11-22-2022

The Government Behind Insurance Governance: Lessons for Ransomware

Tom Baker
University of Pennsylvania Carey Law School

Anja Shortland
King's College London

Recommended Citation
17 Reg. & Governance (2023)

Regulation & Governance

Regulation & Governance (2022) doi:10.1111/rego.12505

The government behind insurance governance: Lessons for ransomware

Tom Baker

Penn Carey Law, University of Pennsylvania, Philadelphia, Pennsylvania, USA

Anja Shortland

Department of Political Economy, King's College London, London, UK

Abstract

The insurance as governance literature focuses on the ability of private enterprises to collectively regulate, pool, and distribute risks. This paper analyzes how governments support insurance markets to maintain insurability and limit risks to society. We propose a new conceptual framework grouping government interventions into three dimensions: regulation of risky activity, public investment in risk reduction, and co-insurance. We apply this framework to six case studies, describing insurance markets' reliance on public support in more analytically precise terms. We analyze how mature insurance markets overcame insurability challenges akin to those currently presented by extortive cybercrime. Private governance struggled when markets grew too big for informal coordination or when (tail) risks escalated. Government interventions vary widely. Some governments prioritize supporting economic activity while others concentrate on containing risks. Governments also choose between risk reduction and ex post socialization of losses. We apply these insights to the market for ransomware insurance, discussing the merits and potential hazards of current proposals for government intervention.

Keywords: insurance, public/private partnership, ransomware, regulation, self-governance.

1. Introduction

A growing body of sociolegal research analyzes the governance functions of insurance (Baker, 2010; Ericson et al., 2003; Herr, 2021). Building on the foundational research of Heimer (1985), scholars and policymakers increasingly recognize that insurance not only pools and shifts risks, but also manages and reduces risks by regulating risk-taking behavior (Abraham & Schwarcz, 2023; Ben-Shahar & Logue, 2012). Governance by insurers is a rational response to the twin problems of moral hazard and adverse selection (Heimer, 1985). Insurers manage adverse selection by screening applicants for their risk exposure, and they manage their applicants' moral hazard through conditionality, incentives, limits, and exclusions (Heimer, 1985). Parchomovsky and Siegelman (2022) highlight a further problem for insurers: third-party moral hazard. Here, criminals target the insured to tap into generous insurance-funded pay-outs or service providers inflate bills covered by insurers. Insurers, therefore, also monitor and reduce opportunities for third parties to cause or exaggerate losses. Shortland (2019) analyzes the sophisticated remedies to reduce third-party moral hazard in kidnap for ransom insurance: making it difficult to discover the insurance relationship, turning the insured into hard targets through security advice and training, and reducing the profitability of kidnaps by taking control of ransom negotiations.

Ben-Shahar and Logue (2012) and O'Malley (1991) argue that in some areas, insurers may have significant advantages over governments in the regulation of safety. That line of research may suggest why we observe a palpable sense of disappointment that cyber-insurance has failed to provide effective governance in the current "ransomware epidemic" (Logue & Shnidermann, 2022; Talesh & Cunningham, 2021; Wolff, 2022). Ransomware insurance may even increase risks by funding ever-increasing ransom demands, facilitating, and normalizing payments to criminal groups, thereby generating more demand for insurance and hence premium income

Correspondence: Anja Shortland, Department of Political Economy, King's College London, London WC2B 6NR, UK. Email: anja.shortland@kcl.ac.uk

Accepted for publication 22 October 2022.

(Dudley, 2019). According to this line of reasoning, it would be in the public interest to tightly regulate or even ban ransomware insurance (Logue & Shnidermann, 2022).

By contrast, liberal scholars and industry insiders expect the market to develop private solutions to reduce the incidence and severity of cybercrime (Lubin, 2021a; Ransomware Task force, 2021). Immature insurance markets countering a dynamic threat are bound to have teething troubles. It is hardly surprising that many insurers underestimated cyber risks. Claims have spiraled due to significant criminal innovations, among them the increasingly sophisticated industrial organization of cybercrime (Lusthaus, 2018), the use of exfiltrated data to drive up ransoms (Coveware, 2021), and criminals sheltering in countries unwilling to extradite them (Kay, 2021). Shifting criminal threats require the adaptation of security and resilience-enhancing strategies (Beaman et al., 2021). It then takes time for the evolutionary competition in private governance systems to select superior solutions and create resilient institutions (Ostrom, 2010). Interrupting that process with public regulation could have the unintended consequence of preventing or stifling innovation (Lubin, 2021b).

The question thus arises whether calls for government action should be heeded at this stage and, if so, what form such intervention should take. This situation presents an opportunity to take a fresh look at public and private governance in insurance markets. In this paper, we present a new conceptual framework for analyzing the relationship between governments and insurance markets. We take the presence of traditional insurance regulation, such as licensing, safety and soundness regulation, market conduct regulation, and contract enforcement as a given. This type of regulation is essential to ensure the functioning of insurance markets and has been studied in detail (e.g., Schwarcz, 2015). The contribution of this paper is to explore how governments can—in addition—influence or shift the risks created by the insured economic activities. We classify and examine such government interventions in three dimensions: regulation of risk-taking, public investment, and co-insurance. We apply this framework to six mature insurance markets to describe their reliance on public support in more analytically precise terms and to analyze how they overcame serious viability challenges akin to those currently presented by extortive cybercrime.

Our three-dimensional framework reveals distinct regimes in different insurance markets, ranging from mostly privately regulated (K&R) to largely publicly governed (aviation terrorism risks, environmental liabilities). We find that private governance regimes can erode in fast-growing markets and can break down when risks suddenly escalate. When risks become (temporarily) uninsurable, governments support private insurance markets in different ways. Some prioritize supporting economic activity while others concentrate on containing risks to society. Governments also face choices between *ex ante* risk reduction and *ex post* socialization of losses. Our analysis suggests that some politically attractive short-term interventions impose longer-run costs on societies. The public interest may be served better if government intervention is designed to support rather than stifle self-protection and innovation.

2. A three-dimensional framework of government intervention

One definition of an efficient insurance market is that all stakeholders mutually satisfy their interests (Pal et al., 2021). When insureds can influence the frequency or severity of loss, insurers may require them to reduce risks that are within their control. Appropriate self-protection makes insurance sustainable and satisfies the policy objective that insurance facilitate private enterprise without raising the overall level of risk to society. However, when insurers compete for large-scale business, customers have market power. Brokers push insurers to compete on terms and conditions as well as price. Competition on terms prevents insurers from being excessively cautious. This is important, because insurance exists to "liberate" economic activity rather than choking off socially desirable activities through costly conditionality (Baker & Shortland, 2022a; Ewald, 1991). Yet, competition can also lead to sub-optimal safety standards. If so, both insurers and society face a higher than optimal level of risk.

In these cases, insurance products can be made more profitable through collective action. Insurers may, for example, agree to impose minimum standards of self-protection. Insurers may also collectively reduce the level of risk faced by their customers. For example, in 1833 t private insurance companies created the London Fire Engine Establishment. They had realized that (a) it was cheaper to put out fires than to rebuild houses, and (b) that major conflagrations could be prevented if fires were put out by the closest-available firefighters rather than waiting for the responsible insurer's brigade to arrive. London insurers thus created an integrated fire service

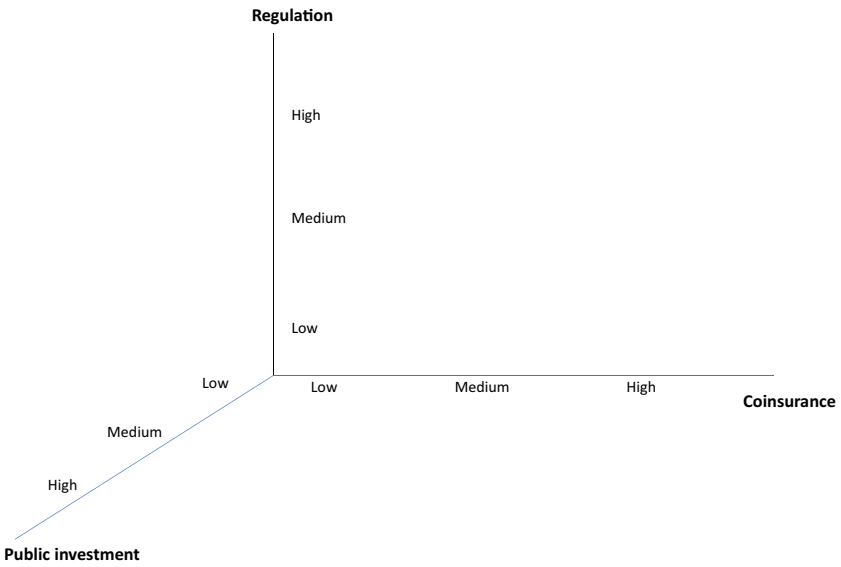

FIGURE 1 Three-dimensional framework

(Zurich, 2020). If collective action is unsuccessful or only partially successful, insurers act individually by reducing the amount of cover they provide. When the insureds bear higher risks, they may behave more carefully, but socially desirable activities may not be undertaken.

We classify the main ways in which governments support insurance markets to reduce insured risks into three categories. First, governments can create safety standards for the underlying insured economic activity through formal regulation. In this case, suitable (levels of) security measures are specified and perhaps officially certified, and their adoption can be encouraged or mandated by the state. State involvement in standard-setting and regulation thus occurs at different intensities. We indicate this on the *y*-axis of our framework as shown in Figure 1. At the lower end of the *y*-axis governments merely support the creation of private security standards, for example, by mandating that incidents are reported and publishing that information. Governments may also create public standards to increase transparency about business practices—for example, the fuel economy standard system in the US.[1] Companies choose the standard they want to operate at, and customers and insurers take this into account when deciding whether to do business with them. At the highest intensity, safety standards are made mandatory.

