9-6-2023

How Crime Shapes Insurance and Insurance Shapes Crime

Tom Baker
University of Pennsylvania Carey Law School, tombaker@law.upenn.edu

Anja Shortland
King's College, London

OXFORD

Journal of Legal Analysis, 2023, **15**, 183–200

https://doi.org/10.1093/jla/laad002
Advance access publication 6 September 2023
Article

How Crime Shapes Insurance and Insurance Shapes Crime

Tom Baker[*] and Anja Shortland[†]

[*]University of Pennsylvania Carey Law School, Philadelphia, PA 19104, USA
[†]Department of Political Economy, Kings College, London, UK

E-mail: tombaker@law.upenn.edu, Anja.Shortland@kcl.ac.uk

Abstract

Crime creates demand for insurance but supplying insurance may promote crime. We examine five case studies of insured crimes (auto theft, art theft, kidnap and hijack for ransom, ransomware, and payment card fraud) and find a co-evolutionary process through which insurers engage with insureds, governments, and legal and extralegal third parties to mitigate losses, particularly when criminal innovations destabilize the insurance market. "Insurance as crime governance" stimulates demand for security, shapes criminal incentives, engages with the state to combat crime, and tolerates some crime in the interest of profitability.

1. INTRODUCTION

For the casual observer, crime appears to come in waves. Suddenly, the media are full of reports of rampant kidnapping activity with multi-million-dollar ransoms such as in South America in the 1970s or Somali Piracy from 2008 to 2012. Similarly, there was a spate of art thefts from British country houses in the 1980s, including the infamous IRA heist of paintings valued at $45 million from Alfred Beit at Russborough House in 1986 (New York Times 1986). In the early 1990s, no prestige car in continental Europe seemed safe from Central and Eastern European motor thieves. Credit card holders are alerted to one "scam" after another, while the early 2020s will likely be remembered for the "ransomware epidemic." But after a while, reports of the latest crime wave fade away. As potential victims, we may notice that new hardware or software comes with unfamiliar security features (like snazzy electronic keys, microchips and PINs, and constant requests for identification and verification). Maybe there is a new regulation or additional law enforcement to keep criminals in check. And when we renew our insurance we may find a whole host of new restrictions, exclusions, and an eyewatering price hike. In this article, we study successive crime waves in five insured criminal markets to examine the role of insurance in fostering the onset of crime waves and expediting their decline.

The Becker model of crime posits that criminals are sensitive to the net payoffs to crime (income minus the cost of carrying out the crime), the probability of being caught and punished, and the severity of punishment (Becker 1968). We, therefore, examine whether and how insurers shape risk and returns to certain crimes, to make or keep them insurable. Insurers can influence the cost of carrying out certain crimes, the payoffs to criminals, and the probability of being punished by interacting with insureds, governments, or third parties. Criminals can respond to these measures by reducing their activity, moderating the harm they inflict on insureds, or by innovating in turn to improve their expected

For helpful comments and suggestions, the authors would like to thank Kenneth Abraham, Sandra Mason, Daniel Schwarcz, Oren Bar Gil, our anonymous reviewers and interviewees, and participants at workshops at Temple University, Penn Carey Law School, Notre Dame Law School, and UConn Law School.

utility. Criminal advances may trigger further innovations by insurers and vice versa: insurance and crime co-evolve.

It has long been established that having assumed the risk of loss, insurers have the incentive to shape the threats their customers face and their efforts to self-protect (Heimer 1985). In this article, we extend and deepen the analysis of reactive risk and insurance to insurance against crime. Examining five case studies of insured crimes—auto theft, art theft, kidnap and hijack for ransom, ransomware, and payment card fraud—we identify three interlinked dimensions in which insurers respond to the loss mitigation incentive. First, insurers incentivize or require their insureds to invest in self-protection, through partial insurance to make the insured more careful and imposing security-related conditions in insurance contracts or underwriting. Second, insurers work with third parties to shape criminal opportunities. They fund research into technical barriers to crime and methods to detect and trace stolen goods. They create or employ service providers that harden targets, increase the potential for recovery or salvage, or limit criminal profits. They also engage with extralegal third parties to obtain protection, facilitate recovery and reduce total resolution costs. Finally, insurers engage with the state to combat crime: by providing technical assistance to lawmakers and law enforcement, co-funding enforcement activities, and lobbying lawmakers to increase enforcement and mandate measures that harden targets or otherwise reduce the return to crime.

The article is structured as follows. In Section 2, we discuss the aims of insurers in the insurance/crime nexus and the institutions insurers have created to obtain leverage over criminals. In Section 3, we present the case studies, tracing the co-evolution of insurance and crime over time, with periods of balance and episodes of innovation and conflict. Insurers address different crimes using different methods, with a view to minimizing (transaction) costs. Section 4 identifies and discusses the key messages from the case studies. Section 5 concludes.

2. THE CRIME/INSURANCE NEXUS

Crime creates demand for insurance. Some media and academic commentators, therefore, surmise that insurance has an ambivalent relationship with crime—particularly profit-motivated crime. On the one hand, insurers have the incentive to reduce the frequency and severity of payouts. On the other hand, insurers understandably hesitate to impose conditions that make crimes extremely difficult to commit (such as armed guards), because they are expensive and unattractive for customers and undermine the demand for insurance. As the critics assert, insurance can even promote crime. Lax underwriting may reduce self-protection, and insurance can fund criminal profits beyond what individual victims would be able to raise or afford. Theft, ransomware, and abductions become less risky to commit if insurers create processes to keep the assets, data, or hostages—and hence the criminals—safe while facilitating ransom payments (Parris 2012; Dudley 2019; Avraham & Porat 2022).

We agree that the insurance industry does not have the incentive to suppress crime to the point where insurance becomes unnecessary. But neither do insurers have the resources, the political mandate, or the (police) powers to do so. Taking collective action is difficult in global insurance markets. Nevertheless, as we describe and analyze in this article, insurers in some property and financial crime domains manage to act collectively in ways that, consistent with their financial incentives, stabilize crime in the interest of insurability. They create institutions to decrease the volatility of crime, reduce the severity of extreme losses, and limit the potential for correlated losses. By encouraging their customers to protect themselves against crime and creating processes for detecting and prosecuting criminals, insurers reduce opportunistic crime. When committing a crime becomes an organizational challenge and a high-risk venture, losses become more predictable and selling insurance less risky.

If insurers successfully help to reduce opportunistic crime, they are left with sophisticated and organized criminal gangs as their main adversaries. This creates the potential for strategic interaction between crime and insurance. If criminals adjust their business model to tap into generous insurance-funded pay-outs, losses may become extreme. If other sophisticated criminal gangs copy the innovation, these increased losses may become correlated and, thus, catastrophic. Hence, insurers have the incentive to manage the maximum return criminals can get from each crime and to direct (or lobby for) resources to catch the most egregious offenders. Insurers can also encourage criminals to reduce the collateral damage of their crimes in the interest of insurability. Finally, insurers may reduce the supply of insurance, by reducing the maximum limits, increasing deductibles, or both. Partial insurance

increases customers' self-protection efforts. At the extreme, a credible threat of withdrawing all insurance from a particular area or activity may force criminals into a compromise.

When we look at insurance for profit-motivated crime, we observe that insurers have indeed created a raft of institutions to obtain leverage over criminals. There are both carrots and sticks. Some institutions exist primarily to prevent crime, improve prosecution, or limit criminal profits. But others offer a cooperative approach to resolving crime in return for criminals limiting harm. We observe multiple types of governance efforts along the three dimensions identified in the introduction: shaping the behavior of the insured, engaging with legal and extralegal third parties, and engaging with the state. In all these efforts, insurers employ a market logic in which the efficient level of crime is not zero, and criminals respond in ways that make any equilibrium at least potentially unstable.

3. CASE STUDIES

In this section, we use case studies to examine insurers' efforts to keep various crimes insurable. We are particularly interested in tracing processes of co-evolution/strategic interaction. In most of our cases, each side innovates in response to the other's initiatives. In some cases, there are (long) episodes of equilibrium where criminals come to understand what the limits of "bad behavior" are. They self-censor their actions to optimize the risk/return characteristics of their activity and crime can be profitably insured. Exogenous shocks or innovations on either side can upset the equilibrium at any time. The table at the end of each case study identifies specific measures we observed in each of the three dimensions and highlights how insurers' efforts have changed over time in response to innovations on the criminal side of the insurance/crime nexus.

