Regulation & Governance

Regulation & Governance (2021) 15, 98–114 doi:10.1111/rego.12266

Cyber insurance and private governance: The enforcement power of markets

Trey Herr

Visiting Fellow at the Hoover Institution at Stanford University, Stanford, California, USA

Abstract

In the last half decade, cyber insurance has emerged as a multi-billion-dollar industry with the authority to set and enforce standards of security behavior. Although cybersecurity has become a concern of national policymakers, insurers appear to have supplanted the state to play an influential role in governing some aspects of client behavior. This paper explores private governance by cyber insurance firms and evaluates two competing explanations for its emergence – either that the private sector advanced to set and enforce cybersecurity standards for financial gain, or that the state retreated from its responsibility to regulate and private sector actors filled the gap only as necessary. To find an answer between these explanations, this article develops a single outcome case study of the American cyber insurance industry. Following a theoretical introduction to private governance and its manifestation through insurance, the article examines the insurance process and its application in cybersecurity, the key role of standards, and the mechanism of enforcing those standards. The article concludes by identifying key elements of this market-based enforcement and discussing implications for crafting effective private governance in other domains and public policy.

Keywords: cyber insurance, cybersecurity, free market, governance, risk.

1. Introduction

In 2013, Target experienced a massive cybersecurity breach. After infecting registers in stores around the country, malicious software spent the holiday shopping season silently vacuuming up credit card information from millions of customers. Attackers deployed this malware by infiltrating Target's networks through a third party vendor, a company that administered environmental controls at the retail giant's outlets in the Midwest (Kreb 2014). The breach was a national event as banks worked to replace millions of credit cards while Target's senior leadership were hauled before Congress. In the years since the breach was first made public, Target has accounted for more than US$250 million in losses related to this huge theft of customer data (Newman 2016). However, more than US$90 million of Target's losses were offset by insurance policies, designed to cover the costs of notifying consumers of a breach and responding to the ensuing litigation. This was one of the first, but not the last, instances of a large cyber insurance payout and it highlighted a trend that has been ongoing for more than a decade: the emergence of cyber insurance.

The insurance industry offers customers the opportunity to transfer risk that might be financially overwhelming in the event of a catastrophe. Since AIG wrote the first cyber insurance policy in 1997, insurers have offered companies a means to protect themselves from the financial liability associated with cybersecurity incidents (Brown 2014). Over time, insurers have come to require security standards in line with conventional best practices, offered recommendations on useful security software, and even partnered with cybersecurity vendors. AIG, for example, now works with cybersecurity vendors CrowdStrike and Darktrace to make risk assessments of some potential clients (Business Wire Staff 2017). Other research has found the same: "Insurance industry officials repeatedly refer to themselves as in a partnership with their policyholders and indicate that the strength of cyber insurance is the assortment of risk management services to which the insured gains access…" (Talesh 2018, p. 428).

Correspondence: Trey Herr, 2480 16th Street NW, Apartment 525, Washington DC, 20009 USA. Email: treyherr@stanford.edu

Accepted for publication 26 May 2019.

After relatively slow growth through the 1990s and 2000s, the size of the cyber insurance industry spiked upwards in 2012, from less than US$1 billion to more than US$2 billion in total premiums (as measured by the Betterley Report – an annual survey of the cybersecurity insurance market). The massive growth in this market provided new customers for existing insurers and brought new insurers into the market (Aon Inpoint 2017, p. 5; Romanosky *et al.* 2017, p. 3). Using security standards to assess and manage the risk of their customers, insurers filled a governance role for clients (Talesh 2018, pp. 428–432). This role grew as the demand for insurance rose alongside companies' insistence that business partners receive coverage (Advisen Ltd. 2014, p. 4; Beazley Breach Response 2016). This emphasis on security standards to reduce the risk of a breach came alongside a steady stream of new and ever riskier coverage offerings as insurers offered new types of coverage and higher limits (Betterley 2015, p. 7–11; Marsh Management Research 2015 pp. 2–3). This growth in the cyber insurance industry has taken place without a substantial corpus of incident data on which to build strong actuarial models for cyber events – a situation that has historical precedent for the early stages of an insurance market (Porter 1995, pp. 106–113; Clark 1999).

The implementation and enforcement of these security standards is an example of private governance, albeit an unusual one. Rather than any direct state intervention or an extended process of historical legitimation by the insurers themselves, the authority of cyber insurers appears to have been derived from the marketplace their clients take part in. Insurers enforcement power is reinforced as companies and other third parties demand each other carry insurance as a requirement for doing business (Advisen Ltd. 2014). The growth in this standard-setting role is ongoing but proves a theoretically interesting question of private governance and a substantively interesting domain of cybersecurity standards enforcement (Romanosky *et al.* 2017).

The remainder of this article proceeds through four sections. Section 2 looks at the theory of private governance and insurance as an example to frame this study. Section 3 provides an explanation of how cyber insurance works, the role of standards in insurance, and delves into what aspects of insurance resemble more classical governance processes. Section 4 traces the development of cyber insurance and evaluates it against the state retreat and private advance arguments, focusing on the role of the marketplace in enforcement to understand how cyber insurance became a form of private governance. This section highlights the importance of the supply chain relationships of insurance customers through a short comparison case of logging governance in North America. Section 5 concludes and highlights implications of this work for the academic and policy communities.

2. Private governance

Governance is characterized by the "decisions issued by one actor that a second is expected to obey," and acts as the sum of rules and standards of behavior that groups employ to manage each other's affairs (Kahler & Lake 2004, pp. 7–8). These standards can be informal holiday traditions passed on from one generation to the next, or highly structured and derived from clear authority, such as the tax code. Governance captures the ordering of political and economic affairs and can be conceptualized as a means to "maintain public order and facilitate collective action" (Stoker 1998, p. 17). This ordering takes place through two key processes – the setting and enforcement of standards.

Private governance represents the provision of these rules and standards, as well as their enforcement, by non-state actors with power derived from non-public sources. Work in private governance initially focused on how (rather than if) non-state actors mattered and what interactions were possible in areas where the state was weak or relatively uninvolved in standard setting and enforcement (Arts *et al.* 2001; Büthe 2004; Börzel & Risse 2005). This body of research has moved beyond discussing self-governance and standard setting within individual firms or industry associations to encompass fully developed regimes of rule setting and enforcement between firms (Knill & Lehmkuhl 2004; Fuchs 2005). This includes diverse examples like the use of formal production certifications in lumber supply chains and the development of the internet's complex of technical protocols (Cashore 2002; Leiner *et al.* 2009).

Basic rules and standards are required for efficient markets, and their provision by private actors can act either to replace state rules or to supplement them when these regulations fall short. Not merely subject to rules, firms often shape and set them; these organizations control substantial resources in their technology, labor pool, and capital available to influence state and non-state behavior (Mattli & Büthe 2005a). This is especially common

in new domains of economic behavior where novel technology or the rapidity of change may challenge the state's ability to provide such rules (Cutler *et al.* 1999, p. 8; Spar 1999, p. 31).

Insurance is an example of this private governance, as it requires both setting and enforcing standards, as well as being subject to many of the same social and economic pressures as the state in regulating the behavior of other parties (Ericson *et al.* 2003).

Various threads of research have begun to examine insurance as a governance activity influencing the behavior of clients in domains of consumer safety and protection, including privacy and food safety (Ericson & Doyle 2004; Ben-Shahar & Logue 2012; Talesh 2018). While much of this work has stemmed from legal and sociological scholarship focused on insurance and its relationship to regulation, it speaks directly and with value to the political questions of how governance processes form, mature, and operate. Talesh puts it best: "by exploring how and why insurance impacts society, and why insurance companies wield considerable influence in society, insurance law scholars lay an excellent foundation for thinking about insurance and insurance institutions" (2015, p. 619).

