that there is a diminishing marginal increase in risk as more attackers enter, both in absolute and relative terms. If successfully attacked, an adopting consumer will incur expected security losses that are positively correlated with their valuation v. That is, consumers with high valuations will suffer higher losses than consumers with lower valuations due to opportunity costs, higher criticality of data and loss of business.[10] Consistent with related literature, we assume that the correlation is of the first order, that is, the loss that a consumer with valuation v suffers if hit by an attack is αv where $\alpha > 0$ is a constant. Therefore, the expected utility for a consumer with valuation v is given by

$$U^c_{BM}(v,\Phi) \triangleq \begin{cases} v - \kappa - c_p & \text{if } \sigma(v) = (A,P); \\ v - \kappa - q(a(\Phi)) \times \alpha v & \text{if } \sigma(v) = (A,NP); \\ 0 & \text{if } \sigma(v) = (NA,NP). \end{cases} \tag{2}$$

Just as the entering attackers affect consumer utility as in (2), unpatched users attract attackers. We similarly

denote the size of the *unpatched* consumer population in the market, contingent on profile Φ, as

$$u(\Phi) \triangleq \int_{\mathcal{V}} \mathbb{1}_{\{\sigma(v)=(A,NP)\}}\, dv. \tag{3}$$

For notational simplicity, we omit subscript *BM* on $a(\cdot)$ and $u(\cdot)$; however, we point out that quantities $a(\cdot)$ and $u(\cdot)$ will be different under *BM* and *RW* models as they are endogenously determined in equilibrium.

The total expected mass of compromised systems by attackers is $\Omega(\Phi) = q(a(\Phi)) \times u(\Phi)$. Each compromised system yields value $\rho > 0$ for the attacker, and each attacker has an equal chance to be the first to successfully compromise any unpatched consumer. Thus, each attacker expects to gain $\rho \times \Omega(\Phi)/a(\Phi) = \frac{q(a(\Phi))\times\rho\times u(\Phi)}{a(\Phi)}$ when entering. Thus, for an attacker with type θ, the expected utility is given by

$$U^a_{BM}(\theta,\Phi) \triangleq \begin{cases} \dfrac{q(a(\Phi)) \times \rho \times u(\Phi)}{a(\Phi)} - \tau(1-\theta) & \text{if } \gamma(\theta) = E; \\ 0 & \text{if } \gamma(\theta) = NE. \end{cases} \tag{4}$$

Note that in (4) the number of entering attackers $a(\Phi)$ impacts attacker utility in two ways, capturing the strategic interactions among attackers. First, $a(\Phi)$ has a direct impact through $q(a(\Phi))/a(\Phi)$. This captures the direct crowding-out effect of attackers in that $\frac{d}{da}\left[\frac{q(a)}{a}\right] < 0$ under the assumptions on $q(\cdot)$. Second, $a(\Phi)$ has an additional, indirect impact from $u(\Phi)$ (via the strategies Φ). This is because $u(\Phi)$ is endogenously determined based on consumers maximizing utility in the face of security risk. Specifically, in the consumer's utility function in (2), $a(\Phi)$ is seen in the loss term should a consumer elect to adopt but not patch. Therefore, the size of attackers entering the threat landscape influences the equilibrium mass of unpatched consumers, as seen in (4).

We study a game of incomplete information where consumers and attackers only know the type distributions of others. In the benchmark game, all decisions are made simultaneously. For all agents, the equilibrium will satisfy a threshold structure as in the following.

Lemma 1. *In the pre-crypto benchmark setting, the equilibrium attacker-consumer strategy profile* $\Phi^*_{BM} = <\gamma^*_{BM}, \sigma^*_{BM}>$ *is characterized by thresholds* $\overline{v}_u, \overline{v}_p, \overline{\theta} \in [0,1]$. *For a consumer of type* $v \in \mathcal{V}$, *the optimal strategy* σ^*_{BM} *satisfies*

$$\sigma^*_{BM}(v) = \begin{cases} (A,P) & \text{if } \overline{v}_p < v \le 1; \\ (A,NP) & \text{if } \overline{v}_u < v \le \overline{v}_p; \\ (NA,NP) & \text{if } 0 \le v \le \overline{v}_u. \end{cases} \tag{5}$$

For an attacker with type $\theta \in \Theta$, *the optimal strategy* γ^*_{BM} *satisfies*

$$\gamma^*_{BM}(\theta) = \begin{cases} E & \text{if } \overline{\theta} < \theta \le 1; \\ NE & \text{if } 0 \le \theta \le \overline{\theta}. \end{cases} \tag{6}$$

In the market equilibrium, high valuation consumers patch and protect their systems, whereas mid-valuation consumers adopt but remained unpatched giving rise to cybersecurity risk. The equilibrium unpatched population $u(\Phi^*_{BM}) = \overline{v}_p - \overline{v}_u$ provides an incentive for attackers to enter the market and strike unpatched systems as seen in the utility function expressed in (4). As a result, attackers can attain positive utility from entering provided that their costs are covered, that is, the attacker skill is greater than $\overline{\theta}$. This gives rise to an equilibrium attacker population of size $a(\Phi^*_{BM}) = 1 - \overline{\theta}$.

3.2. Post-Crypto Ransomware Model (*RW*)

In the post-crypto context, in the presence of ransomware, the threat landscape changes. An attacker may still elect not to enter (*NE*). However, if they decide to enter, they choose the attack mode - standard attack similar to the pre-crypto benchmark setting (*E*) or ransomware attack (*ER*). In the case of the latter, the attacker also selects a ransom amount, thus making two decisions. The attacker action space in this setting becomes $S^a_{RW} = \{\{ER\} \times [0,\infty)\} \cup \{E\} \cup \{NE\}$.

Consistent with the pre-crypto benchmark setting, we assume an attacker entering with a standard attack (*E*) and skill θ will incur a fixed cost of $\tau(1-\theta)$, with $\tau > 0$, to enter the threat landscape, configure attack tools, and initiate the attack campaign. In the case of entry with ransomware (*ER*), there may be additional costs such that an attacker with skill θ incurs a fixed cost of $\tau(1+\omega)(1-\theta)$ where $\omega > 0$.[11] Hence, the additional cost of $\tau(1-\theta)\omega$ represents the skill-based, ransomware-specific *cost differential*. In this case, if a victim chooses not to pay ransom, they are monetized in a similar way as in a standard attack. We let $\tilde{\rho} > 0$ denote the return to an attacker under the ransomware scenario when either (i) the attacker enters with a standard attack or (ii) the attacker enters with ransomware, but the victim elects not to pay. Here, we permit $\tilde{\rho}$ under ransomware to differ from ρ under the benchmark because the existence of ransomware as well as differences in the post-crypto landscape can alter the cybercrime economy in ways that give rise to distinct returns under the two scenarios.

On the consumer side, unpatched consumers that are successfully attacked face a post-attack choice between paying the ransom to mitigate the loss or not paying the ransom and incurring the full loss. Following August et al. (2022), we assume that a victim that agrees to pay ransom will incur an additional residual loss $\delta\alpha v$ with $\delta \in [0,1)$ from the attack.[12] Suppose an attacker with

skill θ sets a ransom amount of R. Thus, if unpatched and hit by this attacker, a consumer of type v incurs a loss of $R + \delta\alpha v$ if they pay the ransom. However, they incur a loss of αv if they decide not to pay the ransom. Thus, the consumer pays ransom if and only if $R \le \alpha v(1-\delta)$. In that this depends on v, we define $R_{max}(v) = \alpha v(1-\delta)$ as the maximum ransom amount that a consumer of type v would be willing to pay if hit with ransomware. If they are hit by an attacker of type θ such that $R > R_{max}(v)$, then they would not pay that ransom. If they are hit by an attacker of type θ such that $R \le R_{max}(v)$, then they would pay the ransom. We define a ransom mapping $R(\theta) = R$ for all $\theta \in \Theta$ to represent a candidate set of ransoms.

Let $\tilde{\gamma} : \Theta \to S^a_{RW}$ and $\tilde{\sigma} : \mathcal{V} \to S^c_{RW}$ denote the strategy functions of the attackers and the consumers, respectively, based on the heterogeneity in each group. For the given attacker-consumer profile $\tilde{\Phi} = <\tilde{\gamma}, \tilde{\sigma}>$, the expected utility for a consumer with valuation v is given by

$$U^c_{RW}(v,\tilde{\Phi}) \triangleq \begin{cases} v - \kappa - c_p & \text{if } \tilde{\sigma}(v) = (A,P); \\ v - \kappa - q(a(\tilde{\Phi})) \times L(v) & \text{if } \tilde{\sigma}(v) = (A,NP); \\ 0 & \text{if } \tilde{\sigma}(v) = (NA,NP), \end{cases} \tag{7}$$

where the attacker population is given by $a(\tilde{\Phi}) \triangleq \int_\Theta \mathbb{1}_{\{\tilde{\gamma}(\theta) \neq NE\}} d\theta$ and the conditional expected loss if hit is $L(v) \triangleq L_1(v) + L_2(v)$. Here, $L_1(v)$ represents the conditional expected loss in the event the victim ends up paying ransom and is given by $L_1(v) = \int_\Theta [\mathbb{1}_{\{\tilde{\gamma}(\theta)=ER \cap R(\theta) \le R_{max}(v)\}} \times (R(\theta) + \delta\alpha v)] \times \frac{1}{a(\tilde{\Phi})} d\theta$. This loss is induced by attackers who enter with ransomware attacks and choose ransoms below the consumer of type v's maximum willingness to pay ransom. On the other hand, $L_2(v)$ represents the conditional expected loss in the event the victim is hit with a ransom amount higher than their maximum willingness to pay or is hit with a standard attack and can be expressed as $L_2(v) = \int_\Theta [\mathbb{1}_{\{(\tilde{\gamma}(\theta)=ER \cap R(\theta) > R_{max}(v)) \cup \tilde{\gamma}(\theta)=E\}} \times \alpha v] \times \frac{1}{a(\tilde{\Phi})} d\theta$.

Ransomware attacks and conventional attacks often exploit a vulnerability to gain access to a system and activate a backdoor. For example, a recent report by IBM (2023) identifies the deployment of backdoors as the most common approach across all types of cyberattacks in 2022. Consistent with these observations and to maintain parity across contexts, as in the *BM* scenario, we assume $q(a(\tilde{\Phi}))$ is the probability that a consumer is randomly hit by a security attack. Above, $1/a(\tilde{\Phi})$ is the conditional density of it originating from each type of entering attacker. As seen in (7), a user that adopts but does not patch ($\tilde{\sigma}(v) = (A,NP)$) incurs an expected security loss that accounts for the likelihood it falls victim to any of the attackers that enter the landscape (either paying ransom or incurring standard losses).