Second, government can invest public funds to reduce risk. They can fund public infrastructure or services that reduce risk directly, and they can provide grants or other incentives to private organizations to reduce their risk. (Insurers may further encourage such investments by reducing the premium to reflect the lowered risk [Kuhnreuter, 2019].) Governments can also invest indirectly by funding enforcement actions, whether against threat actors or against firms that fail to comply with the standards set by regulation. While governments generally finance enforcement efforts, there are many examples of successful co-funding. Government can create private rights of action that recruit private parties to serve as legal enforcers, with the resources of the state coming primarily in the form of the court system (Burbank et al., 2013), and private firms can contribute to public efforts to reduce threats. The latter occurs routinely when private actors fund the suits that enforce private rights of action. Private actors also sometimes fund public enforcement. For example, British financial institutions co-fund a Dedicated Card and Crime Unit within London's Metropolitan Police to tackle card, check, and payment fraud.[2] Who bears what percentage of the cost, and the desired level of provision are negotiated between stakeholders. We examine the intensity of public investment risk reduction on the *z*-axis.

Third, governments can co-insure risks. Co-insurance arrangements can be explicit or implicit and, again, intervention can happen at different intensities. States can directly provide services for individuals who are unable to access private insurance (e.g., state medical facilities). Governments can provide disaster relief for the uninsured and under-insured, for example, after floods or riots, at varying levels of generosity. Governments may

also be residual risk bearers: for example, when the responsible parties lack sufficient assets to fulfill their obligations under liability regimes, as can occur in the case of environmental damage, when governments bail out companies to prevent systemic risk to the economy, or when governments provide guarantee funds when insurers go insolvent (Moss, 2004). States tend to insure catastrophic risks that would bankrupt private insurance companies and for which private reinsurance markets fail to develop—such as terrorism, war, and major natural disasters. Even when markets could theoretically deal with tail risks, private insurance may be more expensive than the private benefit from undertaking an activity. In these cases, governments may support a sector through publicly provided (re)insurance. At the extreme end of our *x*-axis, private insurance no longer exists, because the economic activity is state-owned and state-run.

The importance of government action for private insurance markets helps explain why insurers are so active in lobbying governments. While some lobbying may well represent the rent-seeking behavior commonly assumed, other lobbying represents a form of collective action that creates and preserves sustainable insurance markets. For example, in 1865—after several years of intense pressure by insurers—the public-sector Metropolitan Fire Brigade replaced the private London Fire Engine Establishment. This is widely regarded as a public policy achievement for the public at large as well as the insurance industry (Zurich, 2020).

We place the levels of government activity on these axes in our case studies at low, medium, and high based on the financial and legislative resources committed by governments. Thus, along the regulation dimension: a court recognizing a private standard as a standard of care for tort liability that helps to manage moral hazard is a low intervention; a government agency certifying a private standard is a medium intervention; creating a public standard requires yet higher government effort and a government agency mandating a standard is a high intensity intervention. On the investment dimension: providing a basic public (court) infrastructure for private entities to sue those whose have harmed them is a low intervention; government investment in risk reduction infrastructure and in policing and enforcement can be medium to high interventions depending on intensity; and government funding of private risk reduction and private funding of government enforcement are medium interventions. On the co-insurance dimension: the lowest intervention category is implicit rather than explicit insurance and only for residual risk; the highest intervention is explicit insurance for all risk arising from specific activity; and a medium intervention would be something between those poles, such as discretionary, after-the-fact disaster relief or explicit insurance with a high attachment point or partial coverage.

As should be clear, we do not have a measuring stick or an algorithm. Our goals for this article do not require the precision that a claim to possess either tool would imply. We use the concept of three "dimensions" and the resulting charts that we present for the first case studies as a visual metaphor that illustrates the range and variation of government involvement in tricky insurance markets. In the analysis section below, we present a table that classifies government activity in each of the case studies in a fashion that could be used to generate similar charts for each of the cases studies and the variations within them.

3. Case studies

In this section, we study government involvement in six insurance markets that faced serious viability problems in the past. In all our cases, the economic activity in question would not be undertaken at socially optimal levels without the availability of affordable insurance. If companies operate without insurance they could be bankrupted by extreme losses, with society bearing the residual cost. We selected insurance products where customers have significant market power to resist command-and-control style governance by insurers and where the cost of significant risk-reduction or self-defense is understood to be greater than the premium rebate that insurers can offer to cautious customers. Therefore, insurers can only drive safety improvements when competition on security conditions is restricted.

We do not claim that these six case studies provide the optimal comparison or learning set for the ransomware insurance market. However, they do provide good illustrations of the three-dimensional framework and each case study illuminates one or more challenges that ransomware insurance currently faces: balancing the desire of customers to recover staff or assets safely and quickly against the danger of incentivizing crime, managing moral hazard, and extreme tail risks.

3.1. Art theft insurance

The art price boom of the 1980s expanded the demand for insurance while putting the insurability of top-end art into question. Art theft was relatively easy and increasingly profitable. Insurers struggled to encourage their customers to properly secure their collections: high-end safety interferes with sharing and enjoying art. Mostly, stolen and looted art circulated freely in the art market. Well-known objects that were too hot to fence could be ransomed back to their original owners (Shortland, 2021). Insurers had to act fast to reverse rising losses. Offering partial insurance, that is, insuring objects for a fraction of their market value, encouraged better self-protection. However, insurers also acted collectively to reduce the profitability of art theft by transforming the norms and processes of the art market (Klerman & Shortland, 2022).

In the early 1990s, art insurers at Lloyd's of London co-funded the creation a private database of lost and stolen art from their claims data—the Art Loss Register (ALR). Over time, an ever-increasing proportion of auction houses and dealers made it part of their due diligence procedure to consult the ALR database. If an object is matched to one reported as stolen, it cannot be bought or sold in good faith. Ideally, dealers and auctioneers impound the disputed artwork until the claim is resolved (though sometimes they merely reject the consignment). If it is suspected that the original thief or their accomplices are still in the picture, the police are alerted. If the police are unable to seize the object and apprehend the criminals, they may authorize the ALR to pay a small reward for its retrieval.[3] If a collector has acquired good title through adverse possession, ALR subscribers still refuse to buy or sell the object until the current owners have compensated the former owners (Shortland, 2021). Insurers thereby reduced the attractiveness of art theft. First, the ALR's excellent links with public law enforcement raise the risk of stealing and dealing in stolen art. Second, the expectation of having to settle with former owners reduces the market value of stolen art. Third, although the ALR provides a channel for re-legitimizing stolen artworks, protracted negotiations, the risk of exposure, and low compensation payments discourage further art thefts (Shortland, 2021).

Yet, this is not a purely privately governed insurance market. Governments participate in all three governance dimensions when it is perceived to be in the public interest. In terms of regulation, artworks declared "national treasures" or "cultural heritage" receive public protection. Buyers cannot acquire secure property rights, as "cultural heritage" can be reclaimed by the source government indefinitely. These regulations are publicly enforced by customs: objects crossing state or international borders without the correct paperwork are seized without compensation. Governments also provide police protection for national collections. On the coinsurance dimension, governments sometimes take on the tail-end risks of major exhibitions through formal indemnity schemes. All losses from public museums are borne by society. Some governments pay for the retrieval of stolen artworks, such as the recovery of two Turner paintings on behalf of the Tate Gallery in London in a shady £3.5 million deal (Nairne, 2012). However, this form of coinsurance can be counterproductive in that it may encourage further art thefts. Detailed analysis thus shows that at the top end of the market government involvement is pervasive. Figure 2 reflects our assessment of the resulting government involvement in the trophy art insurance market: medium in the regulatory dimension, reflecting the regulations discussed above; medium in the investment dimension, reflecting government enforcement and government ownership of some museums and their collections; and medium in the co-insurance dimension, reflecting the explicit government insurance for the risks of major exhibitions.

By comparison, we classify the government involvement in the mid-market art insurance markets as low on each of these dimensions: for government regulation there is only the ordinary tort law standard of care and general criminal law, for government investment there is only the access to courts and ordinary criminal law enforcement, and for government co-insurance there is only the general guaranty funds that (partially) backstop insolvent insurance companies.

3.2. Terrorism insurance for commercial property

Like natural catastrophes, terrorism risks are relatively rare but can cause ruinous losses. Unlike natural catastrophes, however, terrorism is not random but targeted and timed to cause maximum economic and psychological damage. This complicates insurers' ability to calculate premium and spread risks. For example, exposure is highly concentrated in the commercial centers of major cities. A major terrorist attack in any metropolis could bankrupt

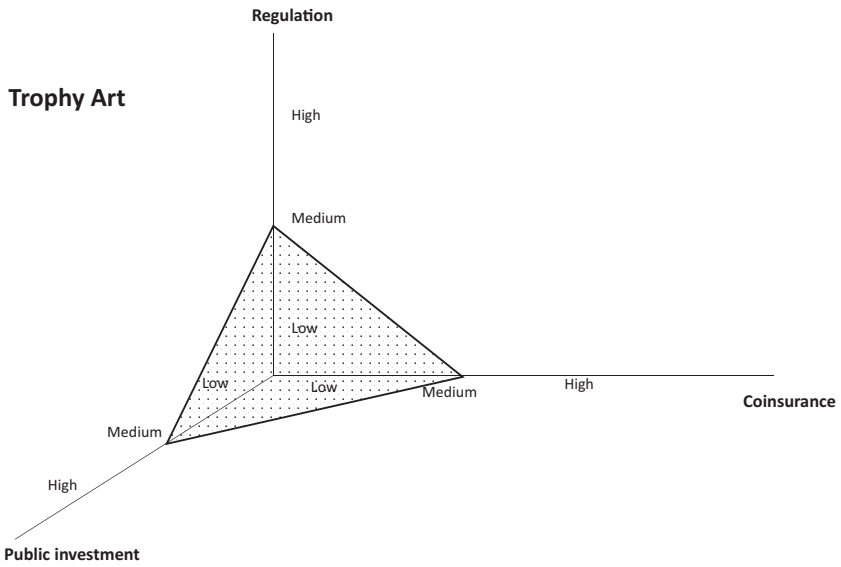

FIGURE 2 Government support for art insurance

some insurers, so terrorism insurance relies on the availability of (affordable) reinsurance. When terrorist activity escalates or terrorists change their tactics, reinsurers may (temporarily) withdraw from the market as they learn to evaluate the new risks. For example, in the early 1990s the Irish Republican Army mounted a bombing campaign in the United Kingdom. When a bomb detonated in London's financial district in April 1992, it caused hundreds of millions of pounds in damages. Unable to assess their exposure under the enhanced threat, European and British reinsurers announced that they would withdraw terrorism cover from reinsurance contracts as of January 1993. Direct insurers reacted by excluding terrorism risks from property insurance, fueling fears of collapsing property prices triggering an economic crisis (Bice, 1994).