A common framework for explaining the development of private governance is the supply and demand model, whereby changes in governance capacity are explained as a function of the demand for standards and their supply by some party, either private or public. Mattli and Büthe (2005a) use this approach to explain the success or failure of government attempts to establish public institutions, while Green (2013) leverages it to explain the emergence of a global regime for environmental standards as a means for firms to reduce transaction costs by codifying standards. There are shortcomings to the supply and demand approach for studying a topic like governance as it typically does not consider the character of institutions being created and presumes a single dimension of political behavior, which is difficult (Büthe 2010, p. 8). It is possible to overcome these issues but requires that analysts consider supply and demand, as well as the politics of their interaction and the resulting behavior of agents in the political system (Spruyt 2001). This added context yields a reasonable starting point to introduce the two potential explanations for the emergence of cyber insurance as a form of private governance, state retreat, and private advance.

2.1. State retreat versus private advance

This article attempts to arbitrate the debate over the emergence of cyber insurance as private governance as a product of private advance or state retreat. State retreat argues that private governance emerges in the absence of state action as a product of state neglect rather than the seizure of a commercial opportunity by private actors. This could be either dereliction by the state or its overt delegation of regulatory responsibility to private actors, potentially to avoid the cost of detailed standard setting and enforcement (Strange 1996; Epstein & O'Halloran 1999; Mattli & Büthe 2003). Where standards are the product of state retreat, they are likely to be limited in scope and develop more slowly as firms lack incentive to adopt them without strong regulation. State retreat is more likely in areas of particular regulatory complexity, such as with multijurisdictional challenges, emerging new technologies, or sophisticated financial products (Büthe & Mattli 2011, pp. 60–98; Farrell 2006; Mosley 2009; Warren 2010). Private actors with relevant specialized knowledge then have some incentive to step in and provide minimal governance in lieu of state action, a relatively cost-effective outcome for the state in terms of direct cost (Alt & Alesina 1998).

Arguments for private advance, by contrast, center on governance as a profitable enterprise where firms have an incentive to bear the cost of standard setting and enforcement as a means to capture material benefit from providing regulation (Lecraw 1984). These arguments point to the expanded number of groups involved with, and widening array of incentives offered for, private sector governance (Büthe 2010). This can drive firms to participate in industry associations or even take on the separate role of standard setting and enforcement bodies, as with insurance underwriters, which may establish an oligopolistic (and thus advantageous) position in the market (Cutler *et al.* 1999). In studies of similar emerging commercial domains, such as maritime transport and the consumer electronics industry, private firms exhibited a greater capacity than state bureaucracies to develop solutions to complex technological problems, driving growth in private governance (Lehmkuhl & Knill 1998; Cutler *et al.* 1999). Thus framed, the state retreat versus private advance debate serves as the basis for evaluating the emergence of cyber insurance as a form of private governance.

3. Cyber insurance

Cyber insurance has been touted to help identify and enforce effective security standards while simultaneously allowing firms to offload liability for major attacks, making it a popular option for firms to invest scarce security resources (Pal 2014; Marsh Management Research 2015; Morgus 2016). In some cases, insurance firms may be equipped to actively monitor their clients and warn of breaches if the standards and enforcement process they have put in place allow for it. For example, in 2014, Liberty Mutual detected attacks on a client's network and notified them in advance of a breach (Hickens 2014). Insurance works by transferring risks posed to a company's assets and business operations over to a third party (Thoyts 2010).

This process reflects the nature of risk being transferred as well as the character of the governance process, "Insurance is managerial … [it] manages risks on a technical basis and at a distance, for a population dispersed in time and space but bound together..." (Ericson *et al.* 2003, p. 48). Transferring risk entails shifting some portion of the financial liability for a cybersecurity incident from the victim to an insurer.

Insurance is a form of risk transfer, allowing companies to move the financial liability associated with a potential cyber security incident from their balance sheet to that of an intermediary firm. Insurance exists in myriad forms around society from health to automotive coverage, liability protection for toy manufacturers, to protection for the potential future value of an athlete. Insurers assemble customers into a risk pool, aiming to create a group whose collective contribution is greater than the cost of their probable payout for claims. This transfer of liability can relieve companies of the burden of a costly breach, leveraging the financial resources of a pool of clients to cover the consequences suffered by only one or two of the total.

Central to this process is the insurance firm, which is responsible for controlling membership in the risk pool, calculating equitable premiums, and ensuring the financial solvency necessary to respond to claims. Managing the total risk of the pool becomes an ongoing challenge, as the insurer can choose to set standards for members to mitigate their risk; add or drop clients to shift the firm's overall risk; or further transfer the risk through reinsurance, catastrophe bonds, or other financial vehicles. Underlying this decisionmaking process is an assessment of the risk of individual clients, as well as the risk associated with the insurer's total portfolio.

Together, the clients of a common set of insurance policies form a pool of risk. For insurance firms, selecting clients and determining the scope of their coverage requires understanding the nature of risk for each applying company. The goal of an insurance firm is to construct a pool of clients whose collective contribution is equal to or greater than the probable cost of payouts for claims. The mechanics of a risk pool function, in part, because no one party can be sure if they will need to submit a claim, but most will not, thereby providing financially viable coverage to the few claimants and an incentivizing profit to the insurer.

The fees associated with insurance, paid by each member of the pool according to their assessed risk, are premiums. These can be a flat fee common to all customers or an equitable rate based on the risk profile of each customer. Judging this risk in order to set the price of the premium requires assessing the frequency and severity of the potential losses for each claimant in a given year. This equitable rate calculation allows firms to adjust premiums based on the risk profile and the potential loss exposure associated with each individual customer – a more computationally intensive but financially advantageous approach.

Particular risk is that which can be efficiently transferred and generally impacts only one or a small number of insured entities. Particular is distinct from correlated risk, in which all or a large portion of a population may be affected. Cybersecurity represents a mix of particular and correlated risk. Certain technologies are used by a wide variety of companies, like credit card and contactless payment systems or Adobe Reader for PDFs; these represent correlated risk. Correlated risk poses the same hazard to a large segment of an insurance firm's customer base, such that the variation in their individual vulnerability is less important than the nature of the catastrophe itself. Hurricanes and other substantially destructive natural events such as floods generally fall into this category. Particular risk varies with individual customers. How widely used technologies are employed; differences in how their risks are mitigated; and where those technologies depend on other, potentially more secure, devices can translate correlated risk into particular risk. Cybersecurity is thus a mix of particular and correlated risk, with much of the latter stemming from non-networked events, such as power failures or physical attacks (Maynard & Beecroft 2015).

Correlated risks are problematic for insurers because they are likely to reduce the member-to-claimant ratio of a risk pool past the point of financial solvency. Insurance firms may prefer to select customers with varying sources of particular risk to help diversify their portfolio, or they may prefer customers with relatively common sources in order to minimize the computational overhead associated with assessing and managing a substantially heterogeneous risk pool. Regardless of pool composition, however, customers should represent a tolerably low probability of loss; otherwise, they undermine the financial viability of any insurance product.

At a high level, insurers consider two broad factors in calculating the risk of loss by a potential client: the likelihood of an event and its probable severity (Thoyts 2010). For instance, using aggregated crash and accident data from American drivers over the last 50 years, insurers can attempt to forecast which clients, young or old, male or female, are more likely to be involved in an incident. This assessment approach is best suited to domains where the frequency of an event is determined largely by chance or forces beyond conscious design and there is a bevy of historical data. For cybersecurity, however, the likelihood of an event is determined by more than aggregated trends or underlying natural conditions. In addition to the vulnerability of an organization to the consequences of an event, risk assessment must consider the presence of active, adaptive adversaries. Criminals interested in credit card data, hacktivists intending mass disruption, or state intelligence agencies looking to destroy data each pose a different threat to insured entities.