3.1 Auto Theft

The history of auto theft cannot adequately be told without considering the role of the insurance industry in paying for and attempting to contain that theft. The industry's collective response to auto theft dates at least as far back as the formation of the first Automobile Theft Bureau in Southern California in 1913 "under the auspices of the Insurance Department of the Automobile Club of Southern California and the Pacific Coast Automobile Underwriters' Association" (Insurance and Investment News 1913). By 1919 the insurance industry had funded auto theft bureaus in Atlanta, Chicago, Dallas, New York City, and San Francisco (Insurance Press 1919), and in 1928 the US insurance theft bureaus consolidated under the umbrella of the National Automobile Insurance Theft Bureau (NATB) (The Standard 1928). The NATB operated under that name until it combined with the Insurance Crime Prevention Institute to form the National Insurance Crime Bureau (NICB) in 1992.

The Bureaus began by maintaining lists of stolen vehicles and assisting police in recovering the vehicles—activities that the NICB continues today (e.g., NICB 2020). The Bureaus maintained private registries of vehicles, identified by serial number, and advocated for the creation of a uniform system of vehicle identification numbers—the VINs that appear on cars today. Created to facilitate the recovery of stolen vehicles, the Bureaus' registries also inhibited professional theft by making it more difficult to dispose of stolen vehicles. Organized crime adapted in response, studying where each auto manufacturer located the serial numbers (later VINs) in the cars and developing procedures to erase or alter the numbers. The NATB adapted as well, for example, by developing cameras that revealed the erasure or alteration of the numbers, and by working with law enforcement to encourage manufacturers to stamp or etch the numbers on the most valuable parts making it more likely that law enforcement could identify a suspicious vehicle as stolen (U.S. Senate 1979 at 62, 66).

By at least the 1930s, the NATB was working closely with law enforcement to combat organized theft rings, serving as an early example of the "police-insurance connection" that Richard Ericson and his collaborators later identified (Ericson & Haggarty 1997, 2004). A 1936 study of "Police in Modern Society" described how the NATB worked with police to address organized auto theft rings:

> Auto-theft investigators of the insurance companies, because of their highly specialized training and wide experience, as well as the fact that they cover much territory, possess information which is extremely valuable to the police, and they have *greatly assisted the law-enforcement officials*. The National

> Automobile Theft Bureau, with its headquarters in New York, maintains five divisions which cover the entire United States. As a rule, this bureau selects capable investigators from police departments, and gives them sufficient financial support to trace large gangs. *The union in this manner of the private organizations and the public officials contrives* to make an effective organization for the reduction of auto theft.

(Vollmer 1936 emphasis added). These activities continue today, with the NICB describing their investigative activities as follows (NICB 2020):

> NICB's investigative efforts focus on multi-claim, multi-carrier investigations of major criminal activity in concert with our members and law enforcement agencies nationwide. We are the country's only private organization that takes a multi-carrier approach to fraud and theft investigations.

The NATB/NICB has prepared training materials and conducted training sessions for police departments for many years (e.g., Gourley 1953). Although there has yet to be a definitive history, the Bureau appears to have been a constant presence in state and federal efforts to address automobile theft through activities such as training, providing financial support, lobbying in favor of laws requiring the adoption of anti-theft measures by automobile manufacturers, and developing investigative tools and techniques (e.g., Motor Vehicle Titling 1994; NICB 2020). These efforts have borne fruit in the dramatic reduction in automobile theft since 1992.

The key explanation for this reduction is the widespread adoption of immobilizer technology, which requires an encrypted electronic signal from a transponder on the key for a car to be started (Barro 2014). Interestingly, the first patent for a car immobilizer stems from 1919, but neither car owners nor manufacturers had the incentive to invest in this relatively expensive security feature (Field 1993; van Ours and Vollaard 2016). Insurers' focus on institutions to aid salvage and recovery kept the insurance market in balance even at relatively high theft levels until car crime exploded in the early 1990s in Europe. The fall of the iron curtain unleashed an immense demand for Western cars in the former Socialist countries and once stolen cars had passed into Eastern Germany and beyond, insurers could no longer recover them. Insurers, therefore, engaged intensively with security engineering firms to bring immobilizer technology up to date. Auto insurers utilized their in-house facility Thatcham Research in the UK to test and create new industry standards for car keys.[1] Struggling to provide appropriate incentives for insureds and unable to collude to make immobilizers a condition for obtaining insurance, car insurers lobbied for government regulation in Europe to mandate that the technology should be built into all new cars. This was marketed to politicians as a social welfare-enhancing policy (van Ours & Vollaard 2016) and approved by the EU in 1995, with manufacturers given just three years to implement it (Rosalski 2022).

The hasty development of immobilizers led to security gaps that were soon exploited by hackers—creating an ongoing arms race between security engineers and sophisticated organized crime (Ferapontov 2020). However, amateur (teenage) opportunists cannot hotwire cars with immobilizers and as a result, the insured value of car theft has dropped steadily. Additionally, insurers benefit from data collection in electronic keys that make it easier to spot attempted insurance fraud (Weber 2015). Insurer-supplied "bait cars" and surveillance (a form of co-funding of law enforcement) put further pressure on organized crime and produce significant returns for insurers. Auto insurers' focus on organized crime makes good financial sense. Autos stolen in opportunity crimes typically are recovered, resulting in smaller, more sustainable losses for insurers, while organized crime breaks down cars for parts or ships them abroad, resulting in a complete loss of the insured value of each car (Longman 2006; Smylie 2006).

Although auto insurers work to contain and reduce theft, they resist anti-crime initiatives that work against their financial interests, as illustrated by the history of "VIN switching," or, as sometimes called, the "salvage switch." Before states enacted automobile titling laws that required insurers to label the title of a car that had been declared a total loss as a "salvage" vehicle, crime rings would buy cars at salvage auctions and then steal cars of the same make, model, and year. They would then put the VIN plates, VIN stickers, and any still operable VIN-labeled parts from the salvaged cars into the stolen cars, repaint the stolen cars as necessary to match the title of the salvaged cars, and sell the stolen cars with

[1] Thatcham Research has been deployed across a range of loss mitigation initiatives since its foundation as the Motor Insurance Repair Research Centre in 1969, such as the cost of repairs, whiplash, and driverless cars https://www.thatcham.org/about/.

a clean title as if it were the salvaged cars (National Association of Attorneys General 1979; U.S. Senate 1979 at 64; California Bill Analysis 1994).

As word of the salvage switch got out, consumer advocates called for insurers to destroy cars rather than sell them for salvage (Tamaki 1993). Insurers resisted, arguing that (i) there were legitimate uses for salvaged cars (e.g., for parts) and (ii) the money earned from selling cars at auctions helped to offset insured losses and thereby reduce auto insurance premiums, and (iii) there were more efficient ways to combat organized crime. Those arguments were persuasive when the only way to prevent the salvage switch was by destroying the cars. But those arguments were less persuasive once the idea of a special "salvage" title emerged. Nevertheless, some insurers resisted efforts to change state auto titling laws, ostensibly on the grounds of administrative complexity, but more likely because cars with a salvage title would be less valuable at auction (U.S. House of Representatives 1994). This situation presented a collective action problem: maintaining higher prices for salvaged cars was in the interest of individual insurers even if it was in the interest of the auto insurance industry to deter the salvage switch. Consistent with that framing, the trade association of the smaller insurers opposed collective action, while the large insurers—led by State Farm, which had the largest market share—promoted it (U.S. House of Representatives 1994, 1996; U.S. Senate 1997). Eventually, the NICB (the successor to the NATB) and most of the insurance industry came down on the side of changing auto titling laws (California Bill Analysis 1994; U.S. House of Representatives 1996; U.S. Senate 1997).

Table 1 summarizes the developments discussed above in the three dimensions. We see an arms race on technical solutions and considerable efforts to provide services and build institutions to improve salvage and recovery. There is also a significant effort to support law enforcement, including discretionary direct funding to combat organized crime. We note that conditionality has not been widely used in this highly competitive insurance market. Instead, higher security standards have been driven to implementation via government lobbying.

3.2 Art Theft

The massive increase in art prices since the 1950s has challenged insurance against art theft. Insurers had been prime supporters of the security industry since the early 1900s, by creating demand for early (but relatively simple) burglar alarms. In 1953, UK insurers formed the Association of Burglary Insurance Surveyors to promote research into security systems, create technical standards and train and license installation experts (Calahane 2015). In a highly concentrated market for fine art insurance, installing a security system became a condition for obtaining insurance, but alarms are ineffective unless responded to. Insurers thus lobbied for police resources to respond to an ever-increasing number of call-outs. Over the following decades, product development occurred on two levels: an arms race with sophisticated burglars to make security systems more sensitive while containing the rate of false alarms (Calahane 2015).