Again, $u(\tilde{\Phi}) \triangleq \int_\mathcal{V} \mathbb{1}_{\{\tilde{\sigma}(v)=(A,NP)\}} dv$ denotes the size of the unpatched adopter population. Similar to model *BM*, here we also omit subscript *RW* for quantities $u(\cdot)$ and $a(\cdot)$ for ease of exposition. However, we remind the reader that these quantities are endogenously determined in equilibrium and hence, potentially different under the two models. Given strategy profile $\tilde{\Phi}$, if an attacker sets a ransom amount of R, then the size of the unpatched adopter population that is willing to pay this ransom is given by

$$r(R,\tilde{\Phi}) \triangleq \int_\mathcal{V} \mathbb{1}_{\{\tilde{\sigma}(v)=(A,NP) \cap R_{max}(v) \ge R\}} dv. \tag{8}$$

For any of the unpatched systems, each attacker that enters the landscape has the same chance to be the one successfully compromising that system, at the rate $\frac{q(a)}{a}$. Hence, an attacker with type θ receives expected net utility:

$$U^a_{RW}(\theta,\tilde{\Phi}) \triangleq \begin{cases} \dfrac{q(a(\tilde{\Phi})) \times [\tilde{\rho} \times (u(\tilde{\Phi}) - r(R,\tilde{\Phi})) + R \times r(R,\tilde{\Phi})]}{a(\tilde{\Phi})} & \\ \quad -\tau(1-\theta)(1+\omega) & \text{if } \tilde{\gamma}(\theta) = (ER,R); \\ \dfrac{q(a(\tilde{\Phi})) \times \tilde{\rho} \times u(\tilde{\Phi})}{a(\tilde{\Phi})} - \tau(1-\theta) & \text{if } \tilde{\gamma}(\theta) = E; \\ 0 & \text{if } \tilde{\gamma}(\theta) = NE. \end{cases} \tag{9}$$

Notably, (9) is consistent with (4) when an attacker enters with standard attacks. However, for an attacker with type θ entering with ransomware and choosing ransom amount R, their payoff can come from two streams: (i) unpatched consumers who are willing to pay R (i.e., a group of size $r(R,\tilde{\Phi})$) and (ii) unpatched consumers who are not willing to pay R and get monetized in the standard way (i.e., the remainder of the unpatched population $u(\tilde{\Phi}) - r(R,\tilde{\Phi})$).

In equilibrium, when attackers choose to enter with ransomware, they have the flexibility to set a type-dependent ransom amount. However, attacker heterogeneity appears only at the entry cost level and does not impact the chance of a successful attack. Then conditional on entry with ransomware, all attackers face the same objective function when determining their optimal ransom. Consequently, in equilibrium, ransomware attackers will optimally set their ransom demand to a common endogenously determined amount $R(\theta) = R^*$, which is to say that their optimal ransoms do not depend on their type. In Online Appendices C and D, we present a generalized model with attacker heterogeneity impacting both revenues and costs that, in turn, leads to type-dependent ransom demands, and we illustrate the robustness of our results under this more

general setting. To streamline the exposition, we utilize the simplified model here in the main body of the paper.

Similar to the pre-crypto benchmark setting, under post-crypto ransomware setting, the market equilibrium has a threshold structure as follows.

Lemma 2. *In the post-crypto ransomware setting, the equilibrium attacker-consumer strategy profile* $\tilde{\Phi}^*_{RW} = <\tilde{\gamma}^*_{RW}, \tilde{\sigma}^*_{RW}>$ *is characterized by thresholds* $\tilde{v}_u, \tilde{v}_p, \tilde{\theta}, \hat{\theta} \in [0,1]$ *and ransom demand* R^**. For a consumer of type* $v \in \mathcal{V}$*, the optimal strategy* $\tilde{\sigma}^*_{RW}$ *satisfies*

$$\tilde{\sigma}^*_{RW}(v) = \begin{cases} (A,P) & \text{if } \tilde{v}_p < v \le 1; \\ (A,NP) & \text{if } \tilde{v}_u < v \le \tilde{v}_p; \\ (NA,NP) & \text{if } 0 \le v \le \tilde{v}_u. \end{cases} \tag{10}$$

For an attacker with type $\theta \in \Theta$*, the optimal strategy* $\tilde{\gamma}^*$ *satisfies*

$$\tilde{\gamma}^*_{RW}(\theta) = \begin{cases} (ER,R^*) & \text{if } \tilde{\theta} < \theta \le 1; \\ E & \text{if } \hat{\theta} \le \theta \le \tilde{\theta}; \\ NE & \text{if } 0 \le \theta < \hat{\theta}. \end{cases} \tag{11}$$

High valuation consumers continue to patch and protect their systems. On the other hand, mid- to high valuation consumers adopt and remain unpatched but elect to pay ransoms if ever hit. Low to mid valuation consumers also adopt and remain unpatched but instead elect not to pay ransoms when compromised. Finally, low valuation consumers choose not to adopt. In this case, the equilibrium unpatched population $u(\tilde{\Phi}^*_{RW}) = \tilde{v}_p - \tilde{v}_u$ (of which a subset will pay ransom, as described in (8), and a subset will not and incur standard losses instead) provides an incentive for attackers to enter the market and strike unpatched systems as seen in the utility function expressed in (9). Similar to the pre-crypto benchmark setting, attackers with types higher than $\hat{\theta}$ enter. This gives rise to the attack likelihood $q(a(\tilde{\Phi}^*_{RW}))$ where $a(\tilde{\Phi}^*_{RW}) = 1 - \hat{\theta}$, as seen in the consumer utility function expressed in (7).

3.3. Focal Region

In the following, we will narrow our attention to a subset of the parameter space, calling this our *focal region*. Although in the entirety of the parameter space, we can enumerate and characterize all the different market structures that obtain in equilibrium, we focus on the more salient ones that are typically observed in these practical software contexts. In particular, our focal region consists of the parameter conditions under which, in both pre-crypto benchmark (*BM*) and post-crypto ransomware (*RW*) settings, we have *all* consumer segments present with positive mass in equilibrium. Also, some attackers will choose to enter, whereas some will stay out of the market. Under *BM*, we have some consumers who opt out of the software, some who use the software but do not patch, and some who use the software and patch. Moreover, under *RW*, consumers that use the software but stay unpatched are split into those who pay ransom and those who do not.

The focal parameter region resembles market realities in that all consumers segments are in play. More specifically, we observe in practice the existence of both patched and unpatched user segments, with a portion of the latter segment paying ransom. In 2022, the majority of ransomware attacks exploited old, known bugs (Vijayan 2023). In fact, 76% of those flaws were from 2019 or before; thus, they were more than three years old at that time. All users had an option to protect but some chose not to do so. Consumers with greater valuation at risk prioritize patching soon after patch release, often using patch management solutions (Kaseya 2020, Polaris Market Research 2024).

In terms of the magnitude of the impact of the cyber-incidents on business consumers, as of 2024, according to analysis by Sophos, ransomware attacks exploiting *unpatched vulnerabilities* have the greatest business impact (Adam 2024). In particular, attacks that started with an exploited vulnerability succeeded in compromising backups in 75% of instances and were followed by data encryption in 67% of cases. With backups compromised and data encrypted, no less than 71% of these organizations chose to pay the ransom when the attack vector was an unpatched vulnerability (Adam 2024). Thus, in reality, the ransom-paying population represents a sizeable segment of the unpatched population.

The parameter conditions that give rise to equilibria matching these outcomes are a low software adoption cost ($\kappa < \overline{\kappa}$), a low residual loss to consumers who pay ransom ($\delta < \overline{\delta}$), an intermediate security loss factor ($\underline{\alpha} < \alpha < \overline{\alpha}$), an intermediate attacker entry cost parameter ($\underline{\tau} < \tau < \overline{\tau}$), an intermediate additional attacker entry cost associated with ransomware ($\underline{\omega} < \omega < \overline{\omega}$), and a sufficient attacker value from executing standard attacks in both benchmark ($\rho > \underline{\rho}$) and ransomware ($\tilde{\rho} > \underline{\tilde{\rho}}$) scenarios. The essence of the conditions is that parameter values need to be within a reasonable range such that consumer segments do not disappear and there is partial entry of attackers into the market. It is important to note that our focal region only serves to simplify the paper while still establishing the main insights; our insights can be shown to hold over broader regions and other market structures. We demonstrate the existence and characterization of the bounds denoted above in Online Appendix A.

4. Equilibrium Behavior Comparative Analysis

Users who choose to remain unpatched in equilibrium attract attackers and thereby contribute to losses across

the market due to this security externality. Hence, consumers' patching behavior is influenced by attacker entry behavior and vice versa. Before diving into the comparative analysis of the benchmark and ransomware scenarios, it is important to note that lower adoption costs tend to exacerbate the security landscape.

Remark 1. Under both pre-crypto benchmark and post-crypto ransomware settings, a decrease in consumer adoption cost (κ) leads to more attackers entering in equilibrium and hence higher security risk.

Taking κ smaller reflects the lower adoption costs associated with OSS, and Remark 1 emphasizes that higher security risk will result for such applications. Because lower adoption costs incentivize more consumers to use the software and some elect to do so in a risky, unpatched manner, a greater number of attackers find it beneficial to enter the market and cause this risk. In contrast, with proprietary software, the price serves dual purposes. Not only does it drive revenue for the vendor but, importantly, the price helps to shrink the user population (by increasing adoption costs) that provides less incentive for attackers to enter and reduces risk in turn.

Therefore, in the OSS world, it is important to examine how patching and attacking behaviors vary across the pre-crypto benchmark and post-crypto ransomware settings to understand how to better manage this critical driver of risk. In the following, we discuss how attacker entry and the equilibrium level of risk are impacted by cost changes associated with attacker technology.

Proposition 1. *An increase in attacker entry costs affects the size of the equilibrium attacker population differently under pre-crypto benchmark and post-crypto ransomware settings:*

(i) *In the pre-crypto benchmark setting, an increase in attacker entry costs always leads to fewer attackers in equilibrium and hence reduced security risk.*

(ii) *In the post-crypto ransomware setting, an increase in attacker entry costs can lead to either fewer or more attackers in equilibrium. Specifically, the size of the equilibrium attacker population and corresponding security risk increase when τ is intermediate and decrease (consistent with the pre-crypto benchmark setting) when τ is either small or large.*