There are two alternative approaches to risk assessment: consequence and threat focused. In a consequence-driven approach, the vulnerability is used to measure the exposure of a system or organization's assets to consequences like the detonation of a bomb or financial loss. This consequence-focused assessment is a more traditional risk management framework. The assessor determines the probability of a given threat, for example, a serious thunderstorm, and judges the potential impact of this threat on insured assets, for instance, a major company's data center. The result is an analysis concerned about the risk of damage to this data center from the thunderstorm rather than the likelihood of the storm's appearance. Risk management occurs where vulnerability to these high impact consequences can be reduced through operational or architectural changes, such as installing lightning rods or adding redundant power infrastructure. Controls are tied to managing these consequences rather than influencing the likelihood of the threat itself.

By contrast, in a threat-driven model, risk assessment analyzes a potential insured entity's vulnerability to different threats and controls are a means to reduce either this vulnerability or the likelihood of a threat event (Thomason *et al.* 2013). Threat-driven analysis focuses on differentiating risk based on exposure to a range of threat actors with varying intentions and capabilities. This could be used to adjust the scope or marketing of a company's product, for instance, downplaying features based on the likelihood they might invite disruptive hacktivist activity. Rather than manage consequences and reduce the change of catastrophe, a control focus is closer to reducing the probability of a harmful event at all.

The distinction between consequence and threat-based assessment is important in the context of cyber insurance. Consequence-driven assessment assumes a relatively static probability of a threat event, like a thunderstorm, taking place given a set of relevant variables, like geographic location and time of year. In this framing, controls become a tool to limit damage and reduce the likelihood of catastrophe rather than trying to prevent the threat. Better power backups for a data center are much more feasible than diverting the path of a thunderstorm.

Threat-driven assessments place great emphasis on the behavior of potential threats and their changing likelihood of harming insured assets. In this context, the focus is on changing threat behavior and blocking or reducing the likelihood of an event taking place. Security controls must change more often in line with adversaries evolving behavior and tactics. This fact places greater importance on standards and security controls that meet contemporary threats. Returning to the data center example for a moment, it may be that a criminal attempting to gain access to the facility first tried to steal corporate access badges from parked vehicles but has since shifted to impersonating an onsite vendor with forged identification. While physical security controls to guard parked cars may have caught these first attempts, without strong validation procedures for vendors, our criminal may find success. Controls must be managed to protect against adapting adversary behavior. The result is a greater emphasis on understanding which controls are most important or effective at any given time, leading to the demand for insurers' role as coordination service firms.

3.1. Players in the game: Insurance as coordination

Scholars recognize the varying form regulators can take depending on functional context and several have theorized governance relationships with more than two players (Kunreuther *et al.* 2002; Büthe 2010; Levi-Faur 2011; Verbruggen 2014; Walker 2014; Abbott *et al.* 2017). This article leverages Büthe's tripartite model of governance, which categorizes three actors: organizations on which standards are imposed, entities who call for standards, and the standard setters who provide this regulation (2010, p. 8). Each actor has a stake in the development and enforcement process with interests that may overlap but nevertheless are independent of each other. For firms in a marketplace, which could be both the requesters and targets of governance, these standards are a requirement for efficient market operation. This looks like a subset of Levi-Faur's third party governance, using a mix of private actors and what he calls "market oriented NGOs" (2011, p. 11).

The nature of insurers' governance power appears to be the critical role they play as coordination service firms, aggregating information and managing the risk of market interactions by "creating standardized cyber risk-management processes" (Odell *et al.* 2015) to reduce the risk posed to other market participants. Insurers offer an ability to reduce uncertainty, and thus the risk, of market transactions by setting security standards in use by one or both sides. The demand for insurance from the market turns this risk management power into an enforcement authority, as insurers set baseline security standards for their clients. While the insurers have a direct material interest in the fees (premiums) they charge for coverage, setting standards for their customers also provides indirect benefit by reducing the risk of a claim. Insurers evaluate the risk profile of clients using a set of criteria, which is communicated to firms and serves as parameters for behavior.

A prominent example of the coordination service firm is credit rating agencies, which view themselves as "quasi-regulatory institutions," and provide a good example of the emergence of private governance as a result of the prospect of financial gain (Sinclair in Cutler *et al.* 1999, p. 159). Rising to prominence out of the financial disintermediation of the 1970s and 1980s – when capital began to flow around, rather than primarily through, commercial banks – rating agencies provide market participants assessments on the risk of new financial issues and their offering firms. Rating agencies provide this information as trusted third parties and act to reduce uncertainty even though they are not backed by public institutions and claim not to persuade but only to offer judgment on the risk of new financial instruments and offering firms.

These ratings agencies create standards of behavior through the metrics used to assess risk, then enforced by the market of investors who respond to ratings by shifting their allocation of capital. The effect is to create a private governance mechanism that increases the efficiency of capital markets by translating uncertainty into more structured risk assessments. Credit rating agencies act as an "uncertainty-reduction device that allows transactions to go ahead without undue friction or costly [loss prevention]," the same goal of market efficiency that helps to explain the emergence of private governance (Sinclair in Cutler *et al.* 1999, p. 160).

Insurers can operate in a similar fashion to credit rating agencies, lowering the transaction costs stemming from cybersecurity risk by providing customers a means to select effective security controls, improve risk assessment practices, and limit potential financial uncertainty by shifting liability. The means to provide this certainty rests on the ability to enforce standards of best practice established to mitigate risk from adverse incidents. The source of those standards is an important determinant of whether insurance as private governance is a product of a retreating state or an advancing private sector.

3.2. Standards in cyber insurance

Standards serve as a structured language to evaluate the development of plans and acquisition of tools to provide security. More significantly, standards are used to mitigate the risk of an adverse event, providing a replicable set of practices, processes, and procedures. Developing security controls, and their integration into a risk assessment and management process, is a form of governance where standards are designed and enforced over organizations to shape their behavior.

Cybersecurity incidents are generally not rare events with massive costs (Romanosky 2016). Instead, they span a range of consequence and frequency values. Under a consequence-driven risk assessment, where vulnerability to particular forms of failure and costly outcomes might mean financial ruin, it can make sense for insurers to avoid customers capable of experiencing catastrophic or otherwise untenable loss. With a threat-driven process,

the challenge instead is to understand consequences as inevitable and structure a mix of clients according to the insurer's risk tolerance, similar to policies for weather events, health care, and automobiles. Moving up the value chain to reinsurers and other secondary markets, this assessment of the distribution of risk within a firm's insured portfolio and its aggregate value compared to revenue is a significant metric for assessing the financial health of the insurer's investments. The process of controlling these risks comes down to the security standards in place.

Another challenge is the issue of systemic risk, where a mix of different sources of risk cascade into each other, multiplying their impact and creating consequences far greater than could be born by a single insurer (Böhme & Schwartz 2010). A company that depends on the computerized logistics system of a port facility is thus linked in some fashion to this system's security. Taken at scale, with dependencies reaching across continents and industry verticals, this systemic risk may be uninsurable. Critical to the analysis of such a scenario, however, is assessing the realistic interdependency of systems that may be linked but are otherwise uninvolved. There are many internet-connected or internet-enabled services that could potentially communicate with each other – thus allowing the spread of contagion – but do not explicitly rely on each other's functions.

Returning to the port example, there is a difference between our notional company's dependence on the port's logistics system and its use of area Wi-Fi networks and automated cargo handlers. The logistics system may be critical, but wireless networks can be supplemented and cargo handled by human-operated equipment. A key mistake in considering systemic risk is assuming that all interconnected systems are equally vulnerable or similarly interdependent. Accurately assessing a potential chain of consequences is key to understanding where systemic risk threatens to be uninsurable. In this, the key is recognizing and limiting linkages between sources of risk rather than trying to mitigate one single high consequence event.