The British government thus set up Pool Reinsurance: a mutual reinsurance company for terrorism property risks drawn from the membership of the Association of British Insurers backed by a government guarantee. After the September 11 attack on the World Trade Center in New York in 2001, the United States and many European governments followed suit with similar schemes (ECB, 2007; US Congress, 2002). The aim is always to support rather than replace private insurance markets, so governments generally assume responsibility for extreme tail risks only. Above a set threshold, liabilities are shared between the public and private sector or covered entirely by the government. To protect the tax-payer interest, governments create means to recoup (at least some of) their assistance payments. For example, beneficiaries may have to repay emergency loans, or governments may levy a surcharge on a wide range of insurance policies after an event (Kuhnreuter, 2019). Figure 3 reflects our assessment of the resulting government involvement in the terrorism risks aspect of the commercial property insurance market: low in the regulatory dimension, reflecting a decision to support private security standards; medium in the investment dimension, reflecting the availability of government security grants for private organizations and government efforts to identify and interdict terrorism; and medium in the co-insurance dimension, reflecting explicit government insurance but only for the extreme tail of terrorism losses.

Notably, the experience of government-backed terrorism insurance raises the question whether terrorism risk is in fact uninsurable. By 2021, Pool Reinsurance had built up £6.5billion in reserves and never called for treasury support to cover more than £1.25billion in claims.[4] Jaffee and Russell (2007) point out that while catastrophic terrorism losses remain a possibility and risks cannot be precisely estimated, major natural disasters such as hurricanes and earthquakes share these properties. Ambiguity can be priced, and ambiguity aversion compensated. The natural disaster insurance market in the United States regularly absorbs losses exceeding the uniquely high cost of the September 11 attacks. However, once a government-backed scheme is implemented its beneficiaries tend to lobby for its continuation. Although the US Terrorism Risk Insurance Act of 2002 was originally intended as a three-year scheme it was renewed in 2005, 2007, 2015, and 2019, with the next review scheduled for 2027.

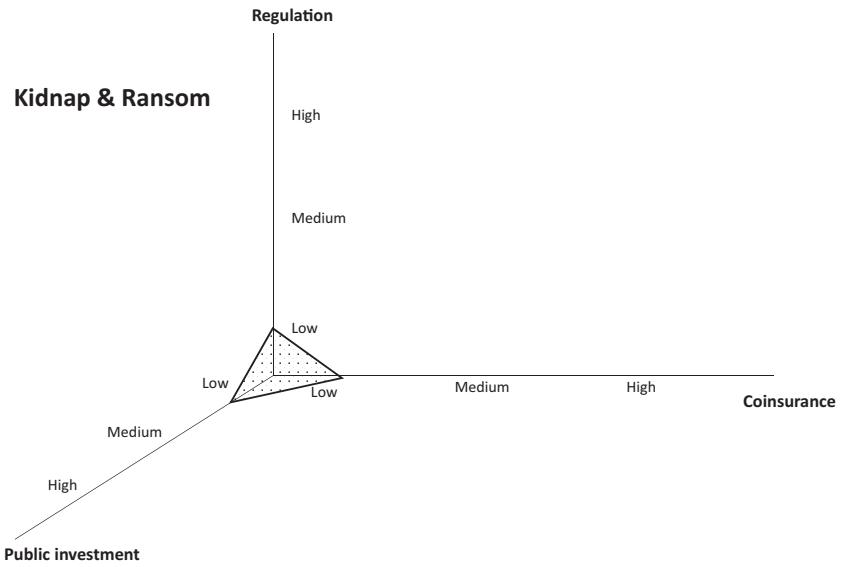

FIGURE 3 Government support for terrorism insurance

Even if government lending facilities are not called upon, co-insurance is not costless: it distorts incentives for self-protection. Under a private regime, insurance premia for real estate in the highest risk locations would rise, encouraging firms to diversify into lower risk areas and take additional precautions. Such adjustments leave the economy more resilient to future attacks (Jaffee, 2005). Kuhnreuter (2019), therefore, suggests that the US government should be more proactive in encouraging commercial enterprises to invest in risk reduction. Governments could also tighten security standards through regulation, but so far, such initiatives have largely been confined to civil aviation. Thus, while explicit co-insurance addresses the (perceived) problem of non-insurability it creates second-order problems that governments may be called upon to fix. The footprint of government in the insurance market may thus grow continuously, beyond whatever underlying need may remain.

3.3. Kidnap for ransom insurance

K&R insurance sold to corporations engaged in international commerce can be seen as a poster child of private governance (Shortland, 2017). It has existed since the 1930s, is widely available, and facilitates foreign direct investment, oil and mineral extraction, aid delivery, research, and reporting in areas of limited statehood. K&R insurance is conditional on customers obtaining and following security advice appropriate to the threat level. This makes the insureds hard targets and transnational kidnaps extremely rare. If they occur, K&R insurers have created strong norms and procedures for how they should be resolved. Safeguarding the life and health of hostages has topmost priority, but the resolution protocol frustrates kidnappers' ambition to make a quick profit from abductions. Tough and slow bargaining—led by professional negotiators—discourages opportunistic kidnapping and puts downward pressure on ransoms. By raising the risks and lowering the rewards of kidnapping, the criminal threat is reduced for all (Shortland, 2017).

The key to preventing an erosion of safety standards and the bargaining protocol is that K&R insurers do not compete on the rules underpinning the market. Almost all K&R insurance is written or reinsured in the Lloyd's market in London (Shortland, 2019). Circa 20 insurance companies in the market, led by three to four dominant syndicates, govern themselves informally as a club. Its members jointly create the common good of market order by sharing information and adhering to the club's rules and norms (Stringham, 2015). If kidnaps or ransoms rise, this indicates that a member or their subcontractors may have made mistakes, or that criminals have innovated. Remedies are discussed and explored within the tightly interlinked underwriting, security consultancy, and crisis response communities. Lloyd's clear and effective rules for ending club membership ensure compliance (Shortland, 2019).

The involvement of governments is subtle but essential in the provision of K&R insurance. First, in the regulation domain K&R insurers rely on firms' legal "duty of care" toward their employees. This justifies paying

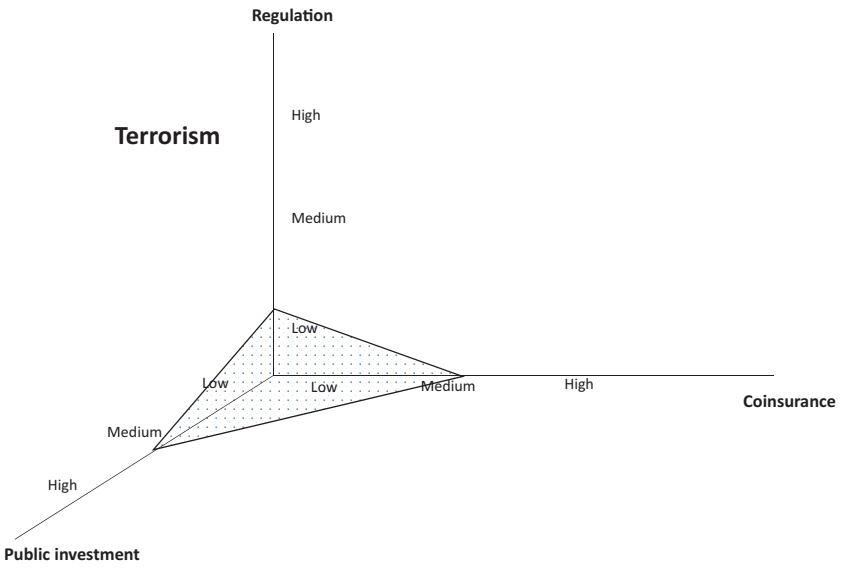

FIGURE 4 Government support for K&R insurance

(limited) ransoms to retrieve kidnapped staff. The legal duty of care also enables hostages and their families to sue employers that took shortcuts in safeguarding staff or bungled ransom negotiations. The track record of K&R insurers' crisis responders in retrieving hostages and the liability risk arising from failing to obtain or ignoring first-class security or negotiation advice makes K&R insurance highly advisable. This reduces the ability of companies to negotiate on conditionality or engage in moral hazard behavior once insurance is obtained. Second, the security consultancies retained by K&R insurers sometimes negotiate deals with host governments to bolster protection for their customers such as police or military guards around their customers' installations. Third, Lloyd's insurers can act collectively to encourage governments to provide additional resources for law enforcement. When the Lloyd's Joint War Committee threatens to list an area as having an "enhanced risk" or a "war risk" affected companies lobby governments to enhance security. When K&R insurers advise their customers to evacuate a location, host governments generally act swiftly to restore order to maintain economic activity and tax income. Thus, while the market is largely privately governed, at a more granular level state management of criminal or rebel threats is not uncommon. Figure 4 reflects our assessment of the resulting government involvement in the K&R insurance: low in the regulation dimension reflecting the ordinary duty of care standard, low in the investment dimension reflecting the limited and sporadic involvement of government in enforcement efforts, and very low in the coinsurance dimension, reflecting the discretionary, implicit government backstop of Lloyd's illustrated by the regulatory support of the Lloyd's Reconstruction and Renewal effort that occurred in the 1990s when Lloyd's solvency was at risk (Baker, 2021).

K&R insurance is highly vulnerable to (naïve) outside competition. A good example is hijack for ransom insurance, which became popular with the rising threat of Somali piracy from 2008. New insurers pushed into what looked like a lucrative business, competing on the basis that "time is money" while ignoring the problem of 3rd party moral hazard. Initially, ransoms were a small fraction of the cost of having a ship out of action, cargo delayed and a crew maltreated. Yet, pirates quickly adjusted their ransoms upwards when they met only token resistance from negotiators. Rising ransoms led to an explosion of piracy: hijacks, ransoms and negotiation periods escalated. Governments responded with an unprecedented international naval counterpiracy effort—that nonetheless failed to contain the problem (World Bank, 2013).