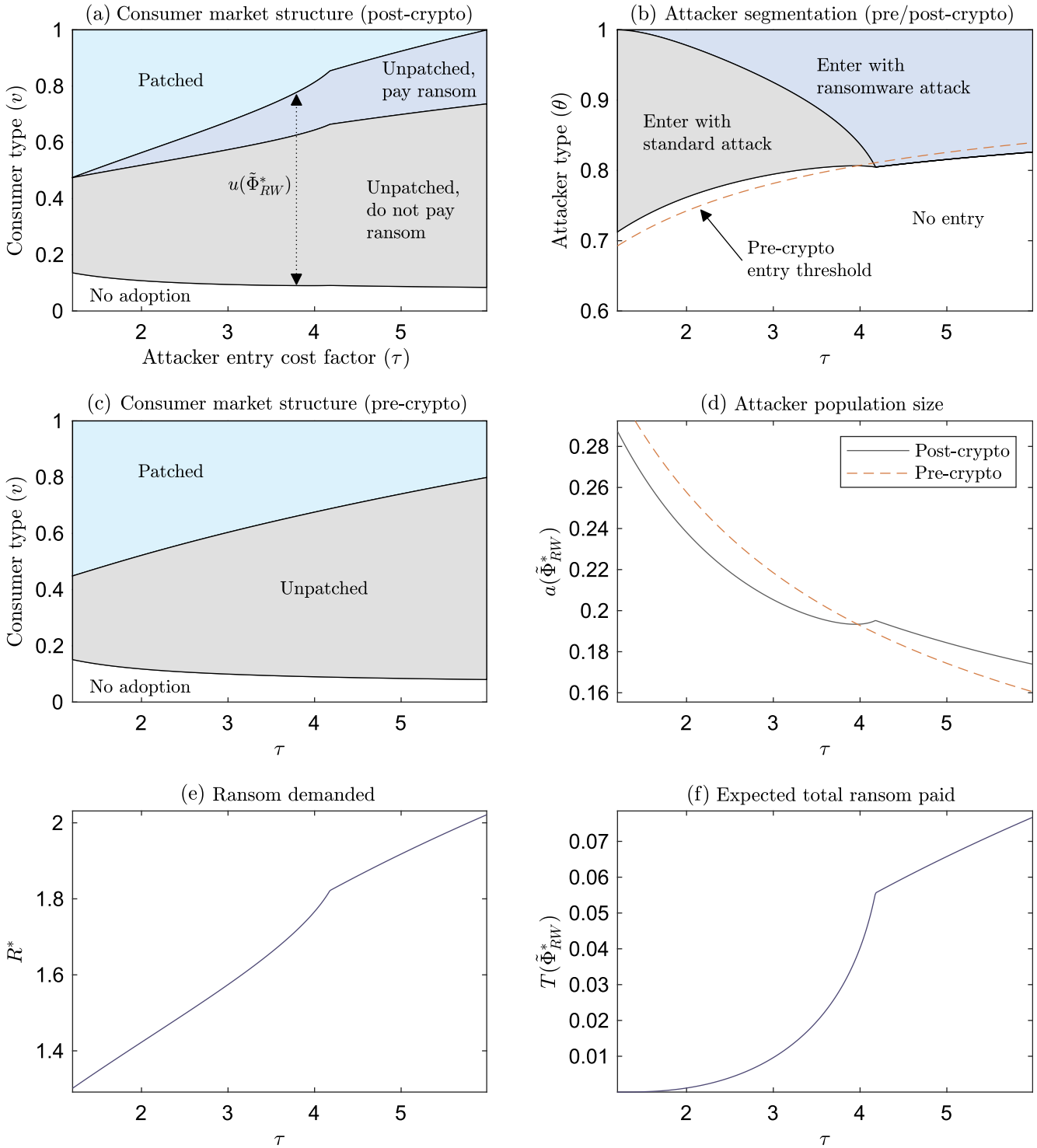
In this proposition, we study how the equilibrium and related metrics vary due to changes in attacker entry costs (τ). First, it is not simple to directly argue that there are less attackers when entry costs rise because any pressure that reduces attacker entry also reduces the risk faced by consumers, which, in turn, increases their incentive to use the software product in an unpatched manner, which indirectly increases the incentive for attackers to enter again. We begin by discussing the pre-crypto benchmark setting using a contradiction argument. Suppose that the attacker population a increases in the entry costs for some interval of τ. The probability a consumer is randomly hit, $q(a)$, increases in a; therefore, consumers bear more risk if choosing to be an unpatched user. By (2), the marginal consumer who is indifferent between being unpatched and not using will no longer use. Similarly, the marginal consumer who is indifferent between patching and being unpatched will shift toward patching. Altogether, u shrinks as a result. Examining the attacker utility in (4), both $q(a)/a$ and u are decreasing in a. Thus, the attacker's revenue decreases in tandem with an increase in entry cost, which would effectively reduce the attacker population in equilibrium, contradicting the supposition that a can be increasing in τ.

However, in the post-crypto ransomware setting, the decision problem is more complex for both consumers and attackers, which can lead to a different relationship between the equilibrium number of attackers and changes to the entry cost. First, note that an attacker always prefers to set a ransom that satisfies $R \geq \tilde{\rho}$ if it enters as a ransomware attacker because it can alternatively enter as a standard attacker and generate $\tilde{\rho}$ per victim. From a consumer standpoint, by (7) and because $R_{max}(v) = \alpha v(1-\delta)$, it is necessary that $\alpha v(1-\delta) > \tilde{\rho}$ for some consumers who choose to remain unpatched in equilibrium; otherwise, an attacker will prefer standard attacks.

We begin with τ near the lower end of the focal region. In this region, as τ declines, there is an incentive for a lot of attackers to enter at low cost which, in turn, is associated with a higher q and hence higher risk that all consumers face. As a result, consumers with higher valuations will have a greater incentive to patch and protect their systems, which is to say that the threshold valuation consumer who is indifferent between patching and not patching will have a tendency to decline. This behavior puts a downward pressure on the ransom price in that the attackers need consumers to be unpatched in equilibrium for attackers to thrive. In order to counter the decline of the aforementioned threshold valuation, attackers will reduce ransom price; however, attackers are willing do so to the extent that their ransom prices remain above $\tilde{\rho}$, as this is the outside option. Therefore, as τ gets small, at some point attackers run out of room to lower price and can no longer provide sufficient incentives for consumers to pay ransom. Because attackers vary in their additional cost of entry particular to ransomware, as τ gets small, more and more attackers switch from entering with ransomware to entering as standard attackers, and the landscape converges to the benchmark case.

When τ is in the middle range, the dynamics at play are significantly different due to attackers' strategic behavior as they sharply modify ransom prices and switch from standard attack to ransomware attack strategies. In Figure 2(e), we depict how the ransom price

Figure 2. (Color online) Impact of the Attacker Entry Cost Factor (τ) on Equilibrium Market Outcomes Under Pre-Crypto Benchmark and Post-Crypto Ransomware Settings



Note. The parameter values are $c_p = 0.3$, $\delta = 0.02$, $\kappa = 0.05$, $\alpha = 2.8$, $\rho = 1.6$, $\tilde{\rho} = 1.3$, $\omega = 0.1$, and $q(a) = 0.9a - 0.4a^2$.

increases as the cost of entry increases through the focal region. Notably, in the middle of the range, attackers choose in equilibrium to increase ransom prices nonlinearly. This occurs because τ reaches a level where a sufficient amount of attackers have exited the market due to the same driving effects discussed in the lower τ region. This smaller attacker population induces an increase in the unpatched population at the higher

portion of the valuation space as consumers strategically switch from being patched to being unpatched. This, in turn, permits higher ransom levels to be charged due to the higher valuations being present in the unpatched population. As τ increases, attackers simultaneously accelerate both the increase in ransom price and their transition away from standard attacks toward ransomware attacks as they benefit from these higher prices. This can be seen in panels (e) and (b), respectively, of Figure 2. This shift in attacker strategy toward ransomware attacks affects the composition of consumers' losses, with a significantly higher probability of being hit by ransomware attacks than standard attacks. However, losses in ransomware attacks are partially mitigated in that consumers can pay the ransom price whereas with standard attacks, victims can incur substantial losses as they are valuation dependent (see the bracketed expression in (7)); in fact, consumers can be better off with a greater proportion of ransomware attacks even if the ransom prices are somewhat higher. As such, unpatched usage also increases at an accelerated rate in τ as can be seen in panel (a) of Figure 2. This drastic increase in u encourages more attackers to enter the market as standard attackers as it dominates the negative impact of higher entry cost (τ) and crowding out effects on revenue (decreasing $q(a)/a$ in a). This increase in the attacker population can be seen in Figure 2(d).

As τ further increases, a point is reached where standard attacks are no longer sustained in equilibrium (e.g., this behavior can be seen around $\tau = 4.2$ in Figure 2(b) for this specific numerical illustration). Because attackers are no longer switching from standard attacks to ransomware attacks at this higher range of τ, the effect discussed above where the attacker population ultimately increases as a result is no longer present. This is because the unpatched population cannot be rapidly increased (as τ increases) without attackers significantly transitioning from entering with standard attacks to entering with ransomware. Solely manipulating the ransom price is insufficient to generate this effect. Instead, the attacker population will decrease in τ throughout this region that, in turn, leads to a relatively flatter increase (in comparison with the intermediate τ region) in the unpatched consumer population, which can be seen in panels (d) and (a), respectively, of Figure 2. Moreover, under higher τ, the attacker population decreases at a slower rate than seen in the benchmark case because attackers can leverage an ability to charge ransoms to higher valuation consumer types to preserve revenue.

Proposition 2. *Under the post-crypto ransomware setting, there exists $\hat{\tau} > 0$ such that, under the focal region, when $\tau > \hat{\tau}$, the ransom-paying population size, equilibrium ransom charged, and expected total ransom paid all strictly increase in τ, despite the attacker population size decreasing in τ.*

The consumer market equilibrium structure is characterized by threshold values $\tilde{v}_u$ and $\tilde{v}_p$ marking the indifference threshold between being an unpatched user and being a non-user and between being a patched and an unpatched user, respectively. Moreover, these thresholds satisfy $\tilde{v}_u < \frac{R^*}{\alpha(1-\delta)} < \tilde{v}_p$. Thus, we can define $\tilde{v}_r = \frac{R^*}{\alpha(1-\delta)}$ as the threshold, unpatched consumer indifferent between paying ransom and incurring losses. Therefore, the mass of consumers who are unpatched and prefer to pay ransom in equilibrium is $r(\cdot) = \tilde{v}_p - \tilde{v}_r$. Also, when $\tau > \hat{\tau}$ (in the numerical illustration in Figure 2, $\hat{\tau} \approx 4.2$), the attacker market equilibrium structure is characterized by a single threshold $\tilde{\theta}$ marking the attacker type who is indifferent between entering with ransomware and not entering the market.[13] Therefore, the mass of attackers entering in equilibrium is given by $a^* = 1 - \tilde{\theta}(\tau)$. For a given τ, the expected total ransom paid can then be computed as $T = q(1 - \tilde{\theta}(\cdot)) \times R^*(\cdot) \times r(\cdot)$.

Taking these three components one at a time, we begin with $q(\cdot)$. As τ reaches a higher level, by part (ii) of Proposition 1, the equilibrium number of attackers decreases in τ. As such, $q(a^*)$ decreases. For the second component, the equilibrium ransom $R^*(\cdot)$, with fewer attackers, there is an opportunity for more consumers to be remain unpatched. This, in turn, provides attackers with an ability to charge higher ransoms in that there are more higher valuation consumers remaining unpatched which can be monetized. As a result, attackers will set an optimal ransom that is gradually increasing in τ. Moving to the last component, $r(\cdot)$, a higher ransom can make some consumers less willing to pay this ransom, and this intuition is true for consumers near the $\tilde{v}_r$ threshold who will switch to not paying ransom. However, it turns out that consumers near the $\tilde{v}_p$ threshold have an incentive to switch *toward paying ransom* instead of patching due to the reduction in the number of attackers and reduced risk, despite the higher ransom. Examining the thresholds $\tilde{v}_r$ and $\tilde{v}_p$ in Figure 2(a), notably $\tilde{v}_p$ increases more sharply than $\tilde{v}_r$. Therefore, overall, the ransom paying population size r is increasing in τ throughout this region. Turning our attention to the expected total ransom paid, as τ increases, $q(\cdot)$ decreases, whereas $R^*(\cdot)$ and $r(\cdot)$ increase. The multiplicative effect of these latter two components dominate the decrease in risk, and hence the expected total ransom paid ultimately increases in τ. We illustrate this net effect in Figure 2(f).

Interestingly, this region is characterized by a higher ransom, a larger unpatched population (as well as a larger ransom-paying subset) and a higher expected total ransom being paid as τ grows. Nevertheless, the attacker population still decreases in aggregate. It is

important to further explore why this is the case and examine how attackers are differentially impacted by this shift in entry costs, which we study in the following proposition.