The content of standards in use by insurers varies, as there are multiple public and private schemes available. US public sector efforts to set standards can be broken into three clusters: critical infrastructure protection (CIP), regulation of protected industries, and federal information technology (IT). CIP has focused on a largely private-owned array of industrial functions and facilities, the loss of which would be acutely harmful or disruptive. These compromise the early history of standard setting, with the initial push beginning in 1996, and have long existed in a state of heightened importance (as a result of their "criticality").

The second cluster, protected industries, focuses on business areas in the US where customer information is deemed particularly sensitive, largely health care and finance. These industries have a history of receiving exceptional treatment by regulatory authorities and lawmakers. In health care, a prominent example of these regulations is the Healthcare Insurance Portability and Accountability Act (HIPAA) passed in 1996 which included a Security Rule requiring minimum security standards of medical facilities or entitles handling personal medical information. HIPAA was strengthened in 2009 with passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act, which specified the application of the Security Rule to business entities beyond hospitals. One recent example in finance is the Sarbanes–Oxley Act of 2002. While Sarbanes–Oxley included no specific cybersecurity provisions, it spurred a great deal of standard setting and certification within private groups to account for the increased requirement of information systems in processing and reporting data (Stults 2004).

The third cluster came through executive and legislative behavior targeting the federal government's own IT infrastructure. The tent pole regulation in this cluster is the Federal Information Security Management Act (FISMA), passed in 2002, which established security controls for public sector organizations and mandated a process of regular evaluation of both the controls application and their associated planning process. It was the first comprehensive law dealing with cybersecurity requirements across the US government and would come to be applied to contractors and companies that provided services to or received funding for government contracts (Deloitte 2013). Importantly, FISMA reaffirmed the National Institute of Standards and Technology (NIST) as the responsible agency for developing US government cybersecurity-specific standards, culminating in the development of the NIST SP 800-53 security controls, which are widely cited in and outside the public sector and form the basis of the NIST Cybersecurity Framework.

There has also been discussion about state attempts to directly support the cyber insurance market, largely focused on comparisons between cybersecurity and terrorism. Insurance products that cover loss related to terrorist activity face a somewhat similar problem to those that cover cybersecurity events. There is limited useful

historical data, and threat actors select targets based in part on their vulnerability to attack. Actions to mitigate risk in one part of a portfolio thus may increase risk elsewhere. There is also an information advantage for the state, whose intelligence or law enforcement arms may be cognizant of a threat but unable or unwilling to pass the information on to insurers and potential victims. Insurance for terrorism has grappled with these challenges repeatedly after major incidents, but the attacks on New York and DC in 2001 are particularly instructive (Kean 2011).

Initially after the attacks, coverage terms shrank and limits were imposed on catastrophic loss to deal with the uncertainty around the potential for new and even more destructive incidents. This limitation on risk transferred to the insurer by way of semantics is not unusual where uncertainty or substantial consequences are suddenly exposed (Ericson & Doyle 2004, pp. 37–39). By 2003, however, the insurance market began to adapt and expand products again to meet the demands of customers (Jaffee 2005). Much of this improvement can be traced to better catastrophe modeling techniques and the beginning of analysis of adversary groups' intentions and capabilities. Insurers understood that the range of potential consequences was determined, in part, by the types of attacks being launched and the capabilities of threat groups (Woo 2002). Existing methodologies offered a chance to forecast the behavior of threat organizations and suggest high and private slow probability targets, allowing more careful management of risk pools. There was also increasing preemption of the risk of a terrorist attack as insurers encouraged more prolific private security measures, and government law enforcement and intelligence agencies sought to reduce the capability of these groups and thus lower the probability of their action (Ericson & Doyle 2004, pp. 232–238).

This resurgence in the market was likely also the result of state intervention, which helped put a safety net under the market for primary and secondary insurance (also called reinsurance). The Terrorism Risk Insurance Act (TRIA), made the US government a reinsurer of last resort for firms, creating a financial entity that could help bear the burden of consequences from a catastrophic attack such as those in 2001 (Webel 2014). In cybersecurity, a similar law could provide a liability backstop for firms to encourage new policies, but it may also reinforce the belief that cybersecurity incidents are low probability, high consequence, and encourage the expectation that failure can be prevented, rather than made less frequent and more recoverable. A TRIA-like law for cybersecurity would also do nothing to directly impact the standards selection or risk assessment process. Identifying and enforcing these standards is critical to governance.

Private sector standards do not come with the weight of the law, but have been developed along multi-stakeholder and for-profit lines. These present a more limited range of coverage, without any attempt at enforcement, but more comprehensive detail. Private sector security standards tend to focus on business IT and the larger risk management process. In discussions with industry executives, two schemes take particular precedence: the International Organization for Standardization (ISO) 27000 series and Information Systems Audit and Control Association (ISACA) Control Objectives for Information and Related Technology (COBiT) (International Organization for Standardization 2014; Tuttle & Vandervelde 2007). The Payment Card Industry Data Security Standard (PCI DSS) is another scheme employed by insurers, with particular relevance to retail firms and those involved in point of sale transactions. PCI DSS was one of the first technical information security standards focused explicitly on payment processing and fines for non-compliance with it are one of the more common forms of coverage, along with data breach notification requirements (Romanosky *et al.* 2017).

The ISO 27000 series is a collection of guiding documents developed for business organizations to manage the acquisition and management of IT systems, focusing on their security. The series includes lists of detailed controls and a bevy of material on how to develop and implement both risk assessment and management programs without specifying procedures. However, the ISO series leaves much of the substantive content up to organizations and their unique requirements and risk tolerance.

COBiT was developed by an industry consortium to identify reliability and security standards for IT systems and networks in prototypical business organizations.

Complimenting specific controls are documentation guides to both risk assessment and the process of selecting controls. There is tremendous emphasis on stakeholder identification and engagement within business organizations. For this schema, security is important but tied to larger IT goals rather than a detailed assessment of the threat environment or potential consequences.

Missing from these approaches, however, was a strong enforcement mechanism. Insurers could use these standards to mitigate risk from customers, directly enforcing them through provisions in policies that would exclude coverage, for example, in the event clients fail to follow required or minimum accepted practices (Aldama & Eyerly 2018). Demand for insurance between firms and vendors in a supply chain helps drive companies to insurers for coverage. The relative expansiveness of cyber insurance compared to covering data breaches and other cybersecurity incidents under traditional lines of coverage adds to this demand, thereby reinforcing insurers enforcement power and governance authority (Talesh 2018).

4. Cyber insurance as governance

Insurance can serve as a form of governance, and is a topic that has received attention from a range of scholars from early work out of sociology through more contemporary legal scholarship on consumer safety and privacy (Ericson *et al.* 2003; Ben-Shahar & Logue 2012; Talesh 2018). Cybersecurity insurance appears to have matured as a private governance mechanism after a major spike in growth in the industry starting in 2012 in the US. There is little evidence to suggest that this sudden growth in the cyber insurance market was a product of state data breach laws. Between 2010 and 2013, only two states passed new laws. The bulk of state notification laws (33 out of 50) were passed between 2003 and 2007, leaving ample time for an increase in companies seeking coverage and a corresponding rise in premiums. In addition, the first cyber insurance policy was written in 1997, six years before the first state cyber breach notification law was passed (in California in 2003).

This sudden growth spurt was likely driven by a variety of factors including an increasingly challenging cybersecurity threat landscape, the expanding cost of breaches, and a regulatory maneuver designed to link firm's financial health to their cybersecurity risk (U.S. Securities and Exchange Commission 2011; Schutzer 2015; Romanosky & Herr 2016). A survey conducted in 2013 found that 71 percent of respondents in US firms indicated "their perception of the risks of cybercrime increased over the past 24 months" (Hartwig & Wilkinson 2014, p. 7). Additional data, based in part on surveys from the Ponemon Institute and Pricewaterhouse Coopers found that the percentage of breaches in the upper cost categories, above US$50,000 and above US$1 million had increased (Hartwig & Wilkinson 2014). The costs associated with attacks continued to rise, with one analysis finding a 22 percent increase in the related expenses of an average incident between 2014 and 2015 (Wright 2015). This growth in the industry tracked increases in the number of cybersecurity incidents as well, jumping from 421 in 2011 to 783 in 2014 across all private industry verticals (Identity Theft Resource Center 2015; Urrico 2015).