Alarm systems do not protect art against insider crime (Rahm 2014) and not everybody correctly operates their state-of-the-art security systems (Barelli 2019). Insurers therefore also created channels for salvaging stolen art. They found that stolen artworks could often be retrieved from the criminal underworld by offering substantial "rewards for information" to whoever could disclose their location. However, this resulted in an attractive criminal business model—or "tickle." Soon after a theft, someone

Table 1 Auto.

	Insureds	Third parties—legal and extra-legal			The state		
	Incentives	**Technical**	**Services**	**Organized crime**	**Assist police**	**Co-fund**	**Lobby**
Early		Car keys, serial numbers	Stolen car register		Inform, Train		
Mid-century	Pricing	+ VINs, Improved keys	Stolen car register with VIN		Inform, Train	Support vs organized crime	VIN
From 1990s	Pricing	+ Immobilizers	Stolen car register with VIN		Inform, Train	Support vs organized crime	Immobilizer, Titling

would report having "overheard" a conversation among complete strangers in an ill-lit bar revealing the location of the stolen paintings in—say—a station locker, dusty attic, or abandoned car and collect the reward. This minimal-risk route to divesting loot served both thieves and insurers, who much preferred paying rewards to reimbursing the full value (McLeave 2003). By setting the rewards (and making clear that only objects in good condition were eligible), insurers stayed in control of losses. If loss adjusters were (somehow) satisfied that the informant was not a criminal, no law was broken in the transaction. Yet, there was public and political disquiet about this cozy coexistence of insurance and crime. In 1968, the UK government amended the Theft Act to insert a new Section 23 that outlawed rewards for information that implied that "no questions will be asked" and threatened those that advertised such rewards with punitive fines.[2] In return, the government founded a dedicated art and antique crime unit within the London Metropolitan Police, promising improved resources for law enforcement (Reyburn 2017).

In the 1970s, insurers focused mainly on making expensive artworks "too hot to handle" (Hayworth 1993). The International Foundation for Art Research (IFAR) was founded in 1969 and became a key resource for fighting high-end art theft from 1970. Reminiscent of the Auto Theft Bureaus, IFAR collected and disseminated information about stolen and looted objects to the art trade, reducing opportunities for thieves, fences, and grey market buyers to monetize their loot. Rewards were made available to *bona fide* traders spotting stolen art—not thieves' accomplices and frequenters of underworld taverns. However, sophisticated thieves could circumvent these efforts: not every trader chose to obtain or act on the information provided by IFAR, and some buyers failed to exercise appropriate due diligence when being offered attractive artworks of suspicious origin—an attitude famously examined in cases such as Autocephalous Greek-Orthodox Church vs Goldberg.[3] While high-end art theft was reduced, theft remained an ever-present—albeit insurable—danger.

The art price boom of the 1980s disrupted this equilibrium. With art prices rocketing, insurance became ever more expensive. Some customers could still afford partial insurance, so insurers were only on the hook for the specified losses rather than ever more extreme market valuations. Others were priced out: institutions like the Isabella Stuart-Gardner Museum could simply not afford insurance (Butterfield 1990). The un- and underinsured offered tiny rewards for information relative to the values at stake, undermining art recoveries. Crooks who found themselves unable to ransom stolen art, either sold it cheaply to plausibly innocent buyers in civil law jurisdictions who could then obtain title through adverse possession (Hayworth 1993; Klerman & Shortland 2022), broke it up for resale or destroyed it. The 1990s thus saw a two-pronged approach to art crime: even greater efforts to trace art losses and close markets to loot, coupled with an improved recovery process.

In 1991, art insurers at Lloyd's of London funded the creation of a database of stolen art—the Art Loss Register (ALR). The ALR created a comprehensive proprietary record of stolen art: amalgamating the information collected by IFAR, art insurers' losses from previous years, and private registrations (Shortland 2021; Klerman & Shortland 2022). Database searches were pushed aggressively into the market as a due diligence product—amongst others by the Council for the Prevention of Art Theft (Flynn 1998). Dealers, auction houses, and fair organizers that facilitated the trade in stolen art were named and shamed and—if necessary—taken to court. At the same time, the ALR facilitated recoveries: developing a reputation for asking searching questions and closely coordinating any compensation or reward with law enforcement (Shortland 2021). As "condition" was a major determinant of any finder's reward (usually a small percentage of the value), careful theft, handling, and storage were strongly incentivized.

Insurers thus succeeded in progressively tightening the market for stolen art. In 1994, the British Insurance Association and Lloyd's supported an amendment to the British Sale of Goods Bill to abolish the medieval common law privilege of so-called "markets overt," where buyers could acquire good title on stolen goods.[4] As illicit art prices collapsed, private art recovery businesses began to thrive. When police forces were reorientated from the property toward violent and drug crime, former officers turned private detectives, assisting loss adjusters with recoveries (Flynn 1998). Their successes facilitated a new line of insurance: "art recovery insurance"—a much cheaper option than insuring the full value of artworks (Kinsella 2004). The market for insurance and art theft can, therefore, be considered in an unstable equilibrium. Iconic masterpieces are not attractive to steal as they are effectively unsaleable. For

[2] United Kingdom Theft Act of 1968 Section 23 https://www.legislation.gov.uk/ukpga/1968/60/section/23.
[3] *Autocephalous Greek-Orthodox Church v. Goldberg*, 717 F. Supp. 1374 (S.D. Ind. 1989).
[4] Sale of Goods (Amendment) Act 1994. Repeal of s. 22(1) of the Sale of Goods Act 1979. See Hansard 1994 Vol 551 col 214.

other high-end art, partial insurance limits losses, and some of the pay-outs are later salvaged through successful recoveries. The mid-market is either directly insurable or insurable for recovery. But high insurance premia and a slow recovery process mean that investment art is best kept in high-security storage areas—often in freeports—rather than displayed and enjoyed.

This observation raises a further interesting observation regarding art theft: why didn't the market develop better technical solutions to art theft? Why can thieves swipe paintings in their frames? Speculations abound (e.g., Rahm 2014)—but damaged art is effectively worthless, and insurers like to avoid total constructive losses. The obvious place for embedding microchips or tracking devices into fine art is the frame. Frames can also be firmly secured to walls. However, this provides a clear incentive to cut pictures from their frames in situ—and older canvases do not bend, they rip and break. So, while a vibration sensor alerting security to an attempted theft makes sense, any innovation that discourages thieves from rushing out with the frame would be against the interest of both art lovers and insurers. This "path not taken" on security is likely an integral part of the interrelationship between art theft and insurance.

Table 2 shows the growing and ever more sophisticated insurance ecosystem around art theft. In the small art insurance market, imposing conditionality is not a problem for high-value art, but in the mid-market insurers operate through positive incentives and limits. There is an ongoing technological arms race with burglars and art thieves, but insurers stay clear of technologies that could produce total constructive losses. Instead, insurers negotiate with criminals for the return of stolen art. Over time, art recovery services become more aligned with the goals of law enforcement, yet in turn insurers have lobbied for more resources from law enforcement. We do not see explicit co-funding of law enforcement, but the information provided by insurer-funded private art detectives and registers on the location of stolen art and their court evidence significantly boosts the effectiveness of policing in this area.

3.3 Kidnap and Hijack for Ransom

To be insurable, kidnapping and piracy must be predictable but rare, affordable to resolve, and essentially non-violent. This is far from the popular image of kidnapping, and indeed insurability is only achieved with significant (public and private) governance efforts. Kidnap- and hijack-for-ransom (K&R) insurance strikes a delicate balance between discouraging hostage-taking and facilitating the safe release of hostages (Shortland 2019). On the one hand, significant value must be attached to living hostages, so that criminals aim not to injure or kill their victims during the abduction and keep them safe thereafter. Negotiations, payments, and releases must be managed as calmly and efficiently as possible to minimize the risk to life. On the other hand, offering ransoms, normalizing extortion, and facilitating payments encourage kidnapping. Rising ransoms can create unstable dynamics: attracting (inexperienced) criminals into abductions and leading to (violent) kidnap hotspots.