Navies thus called on governments and insurers to require better self-protection by ship-owners. The European Naval Force (EUNavFor) started to collect and publish high quality piracy incident data in real time and coordinated the development of increasingly stringent Best Management Practice (BMP) protocols for transits of the high-risk area with a wide range of stakeholders.[5] As the insurance market contracted sharply, the remaining insurers made adopting BMP a precondition of insurance. The mixture of public investment (navies)

and standard setting (BMP) eventually succeeded in suppressing the piracy threat. However, the cost of—temporarily—ignoring 3rd party moral hazard led to a permanently higher state footprint in what had previously been a mostly privately governed insurance market. Accordingly, we classify the government involvement in the hijack for ransom insurance market as medium in the regulation dimension, medium in the public investment dimension, and low in the co-insurance dimension.

Banning ransom payments is a commonly discussed remedy to kidnap for ransom. It is already in place for kidnappings by proscribed organizations. Neither families nor firms may offer a ransom for hostages held by terrorists, crisis responders may not facilitate a payment and insurers cannot reimburse it. Only sovereign governments can decide whether to ransom their citizens, and many do—for exorbitant amounts of money compared to ransoms paid to criminal kidnappers (Shortland & Keatinge, 2017). Governments that negotiate with terrorists thus replace private kidnap insurance with (highly costly) public insurance. Making this public insurance sustainable requires public risk reduction measures both on the regulation and the public investment dimensions to fortify the potential targets (e.g., diplomatic staff). Thus, the cost of maintaining a presence in a "terrorist" area is costly government intervention: at least medium in all three dimensions, if not higher.

3.4. Arctic shipping and marine insurance

As climate change progresses, the Arctic Ocean attracts increasing transit and destination traffic (Sarrabezoles et al., 2014). The Northwest Passage and the North Sea Route between the Atlantic and the Pacific oceans promise significant cost savings for trade between Europe and Asia. The Arctic also holds significant deposits of oil, gas, and minerals (Gautier et al., 2009) and arctic destinations are increasingly popular with cruise ship operators. There are massive risks associated with shipping in this environmentally fragile and remote area. Harsh sea and weather conditions, icebergs, pack ice, and underwater navigational hazards are an ever-present danger. Major incidents could easily overwhelm search and rescue and local health care facilities. Salvage operations are often delayed, increasing the risk of leakage of fuel or loss of cargo. Liability for environmental pollution, loss of life, personal injury, or becoming marooned can run into the hundreds of millions of dollars (Saul, 2020). Thus, availability of (affordable) insurance is a key factor in the development of arctic shipping (Sarrabezoles et al., 2014).

Self-protection and loss mitigation are crucial for insurability. Ships' hulls can be strengthened to withstand ice impact. Ice-trained helmsmen, additional engine room staff and deck-crew, as well as permanently alert lookouts can prevent accidents and equipment failure. Ships should carry additional fuel, water, food stocks, heaters, and blasting equipment. Some voyages require icebreaker and ice pilot support (International Chamber of Shipping, 2019). How do insurers prevent a race to the bottom on these hugely costly security measures? Until the 1990s, the market for marine (and especially hull) insurance was highly concentrated at Lloyd's of London. Conditions for insurance were determined in the Lloyd's club of underwriters through the Navigating Limits Sub-committee. Only the most experienced and cautious ship-owners could obtain arctic insurance (Sarrabezoles et al., 2014). In this era, government intervention was low in all three dimensions.

However, when rising demand was choked off by risk-averse club governance, new competitors entered the market. Chinese, Scandinavian, and London insurers outside Lloyd's gained significant market shares in hull insurance in the 2000s. Underwriting practices deteriorated. The Lloyd's Navigating Limits Sub-committee and the Lloyd's Register which had developed and dominated the design, construction, and in-service standards for "ice class" ships became mere reference points. There were growing concerns that arctic shipping was neither safe nor environmentally sustainable. Collective action was needed to turn "guidelines," "advice," and "recommendations" into binding obligations. Hull insurers, therefore, jointly developed a consensus on desired standards and information-sharing through the International Union of Maritime Insurers and a 2014 workshop at Lloyd's including the Swedish Club, the Swedish Polar Research Secretariat, and the Nordic Association of Marine Insurers. They then lobbied for their preferred standards to be made mandatory though the United Nations Convention on the Law of the Seas (UNCLOS). Even if flag states do not enforce the rules, ship-owners are compelled to comply with IMO regulations by port states or as a condition for passage through territorial waters.

The International Union of Maritime Insurers contributed technical knowledge on best practices in arctic shipping and drafted the amendments to the existing IMO conventions—alongside arctic council members, environmental protection agencies, and ship-owners associations (Arctic Portal, 2016). Insurers succeeded in

incorporating the concept of "ice classes" and polar training for seafarers into the IMO's Polar Code. Compliance with the Polar Code became mandatory for new ships in January 2017 under the conventions of Safety of Life at Sea (SOLAS) and Prevention of Pollution from Ships (MARPOL). In addition, arctic shipping data is centrally collected in the Arctic Shipping Traffic Database (ASTD) improving risk modeling—including that of private insurers.[6]

Governments remain involved in all three dimensions, however, particularly in the littoral states. For example, Russia made a massive public investment in nuclear-powered ice breakers to cut risks for domestic ship-owners. Russia also mandates that foreign ships meet Russian ice class standards in their territorial waters and hire (Russian) pilots and icebreakers on the North Sea Route (Moe, 2020). Canada has its own safety and pollution prevention regulations for arctic shipping, building on the SOLAS and MARPOL regulations. Some governments sponsor or undertake activities that are too expensive to insure such as arctic exploration and seismic mapping. The Chinese state-owned shipping company COSCO uses the Northern Sea Route for cargo transports (Humpert, 2019). We consider these latter activities as examples of government intervention in the (co-) insurance dimension. Thus, we find that the result of increasing competition between insurers is more enterprise as well as pervasive government intervention in all three governance dimensions, with the precise levels differing depending on the location (e.g., Russian territorial waters) or ownership (e.g., COSCO).

3.5. Environmental liability insurance

Liability regimes force companies (and individuals) to take financial responsibility for the damage caused by their actions to their staff, customers, shareholders, the wider public, and the environment. This makes firms more cautious, reduces demands for governments to compensate victims, and shifts the financial burden of clean-up operations to the private sector. And, significantly for our purposes, liability creates a demand for liability insurance.

Until the 1970s, general liability insurance policies covered environmental liabilities for bodily injury and property damage. The standard coverage made insurers liable for insureds' present liabilities under policies sold in the (sometimes distant) past. Insurers were, thus, vulnerable to what European insurers refer to as development risk: changes in the liability rules that expose them to greater liability than expected at the time they sold their policies (Baker, 2002). In the late 1960s and early 1970s, the US government increased the scale of potential liability for environmental damage incidents such as marine oil spills. Insurers that had sold this kind of insurance to industrial enterprises were desperate to avoid these new, difficult-to-assess liabilities and, starting in the 1970s, they attempted to eliminate coverage for future *gradual* pollution by inserting exclusions into their general liabilities policies. Going forward they only offered new coverage for contamination losses related to explosions and the like (Abraham, 1988; Horkovich et al., 2012).

Entrepreneurs, primarily based in London, filled the resulting gap in environmental liabilities insurance by offering insurance for environmental liabilities on a "claims made" basis. These insurance policies covered claims first made during the policy period, regardless of when the activities that produced those liabilities took place. Because claims-made insurance is sold (and priced) closer in time to when insureds are held liable, insurers have greater confidence about the rules and proceedings that govern those liabilities. It soon became clear, however, that these first-generation specialty environmental liability insurers had grossly miscalculated. While the law governing environmental liabilities may have been reasonably well understood at the time insurers sold the policies, the location and extent of the hazardous waste deposits that gave rise to the liabilities were not. The specialty environmental liability insurers had sold policies with coverage that was too broad, based on underwriting that was too superficial, and at prices that were too low (Horkovich et al., 2012). At the same time, the traditional insurers learned that their new pollution exclusions were vulnerable in court: many US states held that the provisions did not unambiguously exclude liability for gradual pollution (Abraham, 1988). As a result, the insurers were made to pay for hazardous waste clean-up actions, not only under the legacy policies sold before they started using pollution exclusions, but also under policies that they had sold since then (Id.). This development risk was especially troubling for the traditional insurers, because the Superfund laws enacted in Congress in 1980 and separately in many states imposed retroactive, strict liability on companies that had produced or transported hazardous waste or owned property on which hazardous waste was located (Abraham, 1988).

The liability insurance crisis that occurred in the middle 1980s provided the insurance industry with the opportunity for a reset (Abraham, 1988; Baker, 2004). The general liability insurers stopped using their earlier, weak pollution exclusions and began using stronger exclusions that courts have enforced to bar coverage for environmental liabilities. The first-generation specialty environmental liability insurers went out of business and were replaced by new underwriters who learned from their mistakes. These second-generation specialty environmental liability insurers sold higher priced, narrower coverage with lower limits to forced buyers: businesses that transported, stored, or otherwise handled hazardous materials and, as a result, had a legal obligation to demonstrate their financial responsibility for liabilities that could arise out of their activities (Horkovich et al., 2012).

Meanwhile, local and state government officials realized that the strict hazardous waste liability rules prevented the redevelopment of former industrial sites. The existing law made every entity in the chain of ownership or occupancy of property—including the redevelopers—liable for the full extent of the clean-up costs. As a result, banks and other financial institutions were unwilling to lend the money needed to redevelop these "brownfields." The risk was too great that redevelopment would reveal additional contamination, or additional costs of cleaning up known contamination, making redevelopment non-viable.

The government's hazardous waste law thus became a pressing political problem. Despite experimentation by some second-generation environmental liability insurers, the market for site-specific insurance to cover excess clean-up costs failed to develop. Not only was it difficult to predict the clean-up costs, but complex legal actions would be needed to allocate financial responsibilities among the potentially responsible parties. Federal and state environmental protection agencies thus began exploring ways to revise hazardous waste liability law to facilitate (insurance for) brownfield redevelopment (U.S. House of Representatives, 2001).

This effort resulted in legislation in the early 2000s that provided substantial protection against liability for clean-up costs to "bona fide prospective purchasers" of contaminated sites. If purchasers demonstrate that they have taken appropriate steps to (attempt to) contain the contamination at the site, they can obtain formal assurances from the environmental agencies that limit their liability (U.S. Environmental Protection Agency, 2021). The availability of these legal safe harbors facilitated the growth of a robust market for prospective liability insurance for brownfield redevelopment (Foggan & Gridley, 2014; Horkovich et al., 2012).