Proposition 3. *When the attacker entry cost parameter τ is at the higher end of the focal region, under both pre-crypto benchmark and post-crypto ransomware settings, an increase in attacker entry costs benefits some entering attackers while hurting others. Specifically, among attackers who enter in equilibrium, high-skill attacker utilities increase in τ, whereas low-skill attacker utilities decrease in τ.*

Technically, under the post-crypto ransomware setting, given $\tau \in (\hat{\tau}, \overline{\tau})$, there exists $\theta' \in (\hat{\theta}(\tau), 1)$ such that $\frac{dU^a_{RW}(\theta, \tilde{\Phi}^*)}{d\tau} < 0$ for all $\theta \in (\hat{\theta}(\tau), \theta')$, whereas $\frac{dU^a_{RW}(\theta, \tilde{\Phi}^*)}{d\tau} > 0$ for all $\theta \in (\theta', 1]$, where $\hat{\theta}(\tau)$ represents the type of the marginal attacker in the market as defined in Lemma 2. The statement under the pre-crypto benchmark setting is similar.

For the post-crypto ransomware setting, as we already established above, in this region, we have increasing equilibrium ransoms, increasing unpatched segment and as a subset, and increasing ransom-paying population, together with an increasing expected total ransom paid in association with an increase in attacker entry costs. As all these metrics increase, it follows from (9) that attacker revenue (the first part of the utility equation) is also increasing in τ for all remaining attackers in the market. Moreover, as previously discussed, attacker revenue is homogeneous across attackers (with heterogeneity manifested only at the entry cost level). Attackers with highest skills (θ close to one) will incur small entry costs which are offset entirely by the increase in revenue, resulting in such attackers being better off as attacker entry costs increase and additional less-skilled attackers drop out of the market, lowering competition. On the other hand, for attackers still in the market but with lower skill, the increase in entry costs takes a bigger toll on the overall utility, erasing the increase in revenue. This results in less-skilled attackers that are still in the market being negatively impacted by an increase in entry costs (with some attackers gradually peeling off). To sum up, while the overall attacker population declines in the attacker entry costs in this region, the impact is in fact positive for some attackers and negative for others.

For the pre-crypto benchmark setting, the argument is similar but simpler in that the revenue portion of the attacker utility function in (4) is more straightforward. Specifically, by part (i) of Proposition 1, a decreases in τ and thus $q(a)/a$ increases in τ. Moreover, the unpatched population increases due to the reduced risk from attackers. Thus, the revenue portion of the utility function increases in τ for all attackers who remain in the market. Similar to the ransomware scenario, the heterogeneity in entry cost leads to the higher-skilled attackers ultimately benefitting from the higher τ and the lower-skilled attackers being worse off.

5. Welfare Comparative Analysis

In this section, we conduct welfare sensitivity analysis and welfare comparisons across scenarios with respect to pertinent model parameters. Because cybercriminals engage in actions prohibited by criminal legislation, and moreover, they often operate outside the sovereign jurisdiction covering their victims, we exclude their criminal gains in our welfare analysis consistent with extant literature (see Lewin and Trumbull (1990) for an elaborate discussion on this topic). Therefore, welfare analysis in this context centers on consumer surplus. We use W_{BM} and W_{RW} to denote the equilibrium welfare metric under pre-crypto benchmark and post-crypto ransomware settings, respectively.

5.1. Impact of Market Primitives of Attackers (τ and $\tilde{\rho}$)

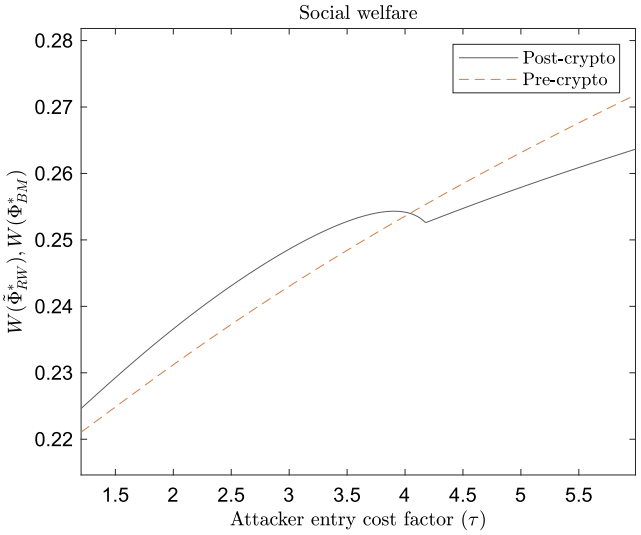
In this section, we discuss how attacker entry costs and gains from traditional attacks impact welfare.

Proposition 4. *In the focal region, the sensitivity of welfare to attacker entry costs is structurally different under pre-crypto benchmark and post-crypto ransomware settings. Under the pre-crypto benchmark setting, welfare always increases as attacker entry costs rise. However, under the post-crypto ransomware setting, welfare actually decreases in attacker entry costs when the latter are within an intermediate range. Outside of that range, the behavior is similar to that under the pre-crypto benchmark setting.*

The essence of Proposition 4 is illustrated in Figure 3. At first thought, one might expect social welfare to (weakly) increase in τ as increased efforts lead to less attackers, and hence lowered risk of a breach. Our result confirms this expectation in the benchmark scenario. However, as it turns out, in the post-crypto scenario, social welfare can actually decrease in τ. By part (ii) of Proposition 1, the size of the equilibrium attacker population and corresponding security risk increase when τ is intermediate. As discussed in Section 4 and illustrated in Figure 2, the effects are complex as this increase in attacker population occurs in tandem with the unpatched consumer population also unexpectedly increasing more steeply in τ in this subregion. This can be seen in Figure 2(a). This behavior, in turn, leads to a steeply increasing ransom being charged by attackers to opportunistically leverage the higher-valuation consumers who are electing to go unpatched which can be seen in Figure 2(e).

Unpacking the aggregate equilibrium movement in these metrics, the impact of a shift in τ on individual consumer decisions varies considerably depending on

Figure 3. (Color online) Impact of the Attacker Entry Cost Factor (τ) on Social Welfare Outcomes Under Pre-Crypto Benchmark and Post-Crypto Ransomware Settings



Note. The parameter values are $c_p = 0.3$, $\delta = 0.02$, $\kappa = 0.05$, $\alpha = 2.8$, $\rho = 1.6$, $\tilde{\rho} = 1.3$, $\omega = 0.1$, and $q(a) = 0.9a - 0.4a^2$.

the type of consumer and their strategic security choices. For example, if a consumer has a high valuation and finds it optimal to patch in equilibrium, then an increase in τ has no effect on the surplus of the consumer provided that they continue to patch. If a consumer prefers to patch but switches to being unpatched and paying ransom due to an increase in τ, then their surplus improves, by revealed preference, at the point where they switch. Next, for a consumer who does not change their strategy and still prefers to be unpatched and pay ransom as τ increases, the analysis is more complex. Consumers' surplus can either increase or decrease in τ depending on their type and the rate at which attackers transition from standard attack to ransomware attack strategies. Next, for a consumer who pays ransom and then switches to not paying due to an increase in τ and the associated increase in ransom, their surplus decreases in that the size of the attacker population increases in τ. The same situation unfolds for consumers who already preferred to be unpatched and not pay ransom even under the lower τ. Finally, some unpatched consumers who were not paying ransom are forced out of the market due to the increased risk which negatively affects consumer surplus. Taking all of these disparate impacts into account, Proposition 4 formally establishes that overall welfare ultimately declines as the attacker entry costs increase in this subregion, largely due to the stark increase in risk facing lower valuation consumers who remain in the market and the loss of consumers from the market.

Outside of the intermediate range of τ, the behavior in the post-crypto ransomware setting is similar in nature to that under the pre-crypto benchmark setting. As can be seen in Figure 2(d), the decrease in the attacker population in equilibrium is much steeper in the lower and upper τ regions in comparison with the intermediate τ region. As a result, the effect that stems from a decrease in security risk associated with the declining attacker population dominates the overall effect on welfare. Therefore, welfare increases in τ in the outer regions, consistent with Proposition 4 and Figure 3.

Next, we continue our exploration of the potential benefits of ransomware attacks on society by directly comparing welfare outcomes in the post-crypto ransomware setting to the pre-crypto benchmark setting. An important question is whether the addition of ransomware to the threat landscape, despite giving strategic attackers multiple ways to monetize victims, can benefit society. In the following proposition, we formally examine this question as moderated by the returns to post-crypto standard attacks and varying levels of attacker entry costs.

Proposition 5. *The societal impact of the presence of ransomware hinges on the returns to standard attacks under the post-crypto ransomware setting ($\tilde{\rho}$), the level of attacker entry costs (τ), and ransomware-specific cost differential (ω). Specifically, when ω is not too high,*

(i) *When $\tilde{\rho}$ is low, $W_{RW} > W_{BM}$ holds under both low and high τ;*

(ii) *When $\tilde{\rho}$ is moderate, $W_{RW} > W_{BM}$ continues to hold under low τ. However, W_{RW} and W_{BM} eventually cross, with $W_{BM} > W_{RW}$ obtaining under high τ;*

(iii) *When $\tilde{\rho}$ is high, $W_{BM} > W_{RW}$ holds under both low and high τ.*

First, we examine the most complex case which is part (ii) of Proposition 5. In this subcase, ω is low such that, post-crypto, attackers can enter with ransomware or standard attacks with a fairly similar cost structure. Moreover, the returns to standard attacks in the post-crypto setting, $\tilde{\rho}$, are at an intermediate range such that the benefits to attackers under the two settings (pre- and post-crypto) are more comparable. As attacker entry costs decrease toward the lower end of the focal region, the equilibrium outcome under the post-crypto ransomware setting is converging to only having standard attacks. This is because the risk is too high due to the size of the attacker population that enters, which drives higher valuation consumers to patch and leaves little ability for attackers to charge ransoms high enough to justify entering with ransomware. As τ increases from this boundary into an intermediate range, high-skill attackers now find it optimal to enter with ransomware with a ransom in excess of $\tilde{\rho}$ such that some consumers prefer to reduce costs by paying ransom instead of patching. In that the highest-skilled attackers have minimally greater costs from entering with ransomware in

comparison with entering with standard attacks, these attackers begin to enter with ransomware instead. As patched consumers shift over to being unpatched and pay ransoms, the unpatched population size increases relatively faster in the post-crypto ransomware setting compared with the benchmark. As a result, the attacker population also increases relatively faster due to the greater incentive. This leads to a decrease in the number of consumers under the *RW* setting, as consumers with lower valuations exit at the bottom of the market due to the increased risk associated with a larger attacker population. However, this negative impact on surplus is less than the positive impact associated with higher valuation consumers reducing costs by paying ransom instead of patching. Therefore, in aggregate, welfare is higher under *RW* than under *BM* when τ is low.

As the attacker entry cost moves to a high level, the equilibrium outcomes in the post-crypto ransomware and pre-crypto benchmark settings diverge. As discussed earlier, as τ gets high, attackers shift greatly toward ransomware strategies and away from standard attacks. As a result, the attacker population can be considerably larger under post-crypto ransomware setting than under benchmark. Comparatively, substantially fewer consumers will elect to use the software under the *RW* setting than under the *BM* setting due to the greater risk associated with this attacker population. Notably, the consumers who remain unpatched and do not pay ransom are also exposed to much greater risk, thereby incurring larger losses that negatively impact surplus. Altogether, under high attacker entry costs, welfare under post-crypto ransomware setting is much lower than under the benchmark setting due to these effects. In Figure B.1 in Online Appendix B, we numerically illustrate the cutoff value for τ that dictates whether welfare is higher under the post-crypto setting. We explore how the cutoff is impacted by patching cost, security losses, and the attacker gains pre-crypto.