Kidnap for ransom insurers have learned how to square this circle through a process of trial and error since they first offered K&R policies in the 1930s (Shortland 2019). Insurers have created complex norms and processes to simultaneously obstruct and selectively reward kidnappers that stick to the rules of the game. In each locality, insurers, the insured, local elites, and organized crime must find an

Table 2 Art.

	Insureds	Third parties—legal and extra-legal			The state		
	Incentives, conditions	**Technical**	**Services**	**Organized crime**	**Assist police**	**Co-fund**	**Lobby**
1950s–1960s	Alarms	Burglar alarms		"Reward for information"			Police resources for burglary
Late 1970s–1980s	Alarms, under-insurance	Improved security systems	Art detective, IFAR	"Finder's fee"	IFAR register		"Art Squad"
1990s–present	Security systems, Trackers, under-insurance	Smart security systems, trackers	Stolen Art Registers	Salvage negotiations	Art Loss register		"Art Squad"

equilibrium where kidnap satisfies the above conditions for insurability. Disequilibrium in one part of the system can easily spread to others.

Kidnap for ransom insurance creates a first-party moral hazard. While few individuals deliberately put themselves or their families at risk of abduction, firms buying insurance on behalf of employees may be less cautious if they know that security lapses have limited financial or reputational consequences. Moreover, once an insured is abducted, the family or firm lead the ransom negotiations. Hostage stakeholders often hope that they can resolve a hostage crisis faster by throwing money at it—and this is especially tempting if the ransom is ultimately reimbursed by an insurer. If these first-party moral hazards are not checked, insurance creates third-party moral hazard: the insured become particularly attractive targets.

K&R insurance thus requires the insured to take adequate security provisions. Generally, this does not mean heavy-handed safety measures to defend all staff against every possible attack. In "complex and hostile" territories for which K&R insurance is sought, this would be socially and economically crippling. Instead, prospective insureds are directed toward security consultants (retained by the insurers) who help them to achieve two objectives. First, to ensure that opportunistic criminals are not presented with easy targets. Second, to reduce kidnap threats by gaining the support of (local) elites that can control the kidnapping activities of organized crime, militias, and rebel groups. This requires channeling a constant stream of revenues to local powerbrokers: e.g., paying taxes, entering joint venture agreements, hiring local staff, supply and maintenance contracts with specific companies, or a well-crafted corporate social responsibility program (Shortland 2019). The security advice is framed in terms of firms' "duty of care"—not of conditionality for obtaining insurance. As firms fear lawsuits by abducted staff or their families, compliance is generally good.

The objective is not to eliminate kidnapping, but to make it infrequent. Occasionally, an opportunist may strike lucky and sometimes there may be frictions in the (implicit) protection contracts. These incidents are handled by professional crisis responders, who are retained by insurers. Crisis response was created when K&R insurance was destabilized by massive ransom inflation in Latin America in the 1970s. Insurers realized that they needed to take control of ransom negotiations—or rather give advice to the insured on how to bargain with criminals to keep hostages safe. Once again, the issue is framed in terms of "duty of care" toward employees.

The negotiation protocol has the apt name "disruptive bargaining" and is designed to frustrate the ambitions of small-time criminals. By drawing out negotiations, risks are raised for opportunists who don't have the infrastructure for holding hostages over long periods. "Express kidnaps" that end at the next cashpoint for a quick pay-out are a common, rational response. This minimizes the harm and cost of opportunistic abductions. Sophisticated criminals and rebel groups can make serious money from kidnapping, but they must be able to wait and expend resources to do so. Ransom offers start low and are raised slowly and in decreasing increments. Eventually, it makes economic sense to release hostages: the next expected increment will not cover the cost of holding the hostages for the required time. The "low and slow" approach makes it very difficult to obtain supernormal profits from kidnapping.

The resolution protocol is also designed to punish (threats of) violence. Responders only start negotiations after proof of life has been received and advise stakeholders to hold firm in response to threats: rewarding "bad" behavior with higher ransom offers encourages further escalation. Threats of violence are countered with slower offers and lower increments. Kidnappers are constantly reminded that ransoming only works if they can give up healthy hostages. Responders collect, pool, and share information to ensure that violent kidnappers are identified, distrusted, closely monitored in subsequent transactions, and come under pressure from law enforcement or extra-legal protectors. Thus, criminals learn that violence is against their own interests.

K&R insurance, therefore, turns kidnapping into a repeated game between firms, crisis responders, and sophisticated kidnapping gangs, where long-time horizons facilitate reputational solutions. In many kidnap-prone areas of the world, equilibria develop where the number of transnational kidnaps, length of detention, and final ransoms become predictable and manageable (Shortland 2019). Bargaining can become so ritualized that negotiators on both sides can foresee each other's next move and victims come to perceive the negotiation as "mere theatre." Once a ransom has been agreed, crisis responders focus on making the payment and release process as smooth as possible, to avoid hostages being hurt or lost at the last minute.

However, these equilibria are inherently unstable. Not every CEO listens to advice that seems blasé about keeping hostages in extended captivity. It can be tempting to try and jump the gun. Fast and generous ransoms inspire copycat crime. This famously happened when ship-owners departed from the established protocol in their bargaining with Somali pirates, setting off a spiral of escalating ransoms and hijackings. Territory, where local elites benefit from the presence of foreign firms, can also be contested by rival groups that destabilize established relations. If ransoms, kidnaps, and violence get out of hand and insurance becomes unprofitable, K&R insurers have two options to collectively change the incentives of kidnappers, as this type of insurance is almost exclusively provided by a cohesive club of insurers at Lloyd's of London (Shortland 2019).

First, Lloyd's insurers can significantly raise insurance premiums across the board by declaring an area a "war risk." This creates strong financial incentives for companies seeking insurance to lobby governments to enhance law enforcement and reduce risks to a level acceptable to insurers. Good examples are the naval task forces deployed against pirates in the Gulf of Aden and the Somali Basin as well as international naval coordination in the Singapore and Malacca Straits and the Gulf of Guinea. Oil and mining companies are also in a good position to lobby host governments to restore control in contested areas. This is aided by a second superpower of K&R insurers: they can coordinate security advice to evacuate expatriate staff (Shortland 2019). The insured must do this to fulfill their duty of care. Lloyd's insurers can thus credibly threaten to withdraw all the revenues foreign companies bring into the host economies until local or national elites have restored the conditions conducive to insurability.

Table 3 shows how K&R insurers moved from incentivizing their customers to self-protect to relying on the duty of care and best management practice to ensure compliance with risk-mitigating measures. K&R insurers created security consulting and crisis response services to shape the insureds' interactions with criminals and engender ransom discipline. Where necessary, insureds buy the services of private security companies, who are engaged in their own technical arms race with kidnappers. K&R insurers do little to engage the state directly for protection but rely on their power to shift prices or withdraw insurance to encourage insureds to demand additional law enforcement from host governments when necessary.

3.4 Ransomware

Ransomware is malware that locks up a computer system until a ransom is paid in return for the decryption "services" provided by the criminal gang that launched the cyber-attack or their associates. Cyber-insurance was first developed in the mid to late 1990s and was initially designed to offer cover against business interruption and third-party liabilities arising from negligence and a broad variety of common computer crimes such as theft of credit cards, malware, and denial of service attacks. Early on, some insurers insisted on security audits, but those were soon dropped as not cost-effective (Baker & Shortland 2022). Only a small minority of special risk insurers at Lloyd's of London specializing in kidnap for ransom insurance explicitly focused on cyber extortion (Baker & Shortland 2022). Although the

Table 3 K&R.

	Insureds	Third parties—legal and extra-legal			The state		
	Incentives, conditions	**Technical**	**Services**	**Organized crime**	**Assist police**	**Co-fund**	**Lobby**
Early	Security advice	Alarms, perimeter security	Private security				
Late 1970s	Professional crisis response, private security	+ Armored cars	+ Security consulting/ ransom negotiation	Protection/ ransom bargaining	Inform		"War risk" causes broad lobbying for state protection
Current	Duty of care/ best management practice	+ Security information	+ Ransom payment, hostage extraction	+ "War risk" and evacuations	Inform	Public/ private security	+ Evacuation advice disrupts business

first known incident of what we would now call ransomware occurred in 1989 (Wilding 1990), and computer scientists predicted highly damaging "cryptoviral extortion" as early as 1996 (Young & Yung 1996, 2017), ransomware took more than two decades to develop into a significant threat for cyber-insurance.