Once again, government is deeply involved along all three dimensions. Government regulation shapes policyholder conduct and informs insurer underwriting. Government enforcement of environmental laws creates much of the liability that stimulates the demand for the insurance. Government enforcement also provides some assurance to the insurance market that companies will comply with modern strict standards and, therefore, be less likely to contaminate ground and water. Additionally, the government enforcement that creates a brownfield also creates a technical record that insurers can use in their underwriting for the prospective coverage. Finally, governments bear the tail risk. When the most recent owner of contaminated property becomes insolvent, property taxes are no longer paid, and the property comes under the control of local government. If the costs of cleaning up the site exceed what can be recovered from the potentially responsible parties, and if there are no uses for the site that can motivate investors to fund a cleanup, the property remains contaminated until government provides the funding through a state or federal cleanup program. The "safe harbor" legislation thus facilitates redevelopment of contaminated sites by protecting brownfield development businesses and, by extension, their insurers (including government), from tail risk. Accordingly, we classify the government involvement in the environmental liability insurance markets as high in the regulation dimension, high in the enforcement dimension and medium in the co-insurance dimension.

3.6. Public directors and officers liability insurance

Corporate and securities liability law protects the shareholders and creditors of publicly traded companies against mismanagement. It makes directors and officers personally liable for financial losses arising from their decisions with the aim of discouraging managerial fraud, theft, and noncompliance. However, managers become inefficiently risk-averse if they fear being sued and punished for honest mistakes and adverse circumstances beyond their control. Directors and Officers (D&O) insurance mitigates this problem by covering the companies' directors and officers for liabilities arising from legally insurable conduct in the course of their duties (Baker & Griffith, 2010).

The primary liability covered by public companies' D&O insurance—securities fraud—has wider scope than the name suggests. At least in the United States, "everything is securities fraud," in the immortal words of Bloomberg's Matt Levine (Strauss, 2022). Levine's point was that companies facing crises tend to avoid precipitating them by being less than forthcoming, or downright untruthful, in public statements to shareholders and the securities authorities. This often leads to securities fraud actions when the crisis erupts. Examples include Dieselgate, the Marsh bid-rigging scandal, the options backdating scandal, the opioid crisis, and even some cyber-attacks and data breaches.[7] As a result, securities fraud actions police the violation of corporate governance norms that go well beyond accounting rules.

Since at least the 1970s, public company securities and corporate liability actions have overwhelmingly been settled, not litigated to judgment (Alexander, 1991; Baker & Griffith, 2010). Public companies do not have the taste for lengthy lawsuits with unpredictable, potentially catastrophic outcomes, particularly when they bought insurance to protect from those lawsuits. This gave rise to two types of moral hazard problems that threatened to undermine the legitimacy of D&O insurance.

First, in the 1980s, there was a flurry of legal actions that settled for amounts within the limits of the D&O insurance—seemingly without regard to their merits (Alexander, 1991). This created a perception that D&O insurance encouraged third party moral hazard. In response, Congress enacted the Private Securities Litigation Reform Act (PSLRA) in the mid-1990s. The PSLRA increased courts' ability to eliminate non-meritorious lawsuits, with the goal of restoring the deterrent effect of securities fraud actions and stabilizing the D&O insurance market (Choi, 2007; Johnson et al., 2007).[8] While forcefully opposed by the trial bar (as evidenced by President Clinton's veto and Senator Metzenbaum's objection that the insurance companies were behind the legislation), the PSLRA arguably preserved the securities litigation "business" by restoring its legitimacy.[9]

Second, out-of-court settlements in liability actions prevent the judicial findings of fraud typically required for the fraud exclusions in the policies to apply. This aggravates insider moral hazard. D&O insurance pays the individual's defense costs, including for criminal prosecutions. Unless and until there is a finding of fraud in a civil action (which almost never occurs because cases settle), the insurer will pay the individual's civil liability, even if they were convicted of criminal fraud. To restore the intended deterrent effect of making directors and officers personally liable for willful damages, shareholders in a private action or a securities regulator in a public action began insisting on a personal payment as a condition of settling the action (Baker & Griffith, 2010).

As in the case of environmental liability, D&O insurers avoid tail risk by selling policies with limits that are far below the potential liability. While there is no explicit government co-insurance, there is implicit co-insurance. This can be seen most obviously in circumstances that motivate a government bailout, such as the Savings & Loan crisis in the United States and the 2008 financial crisis, but other forms of implicit government co-insurance are so routine that they can easily be missed (Moss, 2004). Limited liability protects shareholders from tail risk: the worst that can happen to shareholders is that the value of their shares goes to zero. Bankruptcy protects other constituents of the corporation from (some of the) tail risk. If the corporation has positive net worth without its current liabilities, the corporation can be reorganized to preserve the ongoing business under new ownership and pay the creditors as much or more than they would obtain in a liquidation. Like the brownfield redevelopment safe harbors observed in the environmental liability case study, limited liability and bankruptcy can thus be understood as a form of government co-insurance.

Government is even more deeply involved along the regulation and investment dimensions. Government regulation sets the standards that guide corporate conduct and provide the basis for insured liabilities. The government role in enforcement includes not only civil enforcement actions by securities regulators and criminal enforcement by prosecutors, but also the institutional framework for the extensive private enforcement that takes place through civil litigation. Accordingly, we classify government involvement in the D&O insurance market as high in the regulation dimension, high in the investment dimension, and, while not as high in the co-insurance dimension as in the environmental liability insurance market, nevertheless higher than the very low levels in the ordinary art and K&R insurance markets.

4. Analysis

Table 1 summarizes how we classify each of the six cases studies and the variations within them. We observe pervasive involvement of government in private insurance markets that extends well beyond the activities

TABLE 1 Government support for various insurance regimes

	Regulation	Investment	Co-insurance
Art theft			
Mid-market	Low	Low	Low
Trophy art	Medium	Medium	Medium
Terrorism			
Aviation	High	Medium	High
Commercial prop.	Medium	Medium	Medium
Kidnap & Hijack			
K&R	Low	Low	Low
Hijack for ransom	Medium	Medium	Low
Arctic shipping			
Lloyd's club	Low	Low	Low
Competitive	Medium	Medium	Medium
Environ. liability	High	High	Medium
D&O liability	Medium	Medium	Low/Medium

traditionally understood as insurance regulation, such as the solvency and market conduct regulation of insurance companies. We do not contend that governments always undertake these activities for the purpose of maintaining sustainable insurance markets, but insurers do engage with governments for that purpose. Put another way, our three-dimensional model describes how governments attempt to achieve a better balance of social risk and enterprise. Sometimes this occurs in conscious coordination with insurance markets, while other times this happens in ways that government actors do not explicitly connect to insurance markets. We note the diversity and the evolutionary nature of that involvement along the three governance dimensions we explored. Along the co-insurance dimension, governments can explicitly insure a share of the loss (most usefully the tail risk), as in the case of terrorism and high-end art theft. Alternatively, governments can implicitly insure the tail risk, either by bearing that risk themselves, as in the case of environmental harm, terrorist hostage taking, and the systemic consequences of corporate misconduct, or by protecting private actors from risk in other ways, as in the case of the brownfield safe harbors, limited shareholder liability, and bankruptcy reorganizations. Finally, governments can directly bear the risk by owning the entities facing the loss, as in the case of the Chinese arctic vessels that compete with private vessels.

Along the regulation dimension, information is key to good governance, public or private. Small insurance markets such as K&R and art loss have created private channels for information exchange. In highly competitive markets, however, insurers may withhold information. Mandating central data collection and making information publicly available can improve private decision making—as in the piracy and arctic case studies. In some cases, governments go further and develop regulatory standards, as illustrated in the arctic, environmental liability and D&O insurance case studies. In other cases, governments act indirectly by recognizing a legal duty of care that makes good practices mandatory because of the possibility of civil liability for breach of that duty, as illustrated in the K&R and piracy insurance case studies.

Governments can also act directly and indirectly along the public investment dimension. Governments can directly invest in loss reduction measures, as illustrated by the K&R, arctic shipping, piracy, and terrorism insurance case studies. Governments can invest directly in enforcement actions to enforce standards set through regulation, as illustrated by the environmental liability and D&O insurance case studies. Governments can invest indirectly by maintaining courts that allow private causes of action that enforce specific government standards as well as the more general duty of care. Other forms of government investment in risk reduction include infrastructure investment to discourage attackers from key targets (such as bollards, metal detectors, and barriers), the icebreakers and pilot boats in the arctic, and enhanced security in museums.

The liability insurance case studies introduced an important lever that governments can use across all three dimensions: liability rules and procedures. If recruiting the loss management capacity of the insurance market is one of the objectives of a liability regime, as has been suggested for certain cyber liabilities (Cooper &

Kobayashi, 2022), state actors may adjust the liability rules to better serve that function. Even if recruiting the loss management capacity of the insurance market plays no part in the initial formation of the liability regime, the interaction of that regime with the insurance market may nevertheless lead state actors to adjust the liability rules, as illustrated in the environmental liability and D&O case studies.

Liability rule adjustments can have consequences along all three dimensions. Along the regulation dimension, liability can be adjusted to change the rules or standards governing the insureds or third parties' conduct. The objective of tightening liability standards is to reduce the tail risk of the future. However, it can have the paradoxical effect of increasing insurers' losses in the short run because tighter standards may lead to more liability for past actions that are subject to the new, higher standards. Along the enforcement dimension, liability regimes can be adjusted to increase or decrease private threat reduction efforts. There can be government enforcement, with larger or smaller budgets and greater or lesser forbearance, or no government enforcement at all, other than that of the courts in adjudicating private enforcement actions. Private enforcement regimes can include bigger inducements to bring legal actions, with levers such as multiple damages, success-based fees for lawyers, and the ability to aggregate many small claims into one big action. Finally, along the co-insurance dimension, governments generally do not take on the tail risk of corporate liabilities explicitly, with workers compensation liability as a major exception. However, government may be a residual bearer of the underlying losses that the liability regime seeks to address, and governments create and maintain legal rules that protect private actors from tail risk. These legal rules can function as a kind of insurance, especially when government bears the tail risk (Moss, 2004).