Magnifying the effect of a changing risk landscape was a 2011 U.S. Securities and Exchange Commission (SEC) guidance that outlined the manner in which companies should communicate cybersecurity risk to investors and outside parties: "cybersecurity risk disclosure… must adequately describe the nature of the material risks and specify how each risk affects the registrant" (U.S. Securities and Exchange Commission 2011). Among the potential topics for disclosure by firms was the "description of relevant insurance coverage." While not a binding regulatory output, the guidance framed risk and cybersecurity events as tied directly to the financial health of reporting firms. The move was not an extension of state authority or a binding regulatory action, but rather intended to frame cybersecurity risk as tied to the financial health of reporting firms. The result of these trends, including the SEC guidance, was to align market incentives with cybersecurity risk – granting insurers a means to more effectively profit from the demands of market participants for new vehicles to manage risk and reduce uncertainty.

The result was a sharp rise in the pool of premiums from cyber insurance policies. Figure 1 shows the change after 2012 in gross premiums written, essentially total revenue to insurers. The period between 2012 and 2015 saw an increase of nearly 300 percent. In just over two years from 2012, the total premiums from coverage jumped from US$835 million to US$2 billion in 2014 and an estimated US$4 billion in 2017 (Knockless 2015). More than 90 percent of insurers saw growth in demand between 2012 and 2014, especially from the retail sector (Advisen Ltd. 2014, pp. 4–5).

This expansion made risk transfer a legitimate option for small and medium size firms, making insurance a standard investment option for companies without massive valuation or global size. Rapid growth in the insurance market also helped drive the consensus of legitimacy of insurers as governance actors, enforcing standards

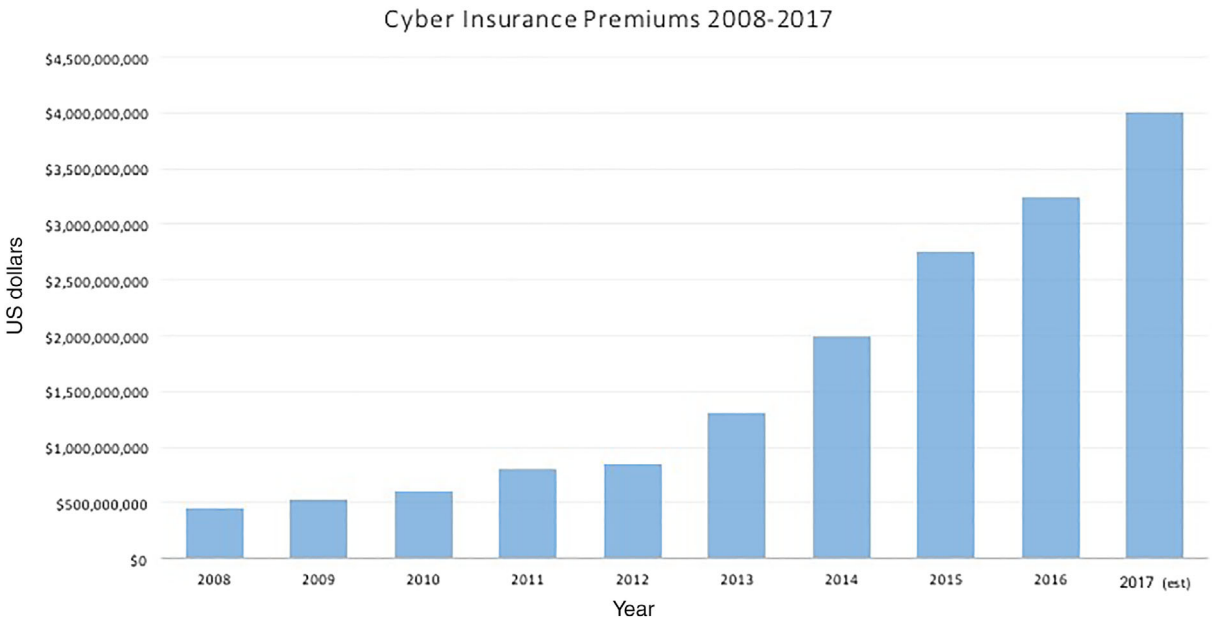

Figure 1 Gross premiums in the cyber insurance industry, 2008–2017. Source: Betterley Report, a "Cyber/Privacy Insurance Market Study," and additional data on 2012 from Timetric.

on clients, as these policies became standard fixtures in corporate cybersecurity planning. While insurers could require clients meet certain security standards in granting a policy, the principal enforcement mechanism in this governance was in driving companies to obtain an insurance policy in the first place.

Clients' use of effective security standards can reduce the risk of incidents, such as data breaches, for customers. This provides incentives for insurance firms to play a central role in encouraging the adoption of new security standards and behavior (Pal 2014). Developing these standards is subject to the same collective action problem as any other public good scenario but so far most standards have been sourced from expert bodies outside the insurance industry. Instead, the chief instrument of gain for insurers is accurately assessing risk and enforcing these security standards, as they are critical to limiting the likelihood of an adverse event and the resulting costs to the insurer.

The structure of insurers enforcement mechanism for cybersecurity standards is rooted in company's demand that those they do business with have insurance coverage, and a growing range of best practice compendiums recommending the purchase of cyber insurance. Failure to properly respond to cybersecurity incidents can cause substantial reputational harm, which serves as incentive for companies to drive business partners to obtain cyber insurance policies (Beazley Brech Response 2016). These companies are the actors who call for standards in Büthe's (2010) model, helping insurers drive compliance with security standards by their clients, the target of these standards.

The key to the cyber insurance market is that it both enables enforcement and drives profit for the insurers. Insurers are aware of the material benefits associated with offering coverage; firms generally receive US$25,000 for every US$1 million in coverage written but can charge a premium of two to three times more than normal for hard hit areas, such as retail and health care, which together constitute the areas of most rapid growth in the adoption of cyber insurance (Deloitte 2015). This coverage drives security standards to establish practices and policies to help control client's cybersecurity risk and their uncertainty over the consequences of cybersecurity events.

As the demand for insurance grows wider, so does the enforcement power of insurers. Where enforcement is weak or narrow, the utility for insurance is smaller than in a broader market where vendors and investors might demand it as part of cybersecurity risk management plans. As this market grew, so did an unusual enforcement mechanism where companies drove each other to obtain policies and adhere to the corresponding cybersecurity

standards. This peculiar market-based enforcement is central to understanding the power of cyber insurance as a governance activity and holds potential theoretical utility in other domains.

4.1. Governance through the market

Governance scholars have previously addressed the market's role in enforcement; initially, market activity was depicted as a way for new constituencies to drive standards of behavior in their suppliers, like the demand for "green" products or fair labor practices behind consumer goods (Andrews 1998, p. 181; Elliott & Freeman 2003). These cases look mostly like self-regulation as industry participants largely determined the rules. This is an advance from the Corporate Social Responsibility (CSR) approach which focused on voluntary standards and moral legitimacy but lacked clear profit motive for either standard setter or adopter (Tollefson 1999; Garriga & Melé 2013). One of the major differences between CSR and market-based governance debates is that the latter needs a profitable incentive for firms to adopt these standards as markets depend on the material incentives of consumers but firms remain central to "cooperate among themselves in designing limits on their own behavior" (Haufler 2003, p. 238). But these CSR debates focused primarily on consumers as the market participants with power, meaning enforcement was, at best, often diffuse and difficult to sustain.