Attackers initially struggled to develop strong encryption that was specific to each victim. Breached enterprises only pay ransoms if they expect this to be by far the cheapest and safest way of restoring their computer systems. Early attacks were often resolved by security engineers. If decryption tools were purchased from hackers, they could be shared between victims, cutting off the attackers' profits. Criminals also needed a payment mechanism that was simple and secure for the victims while protecting the anonymity of the extortionist. Ransoms in early cyber extortion attacks were low: to encourage the victims to pay the attacker rather than a cybersecurity firm and to reduce the probability of detection when receiving payment in gift vouchers, premium telephone calls, or postal and money orders. With negligible ransoms, insurers did not develop institutions to manage criminal profits. Instead, insurers' efforts were focused on mitigating the cost of third-party liabilities from privacy breaches (Woods & Böhme 2021; Baker & Shortland 2022; Schwarcz et al 2023).

The big breakthrough for ransomware came when cryptocurrencies such as Bitcoin emerged from 2008 onward, massively simplifying transactions between legal entities and criminal enterprises (Kharraz et al 2015; Popper 2015). In 2010, the price of stolen credit card details collapsed because of oversupply due to the highly successful ZeuS Trojan (Krebs 2010). Criminal coders were therefore on the lookout for new profit opportunities. The infamous CryptoLocker ransomware attack in 2013 combined several criminal innovations: the powerful ZeuS Trojan, private-key cryptography—so victims could be made to pay individually—and ransom settlement in Bitcoin. The large-scale attack—infecting hundreds of thousands of computers—brought ransomware to widespread attention and led to an arms race between security engineers, crisis responders, and cyber-criminals.

Companies fortified their defenses and security engineers resolved simple attacks without ransom payments. As a result, most hackers failed to make a profit from ransomware. But sophisticated coders still succeeded—often beyond their own ability to handle the business. Ransomware-as-a-Service (RaaS) was born around 2016 when coders started to outsource the time-consuming "breaking and entering" part of the business to affiliates for a share of the profits (Coveware 2022). Once the affiliates had successfully breached a company's defenses, the encryption tool was automatically deployed and the victims were faced with a standardized (but still low) ransom demand, a link to a portal on TOR where software engineers could test the decryption tool and a button to make a payment in cryptocurrency.

The problem from an insurance point of view was two-fold: ransomware attacks became more frequent, but even more concerning was that the criminal coding masterminds had lost control of the resolution process. The affiliates had neither the skills nor the incentive to help the victims through the decryption process—so even if ransoms were paid, many companies still lost their data (Coveware 2022). The total cost of business interruption and recovery escalated. Insurers responded by helping their customers to streamline the resolution and recovery process by putting them directly in touch with professional breach responders. By pooling information, responders created incentives for hackers to provide aftercare in the resolution process. Customers were advised not to pay ransoms to ransomware groups with a track record of poor decryption success.[5] Responders also collected and shared the decryption keys purchased by their customers to help other victims recover for free, thereby further raising the bar for criminals.[6] Criminals thus had to work ever harder to create "brands" of ransomware that were irreversible without a ransom, but reliably resolved once the payment was made (Coveware 2019).

The second generation of RaaS (from 2018 onward) responded to rising costs and lower success rates by escalating ransom demands (Coveware 2022). Instead of posting a standardized ransom likely affordable for all victims, hackers spent time researching the organizations they had breached. They then demanded what they considered the victim (or their insurer) could pay (Haymore 2121). To contain costs and prevent failure, cyber-insurers decided to provide additional help for their customers: few victims were comfortable bartering with criminals or familiar with obtaining and paying large ransoms in cryptocurrencies. Ransomware-Settlement-as-a-Service was born. To drive down ransom demands, breach responders needed a credible threat that the victim could restore their systems from backups without the need for the criminal's decryption tool. Companies started to invest in better

[5] See, for example, the Coveware blog informing the interested public about decryption problems https://www.coveware.com/ransomware-blog

[6] See, for example, the Coveware blog and the *No More Ransom* initiative https://www.nomoreransom.org.

back-ups—and as insurers began to contractually limit their financial exposure to the new generation of ransomware, firms also upgraded their pre-breach security. Once again, criminals had to innovate to save the ransomware business model.

Third-generation RaaS started in 2019 and weaponizes privacy legislation (Coveware 2022). Before encrypting the victim's data, the attackers spend even more time in the system to locate the files that the organization would least like to become public and exfiltrate them. The ransom demand can then be escalated by factoring in the financial and reputational consequences of the exfiltrated data being made public (Fuentes et al 2021). With strict data privacy legislation and punitive fines, the companies' investment in backups becomes irrelevant. Even though companies have no guarantee that the criminals will not copy or sell the stolen data, the so-called "double extortion" strategy makes it extremely painful for companies not to engage in a negotiation and concede to attackers' demands. Third-generation RaaS has thus resulted in a further escalation of ransoms.

Over the same period, insurers have become increasingly concerned about state-sponsored ransomware, whether intended to raise hard currency (as allegedly is the case for North Korea) or to disguise the destructive intent of the state (as allegedly was the intent of the NotPetya malware released in Ukraine). As a result, insurers are stepping back from providing insurance against state-sponsored cyber events, in some cases by taking the controversial step of denying coverage under policies that explicitly provided cyber protection (as in the Merck and Mondelez litigation arising out of NotPetya) and in other cases by adopting new exclusions against state-sponsored cyber actions (Voreacos et al 2019).

As in the other case studies, insurance has shaped crime by reducing opportunities for unsophisticated criminals and engaging with sophisticated criminals to reduce the total cost of criminal activities. However, no stable equilibrium has yet been found. At each stage, innovations by one side decisively tipped the scales in the innovator's favor, requiring a major adjustment by the other side. However, the know-how that makes ransomware attacks successful is highly scalable: RaaS means that less sophisticated criminals which might have been deselected from a "managed" criminal market can continue in the business as affiliates. Insurers and victims have therefore not reaped the full benefits of investments in security, insurance still struggles with a high volume of cases, and insurers have vowed to avoid insuring crimes committed by the most sophisticated and best-organized criminals: those backed by states.

The summary in Table 4 shows that cyber insurance is like car insurance in that insurers have concluded that self-protection is best achieved via government regulation in a highly competitive market. There is a massive ongoing arms race in the engineering and services dimension, but the insureds mostly take advantage of resolution rather than prevention services. In terms of engaging with criminals, efforts to manage criminal profits are still in their infancy, as is a collaboration with law enforcement. However, it is worth noting that ransomware insurance has only seen just over twenty years of product development, rather than the hundred years of the previous case studies.

Table 4 Cyber.

	Insureds	**Third parties—legal and extra-legal**			**The state**		
	Incentives, conditions	**Technical**	**Services**	**Organized crime**	**Assist police**	**Co-fund**	**Lobby**
Pre bitcoin	Security audits	Decryptors	Security audits	Pay minimal ransoms			
2010s	Free audits and advice	+ Back ups	Ex ante security advice and crisis response	Pay rising ransoms, monitor reliability of decryptors			
Current	+ Free advance warning systems, Basic cyber hygiene standards	+ Patches, firewalls, MFI	+ Vulnerability and breach monitoring, RAAS	Barter over ransoms, monitor trustworthiness	Share info		Regulation, Internat'l enforcement, insurance backstop

3.5 Credit Card Fraud

In this case study, the insurance is implicit rather than explicit. Banks and credit card companies effectively insure their customers by reimbursing them for fraudulent transactions. We chose credit card fraud as our final case study to observe whether the same co-evolutionary dynamic occurs in the case of implicit insurance and because most of our readers are likely to have personal experience with payment cards. We find that card providers have made it progressively more difficult for thieves and fraudsters to make transactions not authorized by the card owner. Criminals have reacted with improved counterfeiting technologies, by targeting less secure transactions, and tricking cardholders into divulging confidential information. Financial services institutions have, in turn, reduced the maximum benefit criminals can derive from stolen cards or card details and bolstered the capacity of public law enforcement to detect, apprehend, and successfully prosecute repeat and egregious offenders.

The earliest credit cards—made from cardboard or celluloid—were easy to counterfeit. To make forgeries more difficult, safety features were introduced in the 1970s in the form of tamper-resistant signature panels, embossed identifying information, and microprint security features. Yet, sophisticated fraudsters circumvented these safety features by re-embossing genuine cards or transferring stolen card details to blanks (Wilson 1999). Unable to prevent the manufacture of fake credit cards, the main security advancement of the 1980s was information pooling. From the mid-1980s, information stored in magnetic strips on the back of each card could be checked against a register of stolen, canceled, and expired cards. Later, fraudulent and declined applications were added to a central register of problem cards.