Turning to part (iii) of Proposition 5, as $\tilde{\rho}$ becomes larger, it further encourages the entry of attackers under the post-crypto ransomware setting due to higher returns even with standard attacks. This significantly shifts the tradeoffs discussed above in the direction of the latter effects described where welfare is worse off under the *RW* setting, ultimately dominating for both low and high τ. For part (i) of Proposition 5, the effects shift in the opposing direction in that a low level of $\tilde{\rho}$ will ultimately shift more attackers toward entering with ransomware instead of standard attacks under the post-crypto setting. Moreover, post-crypto, attackers have a more difficult time justifying entering with a standard attack under the lower $\tilde{\rho}$. Therefore, some of these attackers with lower types will prefer to no longer enter the market. As a result, post-crypto, welfare can benefit both from fewer attackers in the market and from consumers who have more options to mitigate loss by paying ransom due to attackers who shifted attack modes.

A similar finding has been established in the context of an exogenous ransomware threat in August et al. (2022). Proposition 5 confirms the nuanced nature of this debate in the context of endogenous attackers. *Depending on the attacker primitives of the security landscape, the post-crypto ransomware setting may be more socially desirable than the pre-crypto benchmark setting from a security standpoint even in the presence of strategic attackers who are endogenously motivated by ransoms being paid and can choose an attack mode that maximizes their own gains.*

5.2. Impact of Market Primitives for Consumers (α and δ)

Next, we discuss the impact of the security loss factor versus the residual loss factor on welfare. Notably, security losses as dictated by parameter α exist under both pre-crypto benchmark and post-crypto ransomware settings. However, the residual loss parameter δ is only relevant under *RW* because it accounts for the *additional* losses sustained by consumers even though they paid the ransom that was demanded.

Proposition 6. *In the focal region, when τ is not too low, welfare decreases in α under both pre-crypto benchmark and post-crypto ransomware settings. However, welfare increases in δ under the post-crypto ransomware setting.*

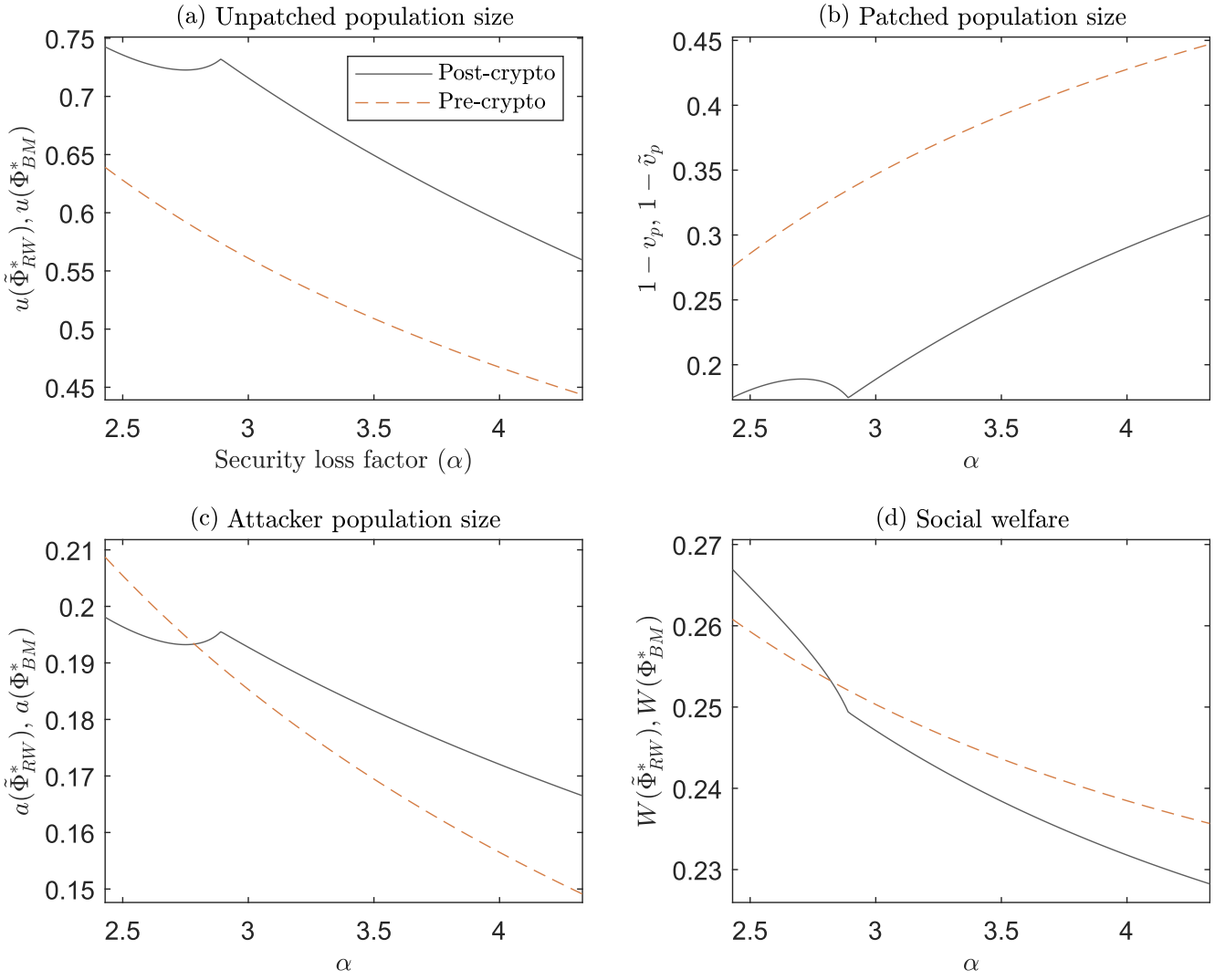
The benchmark scenario can be reasoned as follows. As α increases, there is a pressure on consumers at both ends of the market. Lower valuation consumers exit due to the increased risk, and higher valuation consumers shift toward patching. These two effects make the market less attractive to attackers, thus the attacker population also decreases. This slightly reduces risk for consumers, but the small decrease in attackers does not compensate for the overall higher losses associated with α. The net effect is a decrease in welfare.

The post-crypto scenario is more complex. In the higher range of α, attackers enter predominantly with ransomware attacks. In that range, the losses are so high that consumer demand shrinks, with exits at the bottom of the unpatched population (among consumers who were not willing to pay ransom). However, the difference between standard and residual losses ($(1-\delta)\alpha v$) also increases for remaining unpatched consumers, with increased pressure to patch for those with higher valuations. At the same time, attackers take advantage of an opportunity to increase ransom (given that paying ransom can mitigate a higher loss). Altogether, the compounded effect of higher losses and higher ransoms drives an increase in patching, depressing the unpatched segment. As a result, there is a decrease in the

attacker population; similar to the benchmark setting, that effect is not sufficient to counter the increase in losses on the consumer side, leading to an overall decrease in welfare under post-crypto ransomware setting too. For low α we see similar outcomes: Post-crypto, in that range, most attackers enter with standard attacks. As such, the increase in security losses has a strong impact on consumer welfare as there is a very limited chance to be attacked by ransomware and be able to mitigate such losses.

However, for α in the intermediate range of the focal region, the dynamics at play are more complex, similar to those captured under Propositions 1 and 4 with respect to changes in attacker entry costs (τ). Specifically, attackers will gradually shift from standard attacks toward ransomware attacks as α increases as consumer willingness to pay ransom increases. As the chance to be able to mitigate risk via paying ransom increases at an accelerated rate (i.e., victims are increasingly more likely to be hit with a ransomware rather than a standard attack), we see that both the attacker and the unpatched consumer populations actually increase in α, which represents a structural departure in sensitivity of such metrics compared with the pre-crypto scenario (as seen in panels (a) and (c) of Figure 4). Although fewer consumers patch at the top of the valuation spectrum, at the bottom, consumers still exit the market; hence, overall we have market shrinkage. For similar reasons as in the higher α region, attackers still find it optimal to jack up the ransom demanded. In this intermediate α region, while direct losses to consumers are more moderate, the added risk from the increase in attackers leads to a compounded negative effect of higher losses on welfare post-crypto. At first it might

Figure 4. (Color online) Impact of the Security Loss Factor (α) on Equilibrium Outcomes Under Pre-Crypto Benchmark and Post-Crypto Ransomware Settings



Note. The parameter values are $c_p = 0.3$, $\delta = 0.02$, $\kappa = 0.05$, $\tau = 4$, $\rho = 1.6$, $\tilde{\rho} = 1.3$, $\omega = 0.1$, and $q(a) = 0.9a - 0.4a^2$.

seem that the post-crypto welfare impacts of a shift in τ in the intermediate range and a shift in α in intermediate range differ in nature as only in the latter case does the welfare change exhibit monotonicity. However, that is not necessarily the case - in both instances (moving the attacker entry costs or the security losses) the momentary incentives for more attackers to join add even more stress to consumer welfare. As seen in Proposition 4 and Figure 3, that stress was enough to induce a decline in post-crypto welfare in intermediate τ, whereas in other regions an increase in τ benefits consumers. With sensitivity in α, post-crypto, for large and small losses regimes, consumers suffer if losses further increase, and this trend is actually *amplified* in the intermediate α range (as see in Figure 4(d) through a very fast decline in post-crypto welfare).

Now focusing solely on the post-crypto scenario, Proposition 6 reveals an interesting impact of residual losses on welfare. Although an increase in security losses (through α) has a negative impact on welfare, an isolated increase in residual losses after paying ransom (through δ), surprisingly, has a positive impact on welfare. As consumers are less able to mitigate losses through paying ransom, fewer will end up choosing that route. That lowers the ability of attackers to dip into the more lucrative revenue stream (via extortion), which, in turn, leads to a lot of attackers exiting the market. As such, the overall security risk in the market drops, which in turn benefits all unpatched consumers and even leads to an expansion of the market through entry at the low end of the valuation spectrum (as those consumers would not pay ransom and are unaffected by residual losses but they do benefit from an overall more secure market). For this reason, opportunities for very targeted policy interventions that shift δ higher and increase consumer burden when paying ransom may hold promise, as discussed in Section 6.

We conclude this welfare sensitivity analysis by emphasizing that, post-crypto, shifts in τ, α, and δ induce different correlations between movements in welfare and movements in attacker population, ransom demands, and expected total ransom paid. Shifts in τ in general move welfare and attacker population in opposite directions (e.g., achieving higher welfare comes with the bonus of fewer attackers), but higher welfare is associated with higher ransom amounts and total expected ransoms paid. Moreover, in the intermediate range of τ, higher attacker entry costs can actually shift welfare lower. On the other hand, shifts in α, for the most part, move welfare and attacker population in the same direction, which may seem to pose a dilemma depending on which metric policymakers try to impact (e.g., higher welfare is associated with more attackers in the market). However, there is an intermediate region where increasing α leads to greater attacker entry but only serves to sharply decrease welfare due to the accelerated shift toward ransomware attacks away from standard attacks. Last, shifting δ seems to align the effects in a way that may more easily justify policy action. Specifically, increases in welfare are correlated with decreases in attacker population, ransom demanded, and expected total ransom paid.