Building on this earlier work, other scholars advanced the concept of non-state market driven (NSMD) governance. The basic model of participants is largely the same; standards are developed by one party, demanded by a second, and targeted at a third. Under NSMD however, the demand for governance comes from investors and suppliers to the targeted firm, their influence legitimated and made powerful by business relationships with these targeted firms (Cashore 2002, p. 509). The market becomes a source of enforcement authority as companies above or below the target firm (vendors or investors) push for standards adoption. Building in an outside auditing and verification process with the standard setters helps limit the potential for shirking by companies targeted by standards. This auditing requirement became widespread in environmental regulation in the 1980s, was offered as an alternative to state enforcement of the Clean Air Act, and has long been a central feature in accounting and finance governance (Andrews 1998, p. 182; Mattli & Büthe 2005b). Within the NSMD approach, each participant has a material interest in the outcome of the governance activity but unlike in the CSR model is often removed from the standards development process.

These stakeholders in a targeted firm's supply chain become the participants demanding governance who grant legitimate authority to standard setters. Like consumers, the financial power of requesting firms in a targeted company's supply chain can shape the targeted company's behavior. Relative to the emphasis on consumers in previous scholarship, like labor standards, these companies are more organized and their demands often more coherent. In much of the non-NSMD work by contrast, the demanders of regulation are activist groups and non-governmental organizations without the legitimated influence on the potential targets that stems from contractual relationships (Büthe 2010).

Insurers enforcement of cybersecurity standards has been effectuated through the marketplace as stakeholders in targeted firms' supply chains help drive compliance in an extension of NSMD governance. NSMD was originally developed to study governance in forestry and environmental practices, where certification processes and labels are used as a means of enforcing production and distribution standards of behavior (Cashore 2002).

The comparison of forestry and cybersecurity is a novel one, but there are surprising parallels. In both cases, firms rely heavily on key vendor relationships. In forestry, these relationships are between logging companies and major resellers, such as Lowes or Home Depot; in cybersecurity, this dynamic is mirrored between vendors, whether small and specialized or large like IBM, and their customers. These markets influence firms' choices in the design of supply chains and corporate behavior.

Logging and the associated lumber production pipeline can have a detrimental impact on long-standing forest areas both through excessive harvesting and harmful processes to cut, treat, and refine wood for use. Timber harvesting, especially of softwoods that make up the primary source of global lumber, is big business and a political flashpoint in Canada. There have been a multitude of efforts by both local political actors and international environmental groups to fashion a governance apparatus for these processes with varying but often unsuccessful outcomes. What change did take place, mostly during the 1980s and early 1990s, consisted of a mix of private

and public efforts focused on performance standards and practices, such as biodiversity maintenance and efficient harvesting techniques (Cashore *et al.* 2007, p. 59).

Neither these efforts nor a subsequently developed voluntary Forestry Practice Code did much to impact producer behavior or quell concerns over environmental harms (Rayner *et al.* 2001). In all cases, serious reform of industry practices was limited, with few detailed rules or effective enforcement mechanisms, both preconditions for successful NSMD governance. This follows a similar pattern of voluntary standards and public–private engagement in US cybersecurity debates, ultimately resulting in narrow industry-driven requirements and relatively loose enforcement.

Attempting to evolve from these earlier unsuccessful efforts, a group of environmental groups gathered in Toronto to develop the Forestry Stewardship Certification (FSC) scheme. FSC is a model of private governance applied to forestry, intended to develop and enforce standards of behavior on industry and overcome concerns about the negative externalities of logging and lumber production (Leslie 2004). FSC initially contended with substantial competition from more than 20 other certification schemes developed by trade associations and competing industry groups (Pattberg 2006, p. 582).

Outside certification plays a major role in NSMD governance to enforce standards, and FSC's emphasis on specific requirements and outside auditing helped to distinguish it from alternative programs. The Sustainable Forestry Initiative (SFI), prominent in the Americas, focuses on best practices in management (rather than production). The SFI requires centralized submission of performance data but not public disclosure and has no auditing requirement (Cashore *et al.* 2004, p. 14). The Pan European Forest Certification (PEFC), later renamed the Programme for the Endorsement of Forest Certification in 2003, scheme provides a platform for mutual recognition between different national standard processes. PEFC does include an auditing requirement in certain instances of group certification but leaves the rules and standards development to independently constituted national groups without rules on membership (Cashore *et al.* 2004, p. 15). FSC, by contrast, emphasized performance standards and goals rather than binding rules, and targeted logging companies' supply chains rather than the producers directly.

This emphasis on the supply chain as a means of enforcing standards on logging companies was important to FSC's success. Much of Canada's lumber market was concentrated in sales to Japan and the US, but collapse in demand from Asian markets through the late 1990s forced Canadian firms to reallocate production to the US where they were further limited by export restrictions placed in the Canada–US Softwood Lumber Agreement (Cashore *et al.* 2007). The concentration of Canadian lumber sales into the US helped compress the pool of potential business relationships and made Canadian firms particularly sensitive to disruption there.

FSC groups focused on influencing lumber's production supply chain by winning over firms such as Home Depot and using them to pressure production companies (Cashore *et al.* 2004, p. 79). This improved the legitimacy of the FSC standards as other wholesalers and retail outlets in the US began to require the certification's use in any lumber they purchased. Between 2006 and 2009, the total forest area of FSC-covered lumber producers increased substantially from 60 to 117 million hectares (Chen *et al.* 2010, p. 2; Pattberg 2006, p. 585). The Canadian government was not directly involved in the FSC development process or its initial uptake, matching the second element of NSMD governance whereby government actors have no stake in the decisionmaking associated with enforcement.

The direct involvement of companies in logging firms' supply chain helped drive adoption of the FSC standards, even where there were competing industry schemes. Focusing education and legitimization efforts for the FSC standards on US lumber distributors and wholesalers meant environmental groups had to advocate to a far smaller number of stakeholders than in consumer-focused advocacy (Chen *et al.* 2010, pp. 2–4). The influence of these networks of investors and vendors also exists in cybersecurity as firms are looking to manage their total exposure to risk as well as those of business partners, using the adoption of insurance policies as a means of reducing uncertainty. NSMD governance helps describe the structure of a market-based enforcement mechanism where financial incentives for standards demanders and targeted firms drive adoption and compliance.

5. Conclusion and implications

Insurers represent a private governance activity in cybersecurity, taking on a standard-setting and enforcement role. The variation in underwriting capacity and technical maturity between insurers means this role may not be

universal but it is real and influential. There was a time that cybersecurity standards were more akin to environmental regulation; self-governance enabled companies to keep costs low and maintain a benighted ignorance of the mechanics of IT or the sort of threats that might be arrayed against them. This dynamic has shifted, as cybersecurity has become a prominent issue for firms and their financial health. This sensitivity to cybersecurity exposure combined with new demands from firm's business partners helps enforce the standards set by insurers.

The emergence of this governance role is best explained by the argument for private advance. The lynchpin of the argument for private advance is that the regulators find some financial benefit in setting and enforcing standards and that their activities satisfy the demands of those seeking regulation. Cyber insurance satisfies both of those elements, lending weight to the argument that rapid growth in the cyber insurance market after 2012 and its maturation as a source of governance is the product of private advance rather than a retreating state. Importantly, the period of time during which cyber insurance has had any real authority to enforce security standards has been too short to judge the existence of governance by improved outcomes alone.

Using a set of cybersecurity standards to evaluate and provide coverage to clients does not mean insurers must *also* discount the cost of that coverage for good security behavior. This disconnect has been a major feature in the discussion of insurance coverage as a broader public policy tool – premium discounts as an incentive for client behavior is a still rare phenomenon in cyber insurance (Romanosky *et al.* 2017). There are limited examples of this behavior in existing cyber insurance offerings, including a study of Swedish insurers that use lower premiums in conjunction with security standards requirements to drive behavioral change in their customers (Franke 2017).