The 1990s saw several further refinements to security protocols. To plug the inevitable time lags between thefts and cards being registered as problematic, card providers started to risk-score transactions and block suspicious payment requests—a technique that was refined over the next decades to reduce the number of false positives which interfered with the smooth operation of commerce (NCR 2021). From the mid-1990s, customers were issued with personal identification numbers (PINs) to make payments at stores or withdraw cash—meaning that criminals required an additional piece of information to benefit from a stolen card. For online purchases, where customers could not use their PIN, card companies introduced the Card Verification Value (CVV) and address verification (VISA 2022). This makes it more difficult for fraudsters to abuse account information gleaned from, e.g., old receipts and letters.

As e-commerce took off in the 2000s, "card not present" fraud opportunities multiplied. Hackers obtained credit card details online, and scammers used social engineering to trick cardholders into revealing their account details. Every security protocol was tightened and improved in response: multi-factor authentication, risk scoring, tokenization (to reduce the number of times sensitive card details are transmitted), and the management of compromised account systems. Magnetic stripes were replaced by more secure microchips that are more difficult to read and duplicate and unlock payments with one-time codes. The latest round of innovation centers on biometric and geolocation verification. These manifold innovations and upgrades were introduced at different times by different card providers, depending on their perceived costs and benefits. Sometimes, paying for fraudulent transactions is cheaper than investing in a more secure technology—for example, chip and PIN technology was strongly resisted in the US until a regulatory change in 2015 (Wolff 2016).

But card providers also act collectively. In 2002, the UK financial sector joined with the City of London Police and the Metropolitan Police to establish a Dedicated Card and Payment Crime Unit (DCPCU).[7] This unit has only one brief: to investigate, target, and prosecute payment fraud, acting on the industry's current, pooled threat intelligence. Effectively the UK financial sector pays directly for the police powers it needs to deter and neutralize large-scale and sophisticated fraud threats. In 2017, the firms in the UK financial sector created their own lobbying body: UK Finance.[8] UK Finance collects and publishes information for anti-fraud campaigns, advocates for policy change with the government and regulatory bodies, and delivers national awareness campaigns to stop fraud and scams.

Therefore, despite the insurance relationship being implicit (i.e., banks acting as insurers) Table 5 shows the same pattern of discouraging opportunistic crime and changing the incentives of

[7] See UK Finance website at https://www.ukfinance.org.uk/dedicated-card-and-payment-crime-unit.
[8] See UK Finance website at https://www.ukfinance.org.uk/about-us.

sophisticated criminals to keep their activities below the radar of (suitably beefed up) law enforcement. We also see a very energetic interaction where technological and criminal innovations create ever more sophisticated remedies to keep crime insurable. However, Table 5 also shows that there is a key difference between insurers and financial service providers acting as insurers: card providers can directly enhance security through card renewals and improved protocols that are embedded in the cards and merchant-side devices. Rather than negotiating with the insured and manufacturers about the optimal security level, the main third party to get on board is the merchant, who must invest in the relevant hardware, software, or human capital for each security upgrade (Wolff 2016). So just as in the other case studies, not every possible security enhancement is adopted.

4. DISCUSSION

Our case studies identify several key themes. First, insurance applies a market logic to crime. The "economically efficient" level of crime is non-zero: insurers invest in crime control only until the marginal cost of crime reduction equals the marginal benefit to insurers (Coyne & Leeson 2009). Second, insurance and crime can find different equilibria in different times and contexts, ranging from low levels of insurable crime to partially insurable high crime levels. Third, such equilibria are unstable: cost and benefits of either side may shift through exogenous shocks or through endogenous innovations. Fourth, we observed a general pattern of insurers tackling crime at two levels: they help to create significant (and rising) barriers for opportunistic criminals while engaging in strategic interactions with sophisticated and organized crime.

Of necessity, insurers engage in their crime control initiatives largely through other actors. Across our five case studies, we observed three dimensions in which these governance efforts take place. Insurers work to maintain or stimulate their insureds' demand for security: through conditions and incentives in their contracts and underwriting and by promoting technical solutions that improve or lower the cost of security. Insurers work together or with third parties to shape the incentives of criminals: through protocols, technologies, and services that limit criminal profits, increase the probability of detection, reduce the likelihood of damage to the object of the crime, and increase the potential for recovery or salvage. Insurers engage with the state to combat crime: through providing technical assistance to lawmakers and law enforcement, co-funding enforcement activities, and lobbying lawmakers to mandate or encourage measures that harden criminal targets or otherwise reduce the return to crime. Finally, insurers tolerate crime in the interest of profitability. We briefly discuss each of these below.

Table 5 Cards.

	Insureds	**Third parties—legal and extra-legal**			**The state**		
	Built-in security	**Technical**	**Services**	**Organized crime**	**Assist police**	**Co-fund**	**Lobby**
1970s	Signature strip, microprint	Counterfeits and security features					
1980s	Magnetic strips	Magnetic strips	Central register of problem cards		Inform		
1990s	PINs, CVV and address verification	+ Identify and block suspicious transactions	Identify and block problem cards		Inform		More enforcement
2000–current	CHIP and PIN, MFI, tokenization, Biometric verification	+ MFI, Verification codes/ Biometric verification	Block problem cards		Inform	Payment fraud unit	Dedicated finance lobbying body

4.1 Stimulating Insureds' Demand for Security

Insurers incentivize the insured to increase self-protection with premium reductions, conditionality or by offering only partial insurance (excess payments/ (sub)limits/ exclusions) (for prior research see, e.g., Heimer 1985). Insurers are actively involved with third parties to create new technology for their insureds to adopt that makes it harder to successfully commit a crime, such as more sophisticated locks and keys, immobilizers, alarm systems, and security protocols/ systems (e.g., encryption, backups, credit card enhancements), illustrating that, although we discuss these dimensions separately, they are closely interlinked. Similarly, in some cases, insurers lobby the government to mandate target hardening, so that their insureds have no choice but to adopt the new technology.

4.2 Working Through Third Parties to Shape Criminal Opportunities

We observed several examples of insurers creating or funding the creation of technologies, protocols, and services to deter crime, discourage destructive behavior, and incentivize the preservation of value. Fraud detection algorithms discourage the egregious use of stolen cards or card details. Kidnappers, pirates, cyber criminals, and art thieves are rewarded with higher payoffs for returning assets intact. Police and special forces only try to liberate hostages held by particularly violent groups. Hackers that were unable to reverse encryption lost out on ransom payments as breach responders shared information on who could and could not be trusted to restore affected files.

We also observed several examples of insurers reducing the pay-off from crime and creating salvage mechanisms. Most thefts require a conversion for criminals to fully benefit from their crime. Insurers have therefore created institutions that make resale without detection more difficult and hence less profitable. Registries such as the Art Loss and Stolen Watch Register and the Auto Theft Bureaus not only impede the first resale but may be able to reclaim (or obtain compensation for) stolen assets from subsequent owners, undermining the retail value of the loot. By making the risk/return balance of dealing in stolen assets sufficiently unattractive, insurers can offer criminals a better alternative: "finders' rewards" allow criminals to extricate themselves from a crime by selling the loot back to the original owner at a reduced price.

4.3 Engaging with the State

Insurers create or support institutions to pool information to improve the effectiveness of policing, and insurers provide educational resources and training for police. Private registries (including for autos, ships, and art) and VINs facilitate early detection when thieves try to bring their loot to market and aid the police in recovering stolen assets and apprehending criminals. Pooling information on the crime is particularly helpful when policing is territorial and crime transcends administrative boundaries. For example, insurers are the main donors to the privately funded International Maritime Bureau's piracy reporting center.[9] The insurers' nationwide auto theft investigation network in the US complements the primarily local nature of most policing. Finally, insurers can provide, require, or incentivize the adoption of technology such as alarm systems, CCTV, GPS trackers, and fraud detection algorithms that can help the police secure convictions.

In some cases, insurers' assistance to law enforcement extends beyond the in-kind services and indirect activities just described. When expensive property crimes are insufficiently politically salient to produce adequate public support for law enforcement activities, insurers may opt to pay for the police powers they need to deter and prosecute crime, as we saw in the case of payment card fraud in the UK and the National Automobile Insurance Theft Bureau in the USA.