In addition to highlighting the role of government, the case studies also illustrate the ability of private insurers to develop effective risk mitigation protocols and adapt them to changing threats. Insurers can be highly effective in setting standards for the insured in specialist insurance markets that are small enough to operate as clubs. However, club governance can fail when demand for insurance grows rapidly, and outsiders compete for market share by undercutting the club's conditions. Insurers also have created effective institutions to reduce the profitability of crime (Baker & Shortland, 2022b). However, when these protocols privilege the long-run interest of the club (and society) over the short-term interest of the insureds, they are vulnerable to outside competitors that seemingly offer a "better" deal. In some cases, insurers proved effective at sharing information. This is done at low cost in small clubs but requires more intricate design and perhaps public support for bigger groups. Finally, we note that several mature insurance markets were at one stage considered "uninsurable." In some cases, private solutions were found: especially in small markets, clubs formed to collect information, set standards and fight threats. Once new threats were understood and mitigated, private (re)insurance became available again. However, in major insurance markets there can be pressure for governments to intervene. That intervention can promote or inhibit the evolutionary process.

5. What future(s) for ransomware insurance?

Cyber-insurance has been available since the mid-1990s and was initially governed privately (Wolff, 2022), subject only to ordinary solvency and market conduct insurance regulation. K&R insurers at Lloyd's of London were among the first to insure against cyber extortion with governance efforts focused on containing the crime. Yet, US liability insurers developed a competing product for the US market that insured against cyber extortion as well as the liability risks that were prominent in the United States, but not in Europe (Baker & Shortland, 2022a).[10] Divergent legal regimes thus prevented the formation of a cohesive private governance regime for ransomware when the market was still small enough to facilitate a club-based solution. Demand has grown rapidly in recent years: the cyber insurance market grew from US$2.02bn in 2015, to US$7.01bn in 2020, with projections of more than US$20bn by 2025 (Globaldata, 2021). For comparison, the gross annual premium in K&R insurance is in the region of US$ 250–300 mn per annum (Spross, 2019) and environmental liability insurance stood at US$ 1.51bn in 2019 (Insurance Newsnet, 2021). Intense competition has prevented the formation of an industry consensus on minimum underwriting standards. Recent attacks on infrastructure (Colonial) and service providers (Kaseya) indicate that there are systemic risks and extreme loss scenarios, and the specter of non-insurability has been raised (Abraham & Schwarcz, 2021; Pal et al., 2021).

Escalating cybercrime and significant losses among cyber insurers in 2019 and 2020 have led some insurers to withdraw from or reduce their ransomware cover. A concurrent "hard market" for insurance provides both the

incentive and the opportunity for product innovation. Insurers that remain in the market are undertaking drastic remedial action: reducing available limits, increasing prices, and demanding better cyber-hygiene from their customers (Smith, 2021). These dynamics are further re-enforced by reduced availability of reinsurance (Shi, 2021), which exacerbates the capacity constraint fueling the hard market (Baker, 2004). Current market conditions thus expedite an essential process of product innovation (Ransomware Task Force, 2021 at 60). At the same time, calls for government action have already led to intervention along all the three governance dimensions. To consider the potential futures for cybercrime risks it is, therefore, helpful to consider the present role of government in the United States and United Kingdom across our three dimensions.

Coinsurance: There is explicit government coinsurance in the United States and United Kingdom only for extreme tail events that would qualify as terrorism, but governments implicitly bear tail risk from ransomware attacks with systemic consequences (Abraham & Schwarcz, 2021).

Regulation: There is a wide variety of existing cybersecurity regulation and certification. For example, there are emerging industry-specific legal standards such as the financial services industry standards adopted by the New York State Department of Financial Services.[11] The National Institute of Standards and Technology of the US Department of Commerce has developed a voluntary framework for reducing cyber risks to critical infrastructure that could become a de facto legal standard through the operation of fiduciary and other legal duties of care.[12] The Federal Trade Commission (FTC) has become the de facto authority on consumer data protection with formidable enforcement powers against companies disregarding its basic data security advice (McGeveran, 2019). Finally, existing regulations at national or state level address data privacy standards and requirements that are implicated in some cybercrime events (Wolff, 2022).

Public investment: While we cannot comprehensively describe what governments are doing to reduce the risk of cybercrime, we observe government-funded R&D to help harden targets against criminal attacks, such as the US Federal Cybersecurity Research and Development Strategic Plan. Some governments use law enforcement and the military to disrupt cybercrime (Lyngaas, 2021). They use civil enforcement actions to enforce regulatory standards. They authorize private enforcement, and maintain the courts that enable private enforcement actions. Governments also runs cybersecurity education campaigns and provide resources for their implementation.

Yet in 2020/2021 industry insiders identified a need for significant further government involvement along all three dimensions. For example, the Ransomware Task force (2021) recommended a range of urgent policy priorities. On the regulation dimension, there was a call for using regulation to improve cyber-hygiene, forcing the adoption of minimum standards, and making reporting of ransom payments mandatory. On the coinsurance dimension, there were demands to support companies that resolve incidents without paying ransoms and provide a financial backstop for extreme losses (the Cyber Response and Recovery fund). There were multiple proposals to improve state enforcement, such as (1) ending the impunity of cybercriminals in safe-haven states using diplomacy and military intelligence; (2) deterring extortive cybercrime by making ransomware an investigative and prosecution priority, and (3) disrupting ransom payments.

In the following sections, we draw on the analysis above to discuss how governments can achieve a better balance of social risk and enterprise without stifling private sector innovation. We address the problems of first party moral hazard, third party moral hazard, and tail risks in turn.

5.1. First party moral hazard

Collective action and information problems have so far prevented insurers from developing common standards. Although a hard market and higher loss ratios have helped to focus efforts since 2020, the cyber-insurance market is large and still growing. Any club governance solution among primary insurers would likely collapse when the soft market returns. However, the reinsurance market is highly concentrated and essential to the functioning of the market. Although there is no evidence that this is happening yet, a combination of the top three or four reinsurers and Lloyd's could develop and enforce underwriting standards to improve self-protection of insureds. Given that reinsurers have "skin in the game" they have a clear incentive to identify efficient standards and risk reduction activities (Baker & Swedloff, 2013). Indeed, the leading cyber-insurance reinsurer, Munich Re, has argued that insurers can master ransomware, just as insurers have done "many times in other classes of business" (Sclafane, 2021).

Our case studies demonstrated that insurers find ingenious solutions to tricky governance problems when they can share data and discuss their experience in confidence. The creation of CyberAcuView demonstrates the desire of key cyber insurers to work together on data sharing, standards, coordination with law enforcement and systemic risks evaluation.[13] However, maneuvering for competitive advantage and anti-trust concerns have inhibited such coordination in the past (Miazad, 2021). Governments could therefore support opportunities for the industry to develop coordinated solutions. An important first step would be the mandatory disclosure of ransomware attacks and payments to give stakeholders an accurate picture of the threat landscape. The US legislation of March 2022, which requires entities providing critical infrastructure services to report attacks and ransoms is a step in the right direction.[14] If a more comprehensive reporting requirement fails to curb social risks, governments could disseminate emerging best practice by creating cybersecurity certifications at different levels. Companies would choose to obtain a suitable security standard (perhaps with compliance monitored by government agencies), and insurers could base their premia on the certified security level rather than monitoring customers directly.[15] Our analysis thus tallies with the Ransomware Task Force (2021) recommendation that states should primarily help to coordinate insurance industry collaboration.

5.2. Third party moral hazard(s)

We are less convinced that markets can handle the two types of third-party moral hazard we identify. The first emanates from criminals that specifically target the insured for ransom payments. If insurers pay generously and quickly, they may exacerbate cybersecurity problems (Logue & Shnidermann, 2022). Indeed, crisis responders struggle to drive down criminal profits. The high cost of business interruption creates an awkward mismatch between social and private interests. Unlike real-world kidnappings, where keeping hostages hidden and alive is a logistical challenge, the costs of delay to cyber-extortionists is minimal unless they exfiltrate and store many terabytes of data and, even then, the costs, risks, and complications of delay pale in comparison to that involved in keeping a high-profile hostage. This makes it difficult to keep ransoms low.

However, it is equally problematic to ban ransoms payments and ransomware insurance. Many attacks target critical infrastructure, such as health care, water, and energy. With lives and livelihoods at risk, a ransom ban lacks credibility. Governments would likely step in—and either pay the ransom or permit the victims to do so. Similarly, some managers might decide that they prefer paying an illegal ransom to bankruptcy. Legal businesses are not well placed to conduct transactions with the economic underworld. Without the know-how of experienced crisis responders, ransoms would likely escalate while fewer trades would succeed (Shortland & Keatinge, 2017). The overall effect of a ban is thus questionable: the crime would continue and become more damaging. Companies that fail after (unresolvable and uninsurable) ransomware incidents would likely lobby for bail-outs—that is, demand additional government insurance. To control this, governments would have to increase both regulation (to prevent incidents) and law enforcement against perpetrators and victims of crime. Policing the victims of crime for illegal ransom payments and noncompliance with regulations will strain public sector resources and trust in the government.

Governments could more usefully focus on pursuing the perpetrators of cybercrime. Efforts to indict and extradite cybercriminals and direct action against malware groups, such as those taken by the US military in response to the Colonial Pipeline incident, change the incentives of criminals (e.g., Lyngaas, 2021). Governments could also make ransom payments less secure for criminals by promoting research on de-anonymizing cryptocurrency transactions and taking other efforts to trace crypto payments, efforts we believe are already under way in the fight against money laundering.

Perhaps ironically, the second type of third-party moral hazard is facilitated by the privacy regulation that was enacted to protect individuals from criminal threats to privacy or data integrity. Cybercriminals have recently weaponized that regulation to achieve the opposite of what it was intended to achieve. They exfiltrate and threaten to publicly release data if the company does not pay a ransom (Greisiger, 2019; Verstraete & Zarsky, 2021). Moreover, because of the threat of civil liability for violating privacy regulation, companies are cloaking details of cybercrimes, their responses, and the conditions that created the opportunity for the crime under attorney client privilege and work product immunity. This inhibits government and other efforts to aggregate information about and learn from cyberattacks (Woods & Böhme, 2021).