While there is an important state role in the SEC guidance linking a company's cybersecurity risk to their financial health, this carried no direct enforcement authority, thereby doing more to expand the market than dictate standards of behavior by companies. This guidance also complemented a broader trend in company's awareness of cybersecurity risk. A 2015 report from Moody's, a credit rating agency and classic coordination service firm, found that as a result of the evolving nature of cybersecurity risk and potential loss, "boards have become particularly focused on making sure corporations have adequate systems and controls in place to safeguard their own data and that of their customers" (Wright 2015).

The implementation of Europe's Global Data Protection Regulations (GDPR) should reinforce this incentive to gain and provide coverage. The early growth of cyber insurance in the US was spurred by the passage of state level data breach notification laws. Insurance related to GDPR could cover notification as well as a range of compliance costs and potential penalties. One potential limitation to this is the relatively vague state of some key GDPR controls, such as the lawfulness of processing data, which is currently subject to something of a backdoor clause allowing processing of data anywhere it is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party" (European Parliament and Council 2016). As implementation guidance and the body of case law around GDPR evolve, insurers will likely be more enthusiastic to offer relevant coverage.

There is more work to be done to understand the precise operation and broader applicability of this market-based enforcement mechanism. Cybersecurity standards of practice, at least with respect to the operation and maintenance of IT infrastructure, are relatively well codified in several collections of standards, including the NIST 800–53 series and ISACA COBIT controls. Other areas may not have such specific standards or as large a market for potential insurance customers. Where the process of standards development is more bitterly contested, governance could be characterized by rivalrous leadership. Future work should also address the impact of different supply chain configurations on the efficacy of market-enforcement power.

As cyber insurance continues to grow, it would be useful to evaluate the specific power of firm's contractual arrangements to understand the possibilities (and limits) of supply chain power. Cybersecurity presents a relatively aligned set of interests in that firms all wish to avoid the consequences of a breach, albeit with varying levels of risk tolerance and willingness to invest. Other applications of this market-based enforcement may find instances where actors in a supply chain differ in their preference of ultimate outcomes, for example, where vendors are battling over the adoption of competing technologies. The presence of substantial gaps in domain expertise between supply chain firms and the ultimate target of governance may also impact the ability of these firms to influence the target.

Cyber insurers' ability to set and enforce security standards on clients constitutes an unusual instance of private governance. The policy implications for governments center on the state's willingness to craft neutral

standards. Government standards bodies retain a high degree of legitimacy in the private sector as their codification efforts have provided robust starting points for the design and implementation of security controls. This effort has continued with discussions at the US Food and Drug Administration around cybersecurity-responsive development, production, and operating practices for medical device manufacturers. Continuing engagement with companies and non-profit groups, as well as additional work to improve risk assessment practices, would be a boon to this effort and help reinforce best practices in both private and public sector organizations.

Cyber insurance is a rapidly expanding market whose ability to recognize trends across customers and identify best practices could serve not only to enforce, but also to eventually recognize new best practices. A study in 2013 found that after purchasing an insurance product, firms found their security posture improved, with firms relying on insurers to select controls and risk management policies in more than 75 percent of situations (Ponemon Institute 2013, p. 10). The prospect for insurers to act as arbiters of best practice would be an evolution from the current status quo but holds potential to greatly improve the evolution and promulgation of standards in cybersecurity (Morgus 2016).

At present, the market acts as a form of private governance over existing security standards, a novel form of this governance in cybersecurity. This governance, which works to break down information asymmetries in the private sector and helps to enforce security standards, could well serve as model for policymakers. The keys appear to be emphasizing lateral pressure from companies against their business partners and vendors rather than direct regulation and the role of certain specialized companies, like insurance firms, to monetize standards enforcement.

Acknowledgments

Thank you to Susan Sell, Steve Balla, Robert Adcock, Lance Hoffman, and Allan Friedman for their particularly detailed feedback. Thank you also to the Belfer Cyber Security Project team, as well as Sasha Romanosky, Ryan Ellis, Robert Morgus, Angela McKay, Sam Liles, Tom Finan, Jacob Olcott, Ian Wallace, Costis Toregas, Darrell Morgeson, Yevgeniy Kirpichevsky, and Jason Dechant for comments on previous versions and guidance on the topics of risk and cyber insurance more broadly. Additional thanks to AIG, Zurich, Philadelphia Insurance Companies, and Alvarez & Marsal for information and background discussion.

References

Abbott KW, Levi-Faur D, Snidal D (2017) Theorizing Regulatory Intermediaries: The RIT Model. *ANNALS of the American Academy of Political and Social Science* 670(1), 14–35.

Advisen Ltd. (2014) Cyber Liability Insurance Market Trends: Survey. Advisen. [Last accessed 5 August 2018.] Available from URL: https://www.advisenltd.com/wp-content/uploads/cyber-liability-insurance-market-trend-survey-2014-10-28.pdf

Aldama, K. S., Eyerly, T. R. (2018) Cyber Policies - The Next Wave. In *ABA Insurance Coverage Litigation Committee* (p. 24) Tuscon, AZ. [Last accessed 5 August 2018]. Available from URL: https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2018-insurance/written-materials/cyber-policies.authcheckdam.pdf.

Alt JE, Alesina A (1998) Political Economy: An Overview. In: Goodin RE, Klingemann HD (eds) *New Handbook of Political Science*, pp. 645–674. OUP, Oxford.

Andrews RN (1998) Environmental Regulation and Business "Self-regulation". *Policy Sciences* 31(3), 177–197.

Aon Inpoint (2017) *Global Cyber Market Overview (White Paper)*. Aon Insurance, London.

Arts B, Noortmann M, Reinalda B (2001) *Non-state Actors in International Relations*. Ashgate Publishing, Adlershot.

Beazley Breach Response. (2016) A Data Breach Isn't Always a Disaster: Mishandling It Is. Beazley. [Last accessed 5 August 2018.] Available from URL: https://www.beazley.com/documents/TMB/BBR%20Canada/beazley-bbr-brochure- factsheet-canada.pdf.

Ben-Shahar O, Logue KD (2012) Outsourcing Regulation: How Insurance Reduces Moral Hazard. *University of Michigan Law Review* 111, 197–248.

Betterley, R. S. (2015) Betterley - Cyber/Privacy Insurance Market Survey. Betterley Risk Consultants.

Böhme, R., Schwartz, G. (2010) Modeling Cyber-insurance: Towards a Unifying Framework. In *Proceedings of the 9th Annual Workshop on the Economics of Information Security*, 7–8 June, Cambridge, MA. [Last accessed 5 August 2018.] Available from URL: http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf.

Börzel, T. A., Risse, T. (2005) "Public-private partnerships: Effective and legitimate tools of international governance" in Reconstituting Political Authority. Complex Sovereignty and the Foundations of Global Governance. In: Edgar G, Louis P (eds), Toronto, 195–216.