Finally, insurers lobby for regulation that requires manufacturers and service providers to harden targets (e.g., cars and cyber security). Insurers have also successfully lobbied to improve threat awareness through systematic (international) data collection and publication (e.g., the piracy reporting and statistics published by EU NavFor[10] and the Ransomware Taskforce request for ransomware incidents to be reported). We also observed lobbying for additional police or military support in the domains of kidnapping, piracy, auto theft, and ransomware.

4.4 Tolerating Crime in the Interest of Profitability

We observed insurers making interesting trade-offs between criminal losses and business profits. Security solutions that could deter or prevent many thefts may be resisted if they undermine the

[9] https://www.icc-ccs.org/piracy-reporting-centre/voluntary-sponsors.
[10] https://eunavfor.eu/key-facts-and-figures.

take-up of insurance (e.g., cyber-hygiene standards) or create very high losses when they fail. It is better for art thieves to occasionally take paintings in frames than risk an iconic masterpiece being destroyed. Ships' captains are expected to use passive defenses to prevent hostile boarding, but not to resist pirates once they have entered the ship: the risk of crew deaths and a total constructive loss is greater than the cost of a (well-managed) ransoming. Banks allow some (limited value) payments without the maximally effective authentication methods so that customers reduce their reliance on (overall more expensive) cash transactions. In auto insurance, many insurers resisted the salvage title because they stood to lose more on crashed cars than they stood to gain in terms of deterring theft.

Consistent with our themes of market logic and multiple, unstable equilibria, we found that insurers' mix of approaches varied significantly between crimes and over time. Technological innovations lower the marginal cost of crime deterrence by making it harder to commit a crime or avoid detection and capture. Whether or not insureds adopt them, however, depends on their marginal costs and benefits, as well as the ability of insurers to take collective action to force self-protection through conditionality, exclusions, limits, or regulation. Insurers collect and pool information when there is a mismatch between the geographical reach of criminal markets and that of policing—such as national registers in federal states (e.g., auto-theft), global registers for international markets (e.g., art) and Lloyd's market (transnational kidnap for ransom). Insurers are willing to pay for initiatives to aid law enforcement or to directly enhance police capacity if the economically efficient level of a specific crime from the insurers' point of view is below its current politically optimal level. However, when a crime becomes politically salient, insurers tend to lobby governments to adopt helpful regulation, facilitate or conduct data collection, or direct additional police resources toward the crime in question.

5. CONCLUSION

As our case studies illustrate, insurance organizations employ a host of tools and a market logic to govern crime in the interests of insurability. This research both supports and extends prior work on insurance as governance (e.g., Heimer 1985; Ericson et al 2003; Ben-Shahar & Logue 2012; Talesh 2015b). Much of that prior research, particularly in legal scholarship, has emphasized the potential social welfare benefits of insurance governance, among other reasons to make that governance more visible to scholars accustomed to understanding insurance as simply a mechanism for risk transfer and pooling. That focus has invited recent critique by legal scholars that challenges both the extent to which this governance takes place (Abraham & Schwarcz 2023) and the benign view of insurers said to follow from the prior research (Avraham & Porat 2022). Our case studies are consistent with the analysis of Abraham and Schwarcz, who also emphasized the profit motivation of insurers and who carefully explained the limits of private governance by insurers. On the other hand, the prior research that we draw on for our case studies suggests that the "conventional wisdom" that Avraham and Porat are attacking is something of a straw man. While the insurance as governance research has identified "insurers as private regulators of societal risks" (Avraham & Porat), that research has never suggested that insurers do so for any reason other than their own interests, nor has it suggested that insurers' interests can always be counted upon to line up with the public interest (e.g., Talesh 2015a, 2017; Ericson et al 2003).

With that said, however, our case studies provide several examples of insurers tolerating losses in the interests of profitability that Avraham and Porat could use in support of their argument that there is a "dark side" to insurance. In addition, we suspect that there may also be instances of insurers demanding a level of security that, from a social welfare perspective, may be too great, as is arguably the result when insurance prices and conditions lead investment art to be locked up rather than displayed to the public.

A qualitative meta-analysis of the sort that we employ here cannot quantify the extent or impact of the behavior that we observe. Nevertheless, the case studies further demonstrate that insurers can engage in useful governance (see also Rapaport 2017; Baker & Silver 2019), while illustrating the complex, evolutionary nature of that governance, the underlying market logic, and the limits of private insurance governance. Obviously, insurers govern in their own interests, a social fact that should not be understood as a critique of insurers. When it comes to crime, our case studies suggest that insurers have stepped in to address problems that governments have not adequately addressed, whether because of lack of jurisdiction, resources, or political salience. In stepping in, the insurers' goal is not to eliminate crime (as if that were possible), but rather to make criminal losses sustainably insurable—a goal that is not the same as maximizing social welfare. If the goal is the public

interest, insurance governance should be understood as only a complement to state governance. It is unreasonable to ask the insurance industry to be uniquely responsible for ensuring that insurance governance furthers the public interest. Sometimes, the state is absent or impaired, organized at the wrong level, slow to act, or simply focused on other priorities. In such a case, no one should expect anything from the insurance industry other than governance according to a market logic of the kind revealed in our case studies.

REFERENCES

Abraham, Kenneth & Daniel Schwarcz. 2023. The Limits of Regulation by Insurance. 98 *Indiana Law Rev.* (forthcoming).

Avraham, Ronen & Ariel Porat. 2022. The Dark Side of Insurance. U of Texas Law, Legal Studies Research Paper, SSRN: https://ssrn.com/abstract=4203765 or http://dx.doi.org/10.2139/ssrn.4203765.

Baker, Tom & Anja Shortland. 2022. Insurance and Enterprise: Cyberinsurance for Ransomware. Forthcoming in *Geneva Papers on Risk and Insurance*. https://link.springer.com/article/10.1057/s41288-022-00281-7

Baker, Tom & Charles Silver. 2019. How Liability Insurers Protect Patients and Improve Safety. 68 *DePaul Law Rev.* 209.

Barelli, John. 2019. *Stealing the Show: A History of Art and Crime in Six Thefts*. Lyons Books.

Barro, Josh. 2014. Here's Why Stealing Cars Went out of Fashion. *NYTimes August 12, 2014*.

Becker, Gary. 1968. Crime and Punishment: An Economic Approach. 76 *J. Polit. Econ.* 169–217.

Ben Shahar, Omri & Kyle Logue 2012. Outsourcing Regulation: How Insurance Reduces Moral Hazard. 111 *Mich. L. Rev*. 197–248.

Butterfield, F. 1990. Boston Museum Says It Was Uninsured for Theft. *New York Times* 20 March.

Calahane, Michael. 2015. A History of the UK intruder alarm industry 1852–2004. *Professional Security Magazine*. https://www.professionalsecurity.co.uk/reviews/a-history-of-the-uk-intruder-alarm-industry-1852-2004/

California Assembly. 1994. California Bill Analysis, Assembly Committee, 1993-1994 Regular Session, Senate Bill 1833.

Coveware. 2019. "Ransomware, Hackers, and … Guarantees?" *Coveware Blog* 3 January. https://www.coveware.com/blog/ransomware-guarantee-decryption (accessed 25 October 2022).

Coveware. 2022. "Ransomware as a Service Innovation Curve." *Coveware Blog* 27 January; available at https://www.coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve (accessed 11 October 2022).

Coyne, C. & P. Leeson. 2009. Who's to Protect Cyberspace? In Indira Carr, ed., *Computer Crime*. Routledge.

Dudley, Renee. 2019. The Extortion Economy: How Insurance Companies are Fueling a Rise in Ransomware Attacks. *ProPublica, August 27*.

Ericson, Richard, Aaron Doyle, & Dean Barry. 2003. *Insurance as Governance*. Toronto: University of Toronto Press.

Ericson, Richard V. & Kevin D. Haggarty. 1997. *Policing the Risk Society*. OUP.

Ericson, Richard V. & Kevin D. Haggarty. 2004. The Police Insurance Connection. 58 *CJM*. 28–29.

Ferapontov, A. 2020. Will an Immobilizer Save Your Car from being Stolen? *Kapersky Daily* 10 February https://www.kaspersky.co.uk/blog/36c3-immobilizers/18577/ (accessed 24 October 2022).

Field, Simon. 1993. Crime Prevention and the Costs of Auto Theft: An Economic Analysis. 1 *Crime Prev. Stud.* 69–91.