These unintended consequences could be addressed, just as they were with environmental liability for brownfield redevelopment. Any reform requires deep reflection on the objectives of the data privacy regime. Do we still need punitive remedies to force companies to safeguard their customers' data when cybersecurity is already at or near the top of every board's priority list? Would it be enough for the private sector to bear only the *actual damage* caused to customers, suppliers, or others by data breaches? (And what, exactly, is that actual damage?) Increasingly sophisticated cybercrimes (such as the Kaseya attack) mean that even cautious and well-prepared companies may be breached. Can we tell the difference between bad luck and negligence in practice (Verstraete & Zarsky, 2021)? As the D&O case study showed, when class actions settle out of court, culpability can become irrelevant. It is hard to see the justification for punishing mere bad luck. Data breach legislation could also be amended to create a "safe harbor" from liability when a cyber-extortionist releases data in retaliation for a company's refusal to pay ransom, provided that the company notifies law enforcement of breach and cooperates with law enforcement in responding to the ransom demand.

5.3. Tail risks

There have been repeated calls for the creation of a public backstop for extreme tail risks, especially for state-sponsored cybercrime (Abraham & Schwarcz, 2021; Cunningham & Talesh, 2021; Government Accountability Office, 2022; Pal et al., 2021). At the same time, insurers are drafting new, tighter war-risk provisions for their cyber insurance policies that are designed to avoid coverage for state-sponsored activity (Carter & Enoizi, 2020; Lloyd's Market Association, 2021). Munich Re, the leading cyber reinsurer, advocates a backstop for state-sponsored activity (Sclafane, 2021) and some in the US insurance industry are supporting a broader proposal under consideration in the US Congress. Notably, there is not yet a consensus on the need for a backstop, as indicated by the Ransomware Taskforce leaving this reform off their list. We noted in the Pool Re example in the United Kingdom and the TRIA example in the United States that explicit government guarantees inhibited innovation in the immature and rapidly growing terrorism insurance market.

The current arrangement is effectively an implicit backstop (the criteria for intervention due to terrorist or state-sponsored activity being suitably vague). This leaves significant opportunity for private sector innovation and buys time for (re-) insurers to learn about the scale of the risk and how much of this the market can handle. Unless cyber insurers implement the new state-sponsored activity exclusions or abandon significant parts of the market, there is quite unlikely to be a strong push for an explicit public backstop. Until this time a "wait and see" attitude with an implicit backstop appears to be a viable policy stance.

6. Conclusion

In this paper, we have described and then applied a new framework for analyzing the role of government in maintaining private insurance markets. This framework highlights government activities that go well beyond the tools of traditional insurance regulation. While not all those broader government activities may be undertaken for the purpose of maintaining insurance markets, they nevertheless serve that function. Moreover, government activity that began for reasons that had little or nothing to do with insurance markets can be adapted or fine-tuned for that purpose, as we saw in the case of the amendments to US environmental laws that created the safe harbor component of the brownfield redevelopment program.

Because governments are so involved in so many ways in maintaining insurance markets, it seems inevitable that private insurance organizations will engage with governments to guide them in that process. Some of those efforts likely will involve attempts to obtain inefficient or unjust benefits for insurers, but that is not necessarily the case. Well-functioning private insurance markets provide substantial benefits to the people and organizations that depend on the risk transfer and spreading the markets provide. Thus, collective efforts by insurers to prod governments into acting along our three dimensions can plausibly claim to be serving the public interest. In that regard insurance organizations can be understood to be petitioning the government on behalf of their insureds. That petitioning represents a new aspect of insurance as governance to be added to the aspects described previously in the literature.

Whatever the future holds for insurance against ransomware attacks, we are confident that it will be a public-private partnership. We expect the cyber insurance market to continue its path of evolutionary competition, constantly adapting its protocols to changing threats, opportunities, and prohibitions. Governments will steer this process through co-insurance, regulation, and/or public investment. Our case studies of public-private governance in tricky insurance markets show that designing interventions is not a one-shot game but a slow and often clunky process of trial and error.

In times of a perceived crisis, insurance may be in short supply making it politically tempting for governments to provide explicit co-insurance. Yet, our analysis suggests that hard markets are crucial for weeding out poor underwriting and developing better practices. If hard markets are reframed as opportunities for evolutionary competition and institution-building, it will be easier to resist urgent calls for government backstops. If coinsurance is vital in the short-term, ad-hoc and informal arrangements avoid creating dependencies and inhibiting subsequent innovation.

When governments consider implementing new regulations on ransomware, they should be mindful that any industry consensus on best practice is a momentary snapshot subject to constant review (Anderson & Fuloria, 2009). Best practice enshrined in law runs risks becoming outdated, ineffective, or even counterproductive. Sometimes legislation turns out to be too strict, choking off desirable economic activity (such as brownfield development). Some regulation and enforcement can be evaded by moving activities elsewhere or by sidestepping formal governance in the name of efficiency (such as corporate and securities liability). Laws can also be abused by criminals to increase their own profits (data privacy and the ban on ransom payments to terrorists). We would therefore recommend that governments routinely examine whether legislation truly serves the public interest. As discussed above, we are concerned about the punitive nature of at least some aspects of privacy law. Governments could also do more to help the private sector to develop timely solutions, by collecting and sharing information about ransomware attacks.

Finally, criminals respond to incentives: namely the profitability of crime, the probability of being caught and convicted, and the severity of sanctions. Stakeholders will eventually develop protocols to reduce the success rate and profitability of ransomware. However, to decisively turn the tide on this aspect of cybercrime we likely need more public law enforcement. Only governments can end the impunity of cybercriminals sheltering in foreign jurisdictions.

Acknowledgments

We thank conference and seminar participants at the Haifa and HUJI Cyber Conference (December 2021), the Penn Carey Law School (November 2021), and the British Insurance Law Association (November 2021). We are grateful to Josephine Wolff, Dan Schwarcz, Daniel Woods, and Tal Zarsky and five anonymous referees for comments on an earlier draft of the paper.

DATA AVAILABILITY STATEMENT

Our research is qualitative in nature. The data that support the findings of this study are referenced in the text.

Endnotes

[1] There are also completely private markets for setting and certifying standards in which multiple companies or organizations compete, see, for example, the "grades," "levels," or "belts" certifying achievements in music, drama, or sports.

[2] See website at https://www.ukfinance.org.uk/dedicated-card-and-payment-crime-unit.

[3] Initially on behalf of the insurer, who then offers the recovered object back to the former owner in return for the insured sum.

[4] PoolRe website at https://www.poolre.co.uk/reinsurance/.

[5] See, for example, BMP 5 available on the EUNavFor website https://eunavfor.eu/mission.

[6] Website for ASTD available here: https://www.pame.is/projects/arctic-marine-shipping/astd.

[7] Examples of securities class actions based on these and other corporate disasters can be found through the Stanford Securities Litigation Analytics database and Kevin LaCroix's D&O Diary blog.

[8] Hearings Before the Subcommittee on Telecommunications and Finance of the Committee on Energy and Commers House of Representative, 103rd Congress 2nd Session (July 22, 1994) at 67 (statement by Rep. Tauzin).

[9] Id at p. 28 (statement by Senator Metzenbaum).

[10] Data protection regulation across the EU was tightened only in 2018.

[11] See DFS website at https://www.dfs.ny.gov/industry_guidance/cybersecurity.

[12] See NIST website at https://www.nist.gov/cyberframework.

[13] See website at https://cyberacuview.com.

[14] See website at https://www.cisa.gov/circia.

[15] Anderson and Fuloria (2009) caution that certification may create a false sense of security.

References

Abraham, K. S., & Schwarcz, D. (2021). Courting disaster: The underappreciated risk of cyber-insurance catastrophe. *Connecticut Insurance Law Journal*, 27, 407–473.

Abraham, K. S., & Schwarcz, D. (2023). The limits of regulation by insurance. *Indiana Law Journal*, 98 forthcoming. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4119812

Abraham, K. S. (1988). Environmental liability and the limits of insurance. *Columbia Law Review*, 88, 942–988.

Alexander, J. C. (1991). Do the merits matter? A study of settlement in securities class actions. *Stanford Law Review*, 43, 497–598.

Anderson, R., & Fuloria, S. (2009). Certification and evaluation: A security economics perspective. In *Proceedings of the 14th IEEE international conference on emerging technologies & factory automation (ETFA'09)* (pp. 1156–1162). IEEE Press.

Arctic Portal. (2016). How the Insurance industry contributed to the Polar Code. https://arcticportal.org/ap-library/news/1813-how-the-insurance-industry-contributed-to-the-polar-code

Baker, T. (2002). Liability and insurance after September 11th: Embracing risk meets the precautionary principle. Geneva Papers on Risk & Insurance.

Baker, T. (2004). Insuring liability risks. *Geneva Papers on Risk and Insurance*, 29, 128–149.

Baker, T. (2010). Insurance in sociolegal research. *Annual Review of Law and Social Science*, 6(1), 433–447.

Baker, T. (2021). Uncertainty > risk: Lessons for legal thought from the insurance runoff market. *Boston College Law Review*, 62(1), 58–108.

Baker, T., & Griffith, S. (2010). *Ensuring corporate misconduct: How liability insurance undermines shareholder litigation*. University of Chicago Press.

Baker, T., & Shortland, A. (2022a). Insurance and enterprise: Cyber-insurance for ransomware, forthcoming in Geneva Papers on Risk and Insurance.

Baker, T., & Shortland, A. (2022b). Binary stars: How crime shapes insurance and insurance shapes crime (working paper).

Baker, T., & Swedloff, R. (2013). Regulation by liability insurance: From auto to lawyers professional liability. *UCLA Law Review*, 60, 1412–1450.

Beaman, C., Barkworth, A., Akande, T. A., Hakak, S., & Khurram Khan, M. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, 111, 102490.

Ben-Shahar, O., & Logue, K. D. (2012). Outsourcing regulation: How insurance reduces moral Hazard. *Michigan Law Review*, 197, 197–248.

Bice, W. B. (1994). British government reinsurance and acts of terrorism: The problems of Pool Re. *University of Pennsylvania Journal of International Business Law*, 15, 441–468.

Burbank, S., Farhang, S., & Kritzer, H. (2013). Private enforcement. *Lewis & Clark Law Review*, 17, 637–722.

Carter, R. A., & Enoizi, J. (2020). Cyber war and terrorism: Towards a common language to promote insurability. Geneva Association Report. https://www.genevaassociation.org/research-topics/cyber/CTCW-common-language

Choi, S. J. (2007). Do the merits matter *less* after the private securities litigation reform act? *The Journal of Law, Economics, and Organization*, 23, 598–626.