6. Potential Policy Implications

In our study, we focused on exploring the impact of market conditions on consumer and attacker behavior, and how, in turn, that affects security and welfare metrics. In this section, we comment on potential policy implications by connecting particular policies to the specific market parameters they can impact. The aim of our economic model is to highlight where policy may be fruitful by isolating specific parameters and shifting them to determine the aggregate impact of the shift on welfare. As policymakers can use multiple levers that shift multiple parameters concomitantly, the effects we demonstrate as theoretically possible in isolation can help to inform subsequent research that can substantiate the magnitude of these effects (in separate or combined form) and account for other policy-related concerns and roll-out costs which altogether can lead to sharp policy recommendations.

6.1. Ransomware Legislative Context

Although some more digitally savvy governments such as the U.S. government are well-versed at crypto tracing (House 2021), disruption of a currency explicitly designed to elude governmental control is a challenging task requiring extensive coordination and diplomacy (Geller 2021). Some proposed or enacted regulations require increased transparency around the operation of crypto exchanges and crypto operations in general. Although cryptocurrency exchanges in the United States are required to implement *antimoney laundering* (AML) measures including reporting of large transactions and *know-your-customer* (KYC) data collection, recently proposed bipartisan legislation in the United States, called the Digital Asset Anti-Money Laundering (DAAML) Act, advocates, among other things, for the extension of such regulations to the space of decentralized finance (DeFi) protocols and decentralized autonomous organizations (DAOs), effectively closing a loophole and bringing under AML oversight a significant and until-now largely unregulated part of the crypto industry (Lemire 2022, Lowe et al. 2023). In the European Union, updated AML (including KYC) standards around crypto transactions and the entities facilitating those will come into effect under the Markets in Crypto Assets (MiCA) regulation at the end of 2024, replacing the dated AMLD5 initiatives (Moody's 2022). In tackling the ransomware boom, international consensus is emerging that "consistent international scrutiny

of cryptocurrencies will be key" (Uberti 2021), with many territories following suit (Thompson Reuters 2022). Also some general security policies require reporting of ransom payments. Such legislation will help flag to a greater extent transactions related to ransomware attacks. A much brighter spotlight will be shined on *both* victims and ransomware cybercriminals.

Enhanced focus of law enforcement on ransomware operators and facilitators is also palpable. After the U.S. Department of Justice recovered $2.3 million in cryptocurrency following the DarkSide's extortion of Colonial Pipeline, Deputy Attorney General Lisa Monaco commented, "Ransom payments are the fuel that propels the digital extortion engine, and today's announcement demonstrates that the United States will use all available tools to make these attacks more costly and less profitable for criminal enterprises. We will continue to target the entire ransomware ecosystem to disrupt and deter these attacks" (U.S. DOJ 2021a). In addition to going directly after the ransomware cybercriminals, broader targeting of ecosystem facilitators is illustrated by the recent sanctions issued by the U.S. Department of the Treasury's Office of Foreign Assets Control against cryptocurrency exchanges such as OTC Suex, Chatex, Garantex, and Binance, as well as darknet market portals such as Hydra (Gkritsi 2021; U.S. Department of Treasury 2022, 2023). Utilizing a more coordinated approach to combat ransomware, in October 2021, the U.S. Department of Justice created the National Cryptocurrency Enforcement Team (NCET) "to tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors (U.S. DOJ 2021b).

6.2. Pre-Crypto vs. Post-Crypto Contexts

Other government and law enforcement measures target the ransomware cyberthreat explicitly. In the United States, although some radical measures such as a complete ban on ransomware payments have been floated and even partially implemented in a couple of states (Brumfield 2021, Ikeda 2022), such initiatives have been deemed infeasible, impractical, or suboptimal to fully implement at a federal level and hence momentarily abandoned (CNN 2021, Segal 2021, Wheeler and Martin 2021, Kapko 2022). However, suppose we entertain for a moment the possibility that such restrictive policies were feasible and that policymakers were able to implement measures that effectively and completely disincentivize such attacks. An important question in such a case would be the following: *is it socially optimal to get rid of the ransomware security threat altogether*? It turns out that the answer is complex. In Proposition 5, we formally establish that in a context with strategic attackers making entry and attack mode decisions and strategic consumers making security decisions, social welfare can still be higher in broad regions under the post-crypto scenario with the presence of ransomware.

However, recognizing the potential infeasibility of the most drastic approach, legislators and law enforcement are taking a more pragmatic approach by focusing on disrupting the processes and requirements around such transactions. In other words, *in the near future, instead of completely eliminating the ransomware threat altogether, policymakers aim to strategically contain it*, which we next discuss.

6.3. Attacker Entry Costs (τ and ω)

It is not a stretch to envision today's world more in the range of moderate rather than extreme (low or high) attack costs, consistent with our definition of the focal region. Realistically, policies to dial up or down the attack costs have only so much bite to them (i.e., can move τ only a limited amount), due in many cases to policies operating within territorial jurisdictions whereas attackers operate across physical borders (and, even then, as discussed in Proposition 4, policymakers should be aware of the directional impact as they dial the costs).

One way to increase attacker entry costs is to increase law enforcement resources, forge collaboration at both national and international level, encourage public-private partnerships, and initiate bounty programs to disrupt cybercrime and identify/apprehend operators (White House 2021, INTERPOL 2022, National Cybersecurity Alliance 2022, NSA 2024, U.S. Department of State 2025). Such initiatives increase the risk for cyber criminals to perpetrate the attacks in general, which can be quantified in our models through an increase in τ (i.e., the expected costs of attack campaigns increase due to higher risk of being caught).

Also, more specific to the post-crypto setting, crypto oversight legislation and ransomware-targeted law enforcement activity directly affect the entry cost of attackers. Closer monitoring of the ecosystem of ransomware facilitators and operators, along with aforementioned updated AML (including KYC) requirements on crypto transactions, as well as legislation that requires the reporting of ransom payments, will flag much faster the activity of ransomware operators and will require cybercriminals to jump through more complex hoops to be able to both collect ransom payments in crypto wallets and also withdraw those funds. The ransomware-specific entry costs are captured in our model by the parameter ω, and the crypto transactional costs can be captured by $s(\theta)$ introduced in a generalized model in the extension in Online Appendix C.1.

6.4. Consumer Security Losses (α)

Consumer losses are affected when legislation is enacted that indirectly impacts the IT security threat landscape through disclosure requirements. In March

2022, President Biden signed into law in the United States the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which mandated reporting of certain categories of cyber incidents by certain entities of national strategic importance (CISA 2022). In addition, in the particular case of data breaches, a swath of federal and state laws mandate various degrees of reporting in the United States (National Conference of State Legislatures 2022). In the European Union, data breach reporting requirements are stipulated under the General Data Protection Regulation (Intersoft Consulting 2023), and more general cyber incident reporting requirements for the financial sector are covered by the Digital Operations Resilience Act, which will enter in effect in early 2025 (Morgan Lewis 2024). Such policies can increase the impact of the attack on victims through a trust/reputation cost. In our model, this can be captured through a shift in parameter α (whether the victim incurs the full loss regardless of the attack type, or the residual losses in case of electing to pay ransom).

6.5. Consumer Residual Losses Under Ransomware (δ)

AML (and KYC) legislation adds regulatory burden and increased reputation risk on the victim side explicitly in the case of crypto ransom payments. The recently proposed Ransomware and Financial Stability Act of 2024 would require further scrutiny and approval by law enforcement for ransomware payments in excess of $100K (U.S. Congress 2024). Hence, in our framework, we can link the impact of such initiatives to shifts in δ, the coefficient of residual losses (which encompass all additional costs incurred by the victims in the wake of making a ransom payment). More precisely, on the victims' side, we postulate that such polices will likely lead to an increase in δ. Taken in isolation (ignoring for the moment the effect on attackers), such an effect can lead to resistance to related regulation due to perceived added burden on the victims. At first glance, one might intuitively expect that, as residual losses increase, the ability of consumers to mitigate risk via the ransom payment option decreases, which, in turn, might lead to reduced welfare. However, Proposition 6, establishes there are regions under which welfare actually increases in δ due to the strategic reaction by attackers.

7. Concluding Remarks

To better understand the impact of cryptocurrencies on the cybersecurity landscape, we conduct a comparative analysis of cybersecurity metrics and social welfare prior to and after the adoption of cryptocurrency. To that end, our modeling contribution is the development of a series of connected software-use models in the presence of security externalities, where consumers and attackers endogenously determine this risk, specifically with a *continuum of heterogeneous attackers making entry, attack mode (ransomware or traditional attacks), and ransom decisions.* Leveraging these models, we explore how market parameters impact outcomes under both pre-crypto benchmark and post-crypto ransomware threat landscapes. We show theoretically that post-crypto scenarios that include ransomware threats can be more socially desirable than pre-crypto, conventional threat scenarios when it is not too costly for attackers to enter the market. Hence, the existence of crypto-fueled ransomware, in itself, is not necessarily bad for cybersecurity and welfare.

We further show that directional effects (such as increasing attacker entry costs improving welfare), which hold under conventional attacks, do not necessarily obtain under the ransomware scenario. For example, rather than mitigating the ransomware threat, raising attacker costs can sometimes result in increased attacker entry and harm overall welfare. Moreover, increasing attacker entry costs can have secondary effects including bigger ransoms demanded, larger ransom-paying population segments, and higher expected total ransom paid. We also study in a similar way the impact of security losses as well as residual losses on these metrics. Altogether, the study of these effects offers great value to policymakers as they consider cybersecurity and crypto policies to drive these market parameters toward more favorable outcomes for society.

Our work's focus is on establishing theoretical possibilities, with future empirical work needed to assess the actual prevalence and magnitude of the outcomes we characterize. Our results are intended as an initial exploration to shed light into how shifting directional forces in isolation (i.e., one market parameter at a time) can alter the dynamics of the cybersecurity landscape, especially in the post-crypto era. Thus, quantities are normalized and a certain level of abstraction is applied to enable an in-depth analysis of the specific dynamics at play.

The derived findings serve to inform policymakers of the need to consider more complex policies (or packages of multiple policies in tandem) that apply cybersecurity interventions on multiple dimensions concomitantly. Such complex regulations may be able to achieve welfare benefits without some of the secondary aforementioned effects. This presents great opportunities for further exploratory research into how to regulate crypto and its impact on cybersecurity. Our initial exploration looks at welfare effects net of any implementation costs required to induce a directional shift in market primitives (i.e., costs associated with policy roll out). Armed with accurate estimates of these costs, future work can perform comprehensive analyses and provide policy recommendations aimed at inducing the effects we highlight.

Another potential direction of future research is to expand the model framework to examine the interaction

between user decisions and the additional options and costs that exist in the cybersecurity ecosystem. In our paper, we focus on users' adoption costs and patching costs as they decide whether to use a system and patch it in the face of potential cybersecurity attacks and cognizant of the externality imposed by their patching behavior on attackers' entry incentives. More generally, users also have the option to purchase cyberinsurance which can interact with their adoption and patching decisions and lead to riskier behaviors. There can also possibly be valuation-independent incident reporting costs mandated by the government when systems are breached that are not captured solely by an increase in our α parameter. We acknowledge that the focal costs captured by our model provide a lower bound to the user costs present in a broader cybersecurity context, and we believe our work can provide a foundation to explore these additional factors.