Flynn, T. 1998. Databases of Stolen Art can Help Thwart Art Thieves and Promote Vigilance. *The Art Newspaper 1 July*.

Fuentes, Mayra, Feike Hacquebord, Stephen Hilt, Ian Kenefick, Vladimir Kropotov, Robert McArdle, Fernando Mercês, & David Sancho. 2021. Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises against Them. *Trend Micro Research*. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them (accessed January 16, 2022).

Gourley, G. Douglas. 1953. In-Service Training of Policemen by Universities and Colleges. 44 *J Crim. Law Criminol. Police Sci.* 229–238.

Haymore, A. 2121. We Wait Because We Know You. *NCC Group Research*. https://research.nccgroup.com/2021/11/12/we-wait-because-we-know-you-inside-the-ransomware-negotiation-economics/ (accessed 24 October 2022).

Hayworth, Andrea. 1993. Stolen Artwork: Deciding Ownership Is No Pretty Picture. 43 *Duke Law J.* 337–383.
Heimer, Carol. 1985. *Reactive Risk and Rational Action: Managing Moral Hazard in Insurance Contracts*. Chicago: University of Chicago Press.
Insurance and Investment News. 1913. New Auto Theft Bureau Established. Feb 2014 at p. 184.
The Insurance Press. 1919. Automobile Insurance. May 28, 1919.
Kharraz, Amin, William Robertson, Davide Balzorotti, Leyla Bilge, & Engin Kirda. 2015. Cutting the Gordian Knot: A Look Under the Hook of Ransomware Attacks. In M. Almgren *et al*. eds., *Detection of Intrusion and Malware, and Vulnerability Assessment 2015 Proceedings*, 3–24. doi:10.1007/978-3-319-20550-21
Kinsella, E. 2004. Why Wasn't the Scream Insured? *ArtNews* 1 November.
Klerman D. & A. Shortland. 2022. The Transformation of the Art Market: Law, Norms and Institutions. 23 *Theoretical Enq. Law*. 219–241.
Krebs, Brian. 2010. "I'll Take Two Mastercards and a Visa Please" Krebs on Security Blog 22 September. https://krebsonsecurity.com/2010/09/ill-take-2-mastercards-and-a-visa-please/ (accessed 10 October 2022).
Longman, Mikel. 2006. The Problem of Auto Theft. In Eric Stauffer & Monica S. Bonfanti, eds., *Forensic Investigation of Stolen-Recovered and Other Crime-Related Vehicles*. Oxford: Elsevier.
McLeave, Hugh. 2003. *Rogues in the Gallery: The Modern Plague of Art Thefts*. Raleigh North Carolina: Boson Books.
Motor Vehicle Titling, Registration, and Salvage Advisory Committee. 1994. Final Report to Congress.
National Association of Attorneys General. 1979. Organized Auto Theft.
National Insurance Crime Bureau. 2020. *Vehicle Theft Toolkit for Elected Officials & Law Enforcement*. Chicago: NICB.
NCR. 2021. Credit Card Transaction Fraud Continues to Climb to New Heights. https://www.ncr.com/blogs/payments/credit-card-fraud-detection (accessed 25 October 2022).
New York Times. May 22 1986. Paintings in Ireland are Stolen. Late Edition (East Coast); New York, N.Y. [New York, N.Y].
Parris, Matthew. 2012. The Piracy Racket begins here in the City. *The Times*, 7 January.
Popper, Nathaniel. 2015. *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. Harper.
Rahm, D. 2014. Why Art Collectors Are Still Using Low-Tech Devices to Protect Their Million-Dollar Artwork. *Forbes* June 16. https://www.forbes.com/sites/daniellerahm/2014/06/16/why-art-collectors-are-still-using-low-tech-devices-to-protect-their-million-dollar-artwork/ (accessed 24 October 2022).
Rapaport, J. 2017. How Private Insurers Regulate Public Police, 130 *Harvard Law Rev*. 1539.
Reyburn, S. 2017. A Green Light for Art Criminals? *New York Times* 1 September.
Rosalski, Greg. 2022. Someone Stole my Truck. *NPR Planet Money* 23 August 2022.
Schwarcz, Daniel, Josephine Wolff, & Daniel Woods. 2023. How Privilege Undermines Cybersecurity. 36 *Har. J. Law Technol.* (forthcoming). doi:10.2139/ssrn.4175523
Shortland, Anja. 2019. *Kidnap: Inside the Ransom Business*. Oxford: OUP.
Shortland, Anja. 2021. *Lost Art: The Art Loss Register's Case Book*, Vol. 1. London: Unicorn.
Smylie, William T. 2006. Vehicle Identification. In Eric Stauffer & Monica S. Bonfanti, eds., *Forensic Investigation of Stolen-Recovered and Other Crime-Related Vehicles*. Oxford: Elsevier.
Talesh, Shauhin. 2015a. Legal Intermediaries: How Insurance Companies Construct the Meaning of Compliance with Antidiscrimination Laws. 37 *Law Policy* 209–239.
Talesh, Shauhin. 2015b. Insurance and the Law. In James Wright, ed., *International Encyclopedia of Social and Behavioral Science*, 2nd edition, Vol. 12, 215–220. Oxford: Elsevier.
Talesh, Shauhin A. 2017. Insurance Companies as Corporate Regulators: The Good, The Bad, and The Ugly. 66 *Depaul L. Rev*. 490.
Tamaki, Julie. 1993. Wrecks Die But Not Their IDs. *Los Angeles Times May* 19.
The Standard. 1928. New Auto Theft Organization Formed. 102: 1012. Boston: Standard Publishing. https://spcpub.com/page.cfm?name=The_Standard&teaser=30
United States House of Representatives. 1994. Salvage Vehicle Title Reform. Hearings before the Subcommittee on Commerce, Consumer Protection, and Competitiveness of the Committee on Energy and Commerce, House of Representatives, One Hundred Third Congress, second session, September 21, 1994.
United States House of Representatives. 1996. The National Motor Vehicle Safety, Anti-Theft, Title Reform and Consumer Protection Act of 1995: hearing before the Subcommittee on Commerce, Trade, and

Hazardous Materials of the Committee on Commerce, House of Representatives, One Hundred Fourth Congress, second session, on H.R. 2900, September 12, 1996.

United States Senate. 1979. Professional Motor Vehicle Theft and Chop Shops. Hearings before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, 96th Congress, First Session, November 27, 28, 29, 30 and December 4 1979.

United States Senate. 1997. S. 852, the National Motor Vehicle Safety, Antitheft, Title Reform, and Consumer Protection Act of 1997: hearing before the Committee on Commerce, Science, and Transportation, United States Senate, One Hundred Fifth Congress, first session, September 25, 1997.

van Ours, Jan & Ben Vollaard. 2016. The Engine Immobiliser: A Non-starter for Car Thieves. 126 *Economic J.* 1264–1291.

VISA 2022. The Evolution of Payment Security. https://usa.visa.com/dam/VCOM/regional/na/us/visa-everywhere/documents/visa-security-timeline.pdf (accessed 25 October 2022).

Vollmer, August. 1936. *The Police in Modern Society*. Berkeley: University of California Press.

Voreacos, David, Katherine Chiglinsky, & Riley Griffin. 2019. Merck Cyberattack's $1.3 Billion Question: Was it an Act of War? *Bloomberg, December*.

Weber Tobias, Marc. 2015. Another Reason not to Steal Cars. *Forbes 24 September*.

Wilding, Edward. 1990. Trojan Horse: AIDS Disk. *Virus Bulletin January 1990: 3–7*.

Wilson, J. 1999. How the Counterfeiters Alter and Forge Cards to Fool the Retailers. *The Guardian 17 February*.

Woods, Daniel & Rainer Böhme. 2021. Incident Response as a Lawyers' Service. *IEEE Security & Privacy*. In print, doi:10.1109/MSEC.2021.3096742

Wolff, J. 2016. Why Is the U.S. Determined to Have the Least-Secure Credit Cards in the World? *The Atlantic 10 March*.

Young, Adam & Moti Yung. 1996. Cryptovirology: extortion-based security threats and countermeasures. *Proceedings 1996 IEEE Symposium on Security and Privacy*. IEEE Symposium on Security and Privacy. pp. 129–140. doi:10.1109/SECPRI.1996.502676

Young, Adam & Moti Yung. 2017. Cryptovirology: The Birth, Neglect, and Explosion of Ransomware. 60 *Commun. ACM*. 24–26.