Cooper, J. C., & Kobayashi, B. H. (2022). Unreasonable: A strict liability solution to the FTC's data security problem. *Michigan Technology Law Review*, 28, 257–304.

Coveware. (2021). Ransomware attack vectors shift as new software vulnerability exploits abound. https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

Cunningham, H. B., & Talesh, S. A. (2021). Uncle Sam RE: Improving cyber hygiene and increasing confidence in the cyber insurance ecosystem via government backstopping. *Connecticut Insurance Law Journal*, 28, 1–84.

Dudley, R. (2019). The extortion economy: How insurance companies are fueling a rise in ransomware attacks. https://www.propublica.org/article/the-extortion-economy-howinsurance-companies-are-fueling-a-rise-in-ransomware-attacks

ECB. (2007). Financial Stability Review December 2007 European Central Bank. https://www.ecb.europa.eu/pub/pdf/fsr/financialstabilityreview200712en.pdf

Ericson, R. V., Doyle, A., & Barry, S. (2003). *Insurance as governance*. University of Toronto Press.

Ewald, F. (1991). Insurance and risk. In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault effect: Studies in governmentality* (pp. 197–210). The University of Chicago Press.
Foggan, L. A., & Gridley, M. J. (2014). Issues in coverage for preexisting pollution conditions under pollution liability insurance policies. *Environmental Claims Law Journal*, 26(2), 91–106.
GlobalData. (2021). Cyberinsurance industry to exceed 20bn by 2025. https://www.globaldata.com/cyber-insurance-industry-exceed-20bn-2025-says-globaldata/
Government Accountability Office. (2022). Cyber insurance: Action needed to assess potential federal response to catastrophic attacks. GAO-22-104256.
Greisiger, D. (2019). 5 Ransomware facts you need to know about. https://riskandinsurance.com/5-ransomware-facts-you-need-to-know-about/
Gautier, D. L., Bird, K. J., Charpentier, R. R., et al. (2009). Assessment of undiscovered oil and gas in the arctic. Science, 324, 1175–1179.
Heimer, C. (1985). *Reactive risk and rational action: Managing moral hazard in insurance contracts*. University of California Press.
Herr, T. (2021). Cyber insurance and private governance: The enforcement power of markets. *Regulation and Governance*, 15, 98–114.
Horkovich, R. M., Hertzog, R. F., & Halprin, P. (2012). Site pollution liability insurance. In D. L. Guevera & F. J. Deveau (Eds.), *Environmental liability and insurance recovery* (pp. 499–533). American Bar Association.
Humpert, M. (2019). Chinese Shipping Company COSCO to send record number of ships through arctic. High North News 13 June. https://www.highnorthnews.com/en/chinese-shipping-company-cosco-send-record-number-ships-through-arctic
Insurance Newsnet. (2021). Environmental Liability Insurance market to see huge growth by 2026. https://insurancenewsnet.com/oarticle/environmental-liability-insurance-market-to-see-huge-growth-by-2026-allianz-axa-zurich
International Chamber of Shipping. (2019). Guidelines for the development of a polar water operation manual. https://www.ocimf.org/document-libary/53-guidelines-for-the-development-of-a-pwom/file
Jaffee, D. (2005). The role of government in the coverage of terrorism risks, chapter 8 in OECD 2005. *Terrorism Risk Insurance in OECD Countries*, 189–230. OECD. https://www.oecd-ilibrary.org/finance-and-investment/terrorism-risk-insurance-in-oecd-countries_9789264008748-en
Jaffee, D., & Russell, T. (2007). Terrorism insurance: Rethinking the government's role. *Issues in Legal Scholarship*, 6(2), 1096.
Johnson, M., Nelson, K. K., & Pritchard, A. C. (2007). Do the merits matter more? The impact of the private securities litigation reform *act*. *The Journal of Law, Economics, and Organization*, 23, 627–652.
Kay, B. (2021). The destructive rise of ransomware-as-a-service. Forbes. https://www.forbes.com/sites/servicenow/2021/06/09/the-destructive-rise-of-ransomware-as-a-service/?sh=3ad168561e16
Klerman, D., & Shortland, A. (2022). The transformation of the art market: Law, norms, and institutions. *Theoretical Inquiries in Law*, 23(1), 219–241.
Kuhnreuter, H. (2019). Testimony of Howard Kunreuther before the Committee on Banking, Housing, and Urban Affairs. https://www.banking.senate.gov/imo/media/doc/Kunreuther%20Testimony%206-18-19.pdf
Lloyd's Market Association. (2021). Cyber war and cyber operation exclusion clauses. Lloyd's Market Association Bulletin, LMA21-042-PD.
Logue, K., & Shnidermann, A. (2022). The case for banning (and mandating) ransomware insurance. *Connecticut Insurance Law Journal*, 28(1), 247–316.
Lubin, A. (2021a). Public policy and the insurability of cyber risk. *Journal of Law and Technology at Texas*, 5, 45–110.
Lubin, A. (2021b). Cyber Security Insurance: Is regulation the answer? Event transcript from 18 March 20021. https://henryjacksonsociety.org/members-content/cyber-security-regulation/
Lusthaus, J. (2018). *Industry of anonymity*. Harvard University Press.
Lyngaas, S. (2021). US military hacking unit publicly acknowledges taking offensive action. CNN. https://edition.cnn.com/2021/12/05/politics/us-cyber-command-disrupt-ransomware-operations/index.html
McGeveran, W. (2019). The duty of data security. *Minnesota Law Review*, 103, 1135–1208.
Miazad, A. (2021). Prosocial antitrust. *Hastings Law Journal*, 73(6), 1555–1616.
Moe, A. (2020). A new Russian policy for the Northern Sea route? State interests, key stakeholders and economic opportunities in changing times. *The Polar Journal*, 10(2), 209–227.
Moss, D. (2004). *When all else fails: Government as the ultimate risk manager*. Harvard University Press.
Nairne, S. (2012). *Art theft: And the case of the stolen turners*. Reaktion Books.
O'Malley, P. (1991). Legal networks and domestic security. *Studies in Law, Policy and Society*, 11, 171–190.
Ostrom, E. (2010). Beyond markets and states: Polycentric governance of complex economic systems. *American Economic Review*, 100(3), 641–672.
Pal, R., Huang, Z., Lototsky, S., Yin, X., et al. (2021). Will catastrophic cyber-risk aggregation thrive in the IoT age? A cautionary economics tale for (Re-)insurers and likes. *ACM Transactions on Management Information Systems*, 12(2), 1–36.
Parchomovsky, G., & Siegelman, P. (2022). Third party moral Hazard. *The Journal of Legal Studies*, 51, 93–131.
Ransomware Task Force. (2021). Combating ransomware: A comprehensive framework for action: Key recommendations from the Ransomware Task Force. https://securityandtechnology.org/ransomwaretaskforce/report/
Sarrabezoles, A., Lasserre, F., & Hagouagn'rin, Z. (2014). Arctic shipping insurance: Towards a harmonisation of practices and costs? *Polar Record*, 52(4), 393–398.
Saul, J. (2020). Insurers face liability uncertainties as ships begin to sail through Arctic waters. *Insurance Journal*.
Schwarcz, D. (2015). A critical take on group regulation of insurers in the United States. *University of California Irvine Law Review*, 5, 537–558.

Sclafane, S. (2021). Writing cyber is key to survival, munich re exec says. Carrier Management. https://www.carriermanagement.com/news/2021/09/13/226172.htm
Shi, C. (2021). Cyber in a truly hard market as rates soar. Insurance Insider 17 August. https://www.insuranceinsider.com/article/28xl8hbxqzbirkz1dthq8/cyber-in-a-truly-hard-market-as-rates-accelerate-and-capacity-contracts?utm_source=daily&utm_medium=email+editorial&utm_term=ii_insider_morning_briefing_daily&utm_content=Link342&utm_campaign=ID+Opinion+17+August+2021
Shortland, A. (2017). Governing kidnap for ransom: Lloyd's as a "private regime". *Governance*, 30(2), 283–299.
Shortland, A. (2019). *Kidnap: Inside the ransom business*. OUP.
Shortland, A. (2021). *Lost art: The art loss register's case book* (Vol. 1). Unicorn.
Shortland, A., & Keatinge, T. (2017). Closing the gap: Assessing responses to terrorist-related kidnap-for-ransom. RUSI Occasional Paper.
Smith, I. (2021). Cyber insurers recoil as ransomware attacks 'skyrocket'. *Financial Times*.
Spross, J. (2019). The Weird World of Kidnapping Insurance. The Week June 7. https://theweek.com/articles/840360/weird-world-kidnapping-insurance
Strauss, E. (2022). Is everything securities fraud? *UC Irvine Law Review*, 12(4), 1331–1383. https://doi.org/10.2139/ssrn.3664132
Stringham, E. (2015). *Private governance: Creating order in economic and social life*. Oxford University Press.
Talesh, S., & Cunningham, B. (2021). The technologization of insurance: An empirical analysis of big data and artificial intelligence's impact on cybersecurity and privacy. *UTAH Law Review*, 5, 967–1027.
United States Environmental Protection Agency. (2021). Summary of the Small Business Liability Relief and Brownfields Revitalization Act. https://www.epa.gov/brownfields/summary-small-business-liability-relief-and-brownfields-revitalization-act
United States House of Representatives, Committee on Energy and Commerce, Subcommittee on Environment and Hazardous Materials. (2001). Brownfields Legislation: The Brownfields Revitalization and Environmental Restoration Act of 2001, and Gillmor Discussion Draft, and Democratic Discussion Draft. Serial No. 107-43.
US Congress. (2002). Terrorism Risk Insurance Act of 2002. https://www.treasury.gov/resource-center/fin-mkts/documents/hr3210.pdf
Verstraete, M., & Zarsky, T. (2021). Optimizing breach notification. *University of Illinois Law Review*, 2021, 803–864.
Wolff, J. (2022). *Cyber-insurance policy: Rethinking international risk for the internet age*. MIT Press.
Woods, D., & Böhme, R. (2021). Incident response as a lawyers' service. *IEEE Security & Privacy*, 20(2), 68–74.
World Bank. (2013). *The pirates of Somalia: Ending the threat, rebuilding a nation*. IBRD.
Zurich Magazine. (2020). The original firefighters: How insurers protected London from fire. https://www.zurich.com/en/media/magazine/2020/the-original-firefighters-how-insurers-protected-london-from-fire