Our work identifies effects on cybersecurity metrics (such as ransom payments) as well as welfare. Sometimes they move in the same direction as market parameters shift and sometimes not. Because ransom payments can be directly observable on public blockchains but welfare is more difficult to measure, an interesting extension on the policy front would be to examine scenarios in which planners rely on public blockchains to peek into certain ransomware activity (including volume and destination of transactions), utilizing readily observable signals to inform and manage post-crypto cybersecurity policy agenda. Other interesting avenues for future research include exploring how the subsidization of patching costs or the taxation of ransomware payments (in addition to other regulations such as AML-mandated reporting) can influence the comparison between pre-crypto and post-crypto attack metrics.

Acknowledgments

The authors are listed in alphabetical order and have equally contributed to this work. The authors thank Kay Giesecke (the department editor), the associate editor, and anonymous reviewers for valuable comments and suggestions throughout the review process. The authors also thank the participants in the research seminar at Heinz College at Carnegie Mellon University for helpful discussions and feedback.

Endnotes

[1] The first documented ransomware attack, the AIDS Trojan (also called the "P.C. Cyborg attack") occurred in 1989 (Murphy-Kelly 2021).

[2] The Apache Log4j (Log4Shell) Java logging vulnerability, which exposed a large swath of web servers and services (including those using VMware Horizon) has been extensively used in the deployment of ransomware attacks starting at the end of 2021 and throughout 2022 (Arctic Wolf Labs 2022, Tung 2022). DarkRadiation, written in Bash script that targeted Red Hat, CentOS, and Debian Linux distributions as well as Docker cloud containers was spread via an SSH worm (Lakshmanan 2021, Zahravi 2021). Attackers such as the notorious REvil gang who was responsible for shutting down the operations of JBS, the world's largest meat supplier, and extorting $11 million in ransom, are now porting their ransomware to Linux (Vanian 2021). Being able to attack bare metal hypervisors like VMware's ESXi, as well as Linux-based network storage devices, is a lucrative opportunity for hackers; indeed, ransomware strains DarkSide and RansomEXX have evolved with OSS in their sights (Spring 2021, Winder 2021). Year 2022 saw an acceleration of Linux encryptors being developed and deployed by the most prominent ransomware gangs including, in addition to the aforementioned examples, Conti, LockBit, HelloKitty, AvosLocker, Babuk, PureLocker, Mespinoza, Hive, and IceFire (Gatlan 2023).

[3] Throughout the exposition, we use these terms interchangeably.

[4] For example, our model can inform in-use software with sunk costs. Focusing on the population of *existing* users, we can explore how, based on residual value of the product, consumers decide whether to abandon the product or continue to use it and adjust their security strategy based on the perceived threat landscape.

[5] In general, our analysis applies to all users, individual and business, in that decisions in the model are made on a per-system basis. Business users can be expected to have multiple systems, and can make separate adoption and patching decisions on each of these systems separately. As long as business users only make decisions for a countable set of systems, our model can capture such complexities in business where many systems are managed by a corporate entity. For example, even a year after WannaCry ransomware worm was unleashed, Boeing corporation still had not patched a small number servers in their Commercial Airplanes division, and these systems ended up being compromised in March 2018 in a fairly isolated incident (Gates 2018).

[6] The adoption cost accounts for piloting, configuring and integrating the software with business processes.

[7] The patching cost accounts for the money and effort that a consumer must exert in order to verify, test, and roll-out patched versions of existing systems.

[8] We assume that the variable cost to replicate the attacks on multiple victim systems is negligible compared to the one-time cost to develop/configure needed malware tools and learn how to utilize them to perpetrate such attacks (e.g., some malware are designed with worm-like self-replicating capabilities which automate spread).

[9] We assume imperfect information in both pre-crypto and post-crypto contexts such that agents only know their own types, as well as the overall type distributions. Attackers cannot directly observe valuations, and therefore can only make strategic decisions based on inferred consumer thresholds in equilibrium.

[10] For simplicity, we assume that all attacked victims will address the vulnerability to prevent future attacks, such that the probability of successful repeat attacks on the same system is negligible.

[11] There are additional costs associated with setting up and configuring systems to support the interactions of the ransom process, including the handling of crypto transactions, the encryption of data, and the generation and passing of decryptor tools, in addition to costs to reduce the risk of being caught.

[12] Research indicates that total ransom attack losses can be as high as seven times the ransom demand (Blosil 2022). A study by IBM Security (2022) reports victims incurring average ransomware costs of $4.54 million in excess of the ransom demand. Residual losses can be due to investigation and remediation, lawsuits, reputation impact, etc.

[13] This is because $\hat{\theta} = \tilde{\theta}$ in Equation (11) of Lemma 2 in this particular region.

References

Adam S (2024) Unpatched vulnerabilities: The most brutal ransomware attack vector. *Sophos News* (April 3), https://news.sophos.com/en-us/2024/04/03/unpatched-vulnerabilities-the-most-brutal-ransomware-attack-vector/.

Ahnert T, Brolley M, Cimon D, Riordan R (2022) Cyber security and ransomware in financial markets. Accessed July 2022, https://doi.org/10.34989/swp-2022-32.

Arctic Wolf Labs (2022) A Log4Shell (Log4j) retrospective. Accessed December 19, 2024, https://arcticwolf.com/resources/blog/log4j-retrospective/.

August T, Tunca TI (2006) Network software security and user incentives. *Management Sci.* 52(11):1703–1720.

August T, Tunca TI (2011) Who should be responsible for software security? A comparative analysis of liability policies in network environments. *Management Sci.* 57(5):934–959.

August T, Dao D, Kim K (2019) Market segmentation and software security: Pricing patching rights. *Management Sci.* 65(10):4451–4949.

August T, Dao D, Niculescu MF (2022) Economics of ransomware: Risk interdependence and large-scale attacks. *Management Sci.* 68(12):8979–9002.

Badea L, Mungiu-Pupazan MC (2021) The economic and environmental impact of Bitcoin. *IEEE Access* 9:48091–48104.

Balasubramanian A (2021) Insurance against ransomware. Preprint, submitted May 18, https://dx.doi.org/10.2139/ssrn.3846111.

Bariviera AF, Merediz-Solà I (2021) Where do we stand in cryptocurrencies economic research? A survey based on hybrid analysis. *J. Econom. Surveys* 35(2):377–407.

Black DB (2022) Cryptocurrency fuels growth of crime. Accessed December 19, 2024, https://www.forbes.com/sites/davidblack/2022/03/11/cryptocurrency-fuels-explosive-growth-of-crime/.

Black Duck (2024) Open source security and risk analysis report. Accessed December 19, 2024, https://www.blackduck.com/resources/analyst-reports/open-source-security-risk-analysis.html.

Blosil J (2022) Measuring the true cost of a ransomware attack. *NetApp* (October 22), https://www.netapp.com/blog/ransomware-cost/.

Böhme R, Schwartz G (2010) Modeling cyber-insurance: Towards a unifying framework. *Proc. Workshop Econom. Inform. Security* (Harvard University, Cambridge, MA).

Brumfield C (2021) Four states propose laws to ban ransomware payments. *CSO* (June 28), https://www.csoonline.com/article/570895/four-states-propose-laws-to-ban-ransomware-payments.html.

Cartwright A, Cartwright E (2019) Ransomware and reputation. *Games* 10(2):26.

Cartwright A, Cartwright E (2023) The economics of ransomware attacks on integrated supply chain networks. *Digital Threats* 4(4):1–14.

Cartwright E, Hernandez Castro J, Cartwright A (2019) To pay or not: Game theoretic models of ransomware. *J. Cybersecurity* 5(1):1–12.

Cavusoglu H, Cavusoglu H, Raghunathan S (2007) Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. *IEEE Trans. Software Engrg.* 33(3):171–185.

Chainalysis (2024) Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 decline. Accessed December 19, 2024, https://www.chainalysis.com/blog/ransomware-2024/.

Choi JP, Fershtman C, Gandal N (2010) Network security: Vulnerabilities and disclosure policy. *J. Industrial Econom.* 58(4):868–894.

Cisa (2022) Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Accessed December 19, 2024, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

CNN (2021) FBI tells Congress ransomware payments shouldn't be banned. Accessed December 19, 2024, https://www.cnn.com/2021/07/27/politics/senate-judiciary-ransomware-hearing/index.html.

Crowdstrike (2022) History of ransomware. Accessed December 19, 2024, https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.

Dey D, Lahiri A (2021) Should we outlaw ransomware payments? *Proc. 54th Hawaii Internat. Conf. System Sci.* 6609–6617.

Dey D, Lahiri A, Zhang G (2015) Optimal policies for security patch management. *J. Comput.* 27(3):462–477.

DuBois EB, Peper A, Albert LA (2023) Interdicting attack plans with boundedly-rational players and multiple attackers: An adversarial risk analysis approach. Preprint, submitted February 3, https://arxiv.org/abs/2302.01975.

Fang R, Xu M, Zhao P (2022) Determination of ransomware payment based on Bayesian game models. *Computers Security* 116(May):102685.

FinCEN (2022) Financial trend analysis: Ransomware trends in Bank Secrecy Act data between July 2021 and December 2021. US Treasury. Accessed December 19, 2024, https://www.fincen.gov/sites/default/files/2022-11/Financial\%20Trend\%20Analysis_Ransomware\%20FTA\%202_508\%20FINAL.pdf.

Foley S, Karlsen JR, Putnins TJ (2019) Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *Rev. Financial Stud.* 32 (5):1798–1853.

Gal-Or E, Ghose A (2005) The economic incentives for sharing security information. *Inform. Systems Res.* 16(2):186–208.

Galinkin E (2021) Winning the ransomware lottery: A game-theoretic approach to preventing ransomware attacks. Bošanský B, Gonzalez C, Rass S, Sinha A, eds. *Proc. 12th Internat. Conf. Decision Game Theory Security* (Springer, Cham, Switzerland), 195–207.

Garcia E, Moll AV, Casbeer DW, Pachter M (2019) Strategies for defending a coastline against multiple attackers. *Proc. IEEE 58th Conf. Decision Control* (IEEE, Piscataway, NJ), 7319–7324.

Gates D (2018) Boeing hit by WannaCry virus, but says attack caused little damage. *Seattle Times* (March 28), https://www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/.

Gatlan S (2023) IceFire ransomware now encrypts both Linux and Windows systems. *BleepingComputer* (March 9), https://www.bleepingcomputer.com/news/security/icefire-ransomware-now-encrypts-both-linux-and-windows-systems/.

Geller E (2021) Global 'whack-a-mole': Why it's so hard for the U.S. to go after hackers' digital wallets. *Politico* (August 14), https://www.politico.com/news/2021/08/14/crypto-hackers-ransomware-fight-504460.

GitHub (2024) Octoverse: The state of open source and rise of AI in 2023. Accessed December 19, 2024, https://github.blog/news-insights/research/the-state-of-open-source-and-ai/.

Gkritsi E (2021) Biden administration sanctions crypto exchange chatex over ransomware allegations. *Coindesk* (November 9), https://www.coindesk.com/policy/2021/11/09/biden-administration-sanctions-crypto-exchange-chatex-over-ransomware-allegations/.

Halaburda H, Haeringer G, Gans JS, Gandal N (2020) The microeconomics of cryptocurrencies. NBER Working Paper No. 27477, National Bureau of Economic Research, Cambridge, MA.

Hausken K, Bier VM (2011) Defending against multiple different attackers. *Eur. J. Oper. Res.* 211(2):370–384.

Hernandez-Castro J, Cartwright A, Cartwright E (2020) An economic analysis of ransomware and its welfare consequences. *R Soc. Open Sci.* 7(3):190023.

House B (2021) U.S. plans to counter ransomware attacks through crypto tracing. *Bloomberg* (July 14), https://www.bloomberg.com/news/articles/2021-07-15/u-s-plans-to-counter-ransomware-attacks-through-crypto-tracing.

IBM (2023) IBM report: Ransomware persisted despite improved detection in 2022. Accessed December 19, 2024, https://newsroom.ibm.com/2023-02-22-IBM-Report-Ransomware-Persisted-Despite-Improved-Detection-in-2022.

IBM Security (2022) Cost of a data breach report 2022. Accessed December 19, 2024, https://www.ibm.com/downloads/cas/3R8N1DZJ.

Ikeda S (2022) Patchwork of US state regulations becomes more complex as Florida, North Carolina ban ransomware payments. *CPO Magazine* (August 19), https://www.cpomagazine.com/cyber-security/patchwork-of-us-state-regulations-becomes-more-complex-as-florida-north-carolina-ban-ransomware-payments/.

INTERPOL (2022) INTERPOL cybercrime capacity building project in the Americas, phase II. Accessed December 19, 2024, https://www.interpol.int/News-and-Events/News/2022/INTERPOL-Working-Group-highlights-cyber-threats-across-the-Americas.

Intersoft Consulting (2023) Art. 33 GDPR: Notification of a personal data breach to the supervisory authority. Accessed December 19, 2024, https://gdpr-info.eu/art-33-gdpr/.

Ioannidis C, Pym D, Williams J (2012) Information security trade-offs and optimal patching policies. *Eur. J. Oper. Res.* 216(2): 434–444.

Jeffery L, Ramachandran V (2021) Why ransomware attacks are on the rise—And what can be done to stop them. *PBS News Hour, Nation* (July 8), https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them.

Kapko M (2022) US government rejects ransom payment ban to spur disclosure. *Cybersecurity Dive* (September 19), https://www.cybersecuritydive.com/news/government-ransomware-guidance/632136/.

Kaseya (2020) The 2019 Kaseya state of IT operations report for small and midsized businesses. Accessed December 18, 2024, https://www.kaseya.com/wp-content/uploads/dlm_uploads/2020/05/Kaseya-Whitepaper-2019-IT-Operations-Survey-Report.pdf.

Lakshmanan R (2021) Wormable DarkRadiation ransomware targets Linux and Docker instances. *The Hacker News* (June 22), https://thehackernews.com/2021/06/wormable-darkradiation-ransomware.html.

Laszka A, Farhang S, Grossklags J (2017) On the economics of ransomware. *Proc. 8th Internat. Conf. Decision Game Theory Security* (Springer, New York), 397–417.

Lemire KA (2022) Cryptocurrency and anti-money laundering enforcement. *Reuters* (September 26), https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26/.

Levy A (2024) 8 benefits of cryptocurrency & Why you should use it. *The Motley Fool* (September 11), https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/benefits-of-cryptocurrency/.

Lewin JL, Trumbull WN (1990) The social value of crime? *Internat. Rev. Law Econom.* 10(3):271–284.

Li Z, Liao Q (2020) Ransomware 2.0: To sell, or not to sell: A game-theoretical model of data-selling ransomware. *Proc. 15th Internat. Conf. Availability Reliability Security*, 1–9.

Li X, Whinston A (2020) The economics of cyber crime. Preprint, submitted June 11, https://dx.doi.org/10.2139/ssrn.3603694.

Lowe MS, Ostroff EG, Rogers SF (2023) Bank Secrecy Act's crypto expansion is on the horizon. *Law360* (February 7), https://www.law360.com/articles/1573438.

Maudrill B (2024) Sonatype reports 156% increase in OSS malicious packages. *Infosecurity Magazine* (October 11), https://www.infosecurity-magazine.com/news/156-increase-in-oss-malicious/.

Mitra S, Ransbotham S (2015) Information disclosure and the diffusion of information security attacks. *Inform. Systems Res.* 26(3):565–584.

Moody's (2022) What does the proposed EU markets in Crypto-Assets Act (MiCA) mean for the industry? Accessed December 19, 2024, https://kyc.moodys.io/content-highlights-section/what-does-proposed-eu-markets-crypto-assets-act-mica-mean-industry.

Morgan Lewis (2024) Preparing for DORA: ESAs publish incident reporting requirements. Accessed December 19, 2024, https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/08/preparing-for-dora-esas-publish-incident-reporting-requirements.

Murphy-Kelly S (2021) The bizarre story of the inventor of ransomware. *CNN* (May 16), https://www.cnn.com/2021/05/16/tech/ransomware-joseph-popp/index.html.

National Conference of State Legislatures (2022) Summary: 2022 security breach legislation. Accessed December 19, 2024, https://www.ncsl.org/technologyand-communication/2022-security-breach-legislation.

National Cybersecurity Alliance (2022) Cybersecurity collaboration as a national imperative. Accessed December 19, 2024, https://www.staysafeonline.org/articles/cybersecurity-collaboration-as-a-national-imperative.

NSA (2024) NSA Cybersecurity Collaboration Center. Accessed December 19, 2024, https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/.

Polaris Market Research (2024) Patch management market. Accessed December 18, 2024, https://www.polarismarketresearch.com/industry-analysis/patch-management-market.

Red Hat (2021) *The State of Enterprise Open Source* (Red Hat, Raleigh, NC).

Ryan P, Fokker J, Healy S, Amann A (2022) Dynamics of targeted ransomware negotiation. *IEEE Access* 10:32836–32844.

Schryen G, Rich E (2010) Increasing software security through open source or closed source development? Empirics suggest that we have asked the wrong question. *Proc. 43rd Hawaii Internat. Conf. System Sci.* (IEEE, Piscataway, NJ), 1–10.

Segal E (2021) Banning ransomware payments could create new crisis situations. *Forbes* (June 8), https://www.forbes.com/sites/edwardsegal/2021/06/08/banning-ransomware-payments-could-create-new-crisis-situations/.

Selten R (1988) Models of strategic rationality. *A Simple Game Model of Kidnapping* (Theory and Decision Library C. Springer, Dordrecht, Netherlands), 77–93.

Spring T (2021) Linux variant of REvil ransomware targets VMware's ESXi, NAS devices. *ThreatPost* (July 1), https://threatpost.com/linux-variant-ransomware-vmwares-nas/167511/.

Statista (2024) Number of supply chain attacks on open source software (OSS) from 2019 to 2023. Accessed December 19, 2024, https://www.statista.com/statistics/1268934/worldwide-open-source-supply-chain-attacks/.

Swire PP (2005) A theory of disclosure for security and competitive reasons: Open source, proprietary software, and government systems. *House Law Rev.* 42:1333.

Thompson Reuters (2022) Cryptocurrency regulations by country. Accessed December 19, 2024, https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf.

Tung L (2022) Ransomware: Hackers are using Log4j flaw as part of their attacks, warns Microsoft. *ZDNET* (January 11), https://www.zdnet.com/article/ransomware-warning-hackers-are-using-log4j-flaw-as-part-of-their-attacks-warns-microsoft/.

Uberti D (2021) White House ransomware summit eyes tighter global scrutiny for crypto. *Wall Street Journal* (October 14), https://www.wsj.com/articles/white-house-ransomware-summit-eyes-tighter-global-scrutiny-for-crypto-11634227377.

United Kingdom (2016) National cyber security strategy 2016–2021. Accessed December 19, 2024, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

U.S. Congress (2024) H.R.7965 - Ransomware and Financial Stability Act of 2024. Accessed December 19, 2024, https://www.congress.gov/bill/118th-congress/house-bill/7965/all-info.

U.S. Department of State (2025) Rewards for justice. Accessed February 13, 2025, https://www.state.gov/rewards-for-justice/.

U.S. Department of Treasury (2022) Treasury sanctions Russia-based Hydra, world's largest darknet market, and ransomware-enabling virtual currency exchange Garantex. Accessed December 19, 2024, https://home.treasury.gov/news/press-releases/jy0701.

U.S. Department of Treasury (2023) U.S. treasury announces largest settlements in history with world's largest virtual currency exchange Binance for violations of U.S. anti-money laundering and sanctions laws. Accessed December 19, 2024, https://home.treasury.gov/news/press-releases/jy1925.

U.S. DOJ (2021a) Department of Justice Seizes $2.3 million in cryptocurrency paid to the ransomware extortionists darkside. Accessed December 19, 2024, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

U.S. DOJ (2021b) Deputy attorney general Lisa O. Monaco announces National Cryptocurrency Enforcement Team. Accessed December 19, 2024, https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team.

Vakilinia I, Khalili MM, Li M (2021) A mechanism design approach to solve ransomware dilemmas. *Proc. 12th Internat. Conf. Decision Game Theory Security* (Springer, New York), 181–194.

Vanian J (2021) Everything to know about REvil, the group behind a big ransomware spree. *Fortune* (July 7), https://fortune.com/2021/07/07/what-is-revil-ransomware-attack-kaseya/.

Vijayan J (2023) Majority of ransomware attacks last year exploited old bugs. *Dark Reading* (February 20), https://www.darkreading.com/cyberattacks-data-breaches/dozens-of-vulns-in-ransomware-attacks-offer-adversaries-full-kill-chain/.

Wheeler T, Martin C (2021) Should ransomware payments be banned? *Brookings* (July 26), https://www.brookings.edu/techstream/should-ransomware-payments-be-banned/.

White House (2021) Executive order on improving the nation's cybersecurity. Accessed February 13, 2025, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

White House (2023) National cybersecurity strategy. Accessed February 13, 2025, https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/.

Winder D (2021) New ransomware threat jumps from Windows to Linux: What you need to know. *Forbes* (November 8), https://www.forbes.com/sites/daveywinder/2020/11/08/new-ransomware-threat-jumps-from-windows-to-linux-what-you-need-to-know/?sh=39d9d4893265.

Witten B, Landwehr C, Caloyannides M (2001) Does open source improve system security? *IEEE Software* 18(1):57–61.

Xu Z, Zhuang J (2019) A study on a sequential one-defender-n-attacker game. *Risk Anal.* 39(6):1414–1432.

Yin T, Sarabi A, Liu M (2023) Deterrence, backup, or insurance: Game-theoretic modeling of ransomware. *Games* 14(2):20.

Yue Y, Li X, Zhang D, Wang S (2021) How cryptocurrency affects economy? A network analysis using bibliometric methods. *Internat. Rev. Financial Anal. (Oxford)* 77:101819.

Zahravi A (2021) Bash ransomware DarkRadiation targets Red Hat- and Debian-based Linux distributions. *Trend Micro* (June 17), https://www.trendmicro.com/en_us/research/21/f/bash-ransomware-darkradiation-targets-red-hat-and-debian-based-linux-distributions.html.

Zhao Y, Ge Y, Zhu Q (2021) Combating ransomware in internet of things: A games-in-games approach for cross-layer cyber defense and security investment. *Proc. 12th Internat. Conf. Decision Game Theory Security* (Springer, New York), 208–228.

Zhao X, Xue L, Whinston AB (2013) Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *J. Management Inform. Systems* 30(1):123–152.