Brown BD (2014) The Ever-evolving Nature of Cyber Coverage. *The Insurance Journal*. [Last accessed 5 August 2018.] Available from URL: http://www.insurancejournal.com/magazines/features/2014/09/22/340633.htm.
Business Wire Staff. (2017) AIG Launches New Cyber Model That Scores Client Cyber Risk. *Business Wire*. [Last accessed 5 August 2018.] Available from URL: https://www.businesswire.com/news/home/20171212005720/en/AIG-Launches-New-Cyber-Model-Scores-Client.
Büthe T (2004) Governance through Private Authority? Non-state Actors in World Politics. *Journal of International Affairs* 58 (1), 281–290.
Büthe T (2010) Private Regulation in the Global Economy: Guest Editor's Note. *Business and Politics* 12(3), 1.
Büthe T, Mattli W (2011) *The New Global Rulers: The Privatization of Regulation in the World Economy*. Princeton University Press, Princeton, NJ.
Cashore B (2002) Legitimacy and the Privatization of Environmental Governance: How Non-state Market-driven (NSMD) Governance Systems Gain Rule-making Authority. *Governance* 15(4), 503–529.
Cashore B, Auld G, Newsom D (2004) *Governing through Markets: Forest Certification and the Emergence of Non-state Authority*. Yale University Press, New Haven, CT.
Cashore B, Egan E, Auld G, Newsom D (2007) Revising Theories of Nonstate Market-driven (NSMD) Governance: Lessons from the Finnish Forest Certification Experience. *Global Environmental Politics* 7(1), 1–44.
Chen J, Innes J, Tikina A (2010) Private Cost-benefits of Voluntary Forest Product Certification. *International Forestry Review* 12(1), 1–12.
Clark G (1999) *Betting on Lives: The Culture of Life Insurance in England*, pp. 1695–1775. Manchester University Press, New York.
Cutler AC, Haufler V, Porter T (1999) *Private Authority and International Affairs*. Suny Press, Albany, NY.
Deloitte. (2013) *FISMA Takes Private Sector By Surprise*. [Last accessed 31 Dec 2015.] Available from URL: http://deloitte.wsj.com/cio/2013/06/03/fisma-takes-private-sector-by- surprise/.
Deloitte. (2015) *Cyber Insurance: One Element of Risk Management - Deloitte Risk & Compliance - WSJ*. [Last accessed 31 Dec 2015.] Available from URL: http://deloitte.wsj.com/riskandcompliance/2015/03/18/cyber-insurance-one- element-of-a-cyber-risk-management-strategy/.
Elliott KA, Freeman RB (2003) *Can Labor Standards Improve under Globalization?* Peterson Institute Press, Washington, DC.
Epstein D, O'Halloran S (1999) *Delegating Powers: A Transaction Cost Politics Approach to Policy Making under Separate Powers*. CUP, Cambridge, UK.
Ericson RV, Doyle A (2004) *Uncertain Business : Risk, Insurance and the Limits of Knowledge*. University of Toronto Press, Toronto.
Ericson RV, Doyle A, Barry D, Ericson D (2003) *Insurance as Governance*. University of Toronto Press, Toronto.
European Parliament and Council (2016) General Data Protection Regulation, Regulation (EU) 2016/679 §.
Farrell H (2006) Regulation Information Flows: States, Private Actors, and E-commerce. *Annual Review of Political Science* 9 (1), 353–374.
Franke U (2017) The Cyber Insurance Market in Sweden. *Computers & Security* 68, 130–144.
Fuchs D (2005) Commanding Heights? The Strength and Fragility of Business Power in Global Politics. *Millennium-Journal of International Studies* 33(3), 771–801.
Garriga E, Melé D (2013) Corporate Social Responsibility Theories: Mapping the Territory. In: Michalos AC, Poff DC (eds) *Citation Classics from the Journal of Business Ethics*, pp. 69–96. Springer, New York.
Green JF (2013) *Rethinking Private Authority: Agents and Entrepreneurs in Global Environmental Governance*. Princeton University Press, Princeton, NJ.
Hartwig RP, Wilkinson C (2014) *Cyber Risks: The Growing Threat*. Insurance Information Institute, New York. [Last accessed 5 August 2018.] Available from URL: http://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf.
Haufler V (2003) New Forms of Governance: Certification Regimes as Social Regulations of the Global Market. In: Gerhard O, Chris E, Errol M (eds) *Social and Political Dimensions of Forest Certification*, pp. 237–247. Remagen, Germany: Forstbuch.
Hickens, M. (2014) *Insurer Warns Client of Possible Breach*. [Last accessed 31 Dec 2015.] Available from URL: http://blogs.wsj.com/cio/2014/03/11/insurer-warns-client-of-possible-breach/.
Identity Theft Resource Center. (2015) 2011 ITRC Breach Report Key Findings. [Last accessed 5 August 2018.] Available from URL: https://www.idtheftcenter.org/2011-data-breaches/.
International Organization for Standardization. (2014) *ISO/IEC 27001 - Information Security Management*. [Last accessed 5 August 2018.] Available from URL: http://www.iso.org/iso/home/standards/management- standards/iso27001.htm.
Jaffee DM (2005) The Role of Government in the Coverage of Terrorism Risks. *Terrorism Risk Insurance in OECD Countries*, Vol. 9. OECD Publishing, Paris [Last accessed 5 August 2018.] Available from URL: http://faculty.haas.berkeley.edu/jaffee/papers/091DJOECD.pdf.
Kahler M, Lake DA (eds) (2004) *Governance in a Global Economy: Political Authority in Transition*. Princeton University Press, Princeton, NJ.
Kean T (ed) (2011) *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Government Printing Office, Washington DC [Last accessed 5 August 2018.] Available from URL: https://books.google.com/books?hl=en&lr=&id=UabGPLhbGckC&oi=fnd&pg=PA 1&dq=9–11+commission&ots=KEWrVMKEEU&sig=BOR06yIdF8Swt0hyTUSptg4R o.
Knill C, Lehmkuhl D (2004) Private Actors and the State. *Global Governance: Critical Concepts in Political Science* 3(1), 41–63.
Knockless, T. (2015) *Demand for Cyber Risk Insurance Market on the Rise*. [Last accessed 31 Dec 2015.] Available from URL: http://www.propertycasualty360.com/2015/10/01/demand-for-cyber-risk-insurance- market-on-the-rise.

Kreb, B. (2014) *Target Hackers Broke in Via HVAC Company — Krebs on Security*. [Last accessed 31 Dec 2015.] Available from URL: http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
Kunreuther HC, McNulty PJ, Kang Y (2002) Third-party Inspection as an Alternative to Command and Control Regulation. *Risk Analysis* 22(2), 309–318.
Lecraw DJ (1984) Some Economic Effects of Standards. *Applied Economics* 16(4), 507–522.
Lehmkuhl D, Knill C (1998) Integration by Globalisation: The European Representation of the Consumer Electronics Industry. *Current Politics and Economics of Europe* 8(2), 131–153.
Leiner BM, Cerf VG, Clark DD *et al.* (2009) A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review* 39(5), 22–31.
Leslie AD (2004) The Impacts and Mechanics of Certification. *International Forestry Review* 6(1), 30–39.
Levi-Faur D (2011) Regulation and Regulatory Governance. In: Levi-Faur D (ed) *Handbook on the Politics of Regulation*, pp. 3–25. Edward Elgar, Cheltenham, UK.
Marsh Management Research. (2015) *Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise*. Marsh Management, New york. [Last accessed 5 August 2018.] Available from URL: https://www.content/oliverwyman.com/dam/marsh/Documents/PDF/US-en/Benchmarking Trends Cyber Concerns Broaden, Insurance Purchases Rise-03-2015.pdf.
Mattli W, Büthe T (2003) Setting International Standards: Technological Rationality or Primacy of Power? *World Politics* 56 (1), 1–42.
Mattli W, Büthe T (2005a) Accountability in Accounting? The Politics of Private Rule-making in the Public Interest. *Governance* 18(3), 399–429.
Mattli W, Büthe T (2005b) Global Private Governance: Lessons from a National Model of Setting Standards in Accounting. *Law and Contemporary Problems* 68(3/4), 225–262.
Maynard T, Beecroft N (2015) *Business Blackout - the Insurance Implications of a Cyber Attack on the US Power Grid*. Lloyds of London, London. [Last accessed 5 August 2018.] Available from URL: https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/business-blackout/business-blackout20150708.pdf.
Morgus R (2016) Cyber Insurance: A Market-based Approach to Information Assurance. In: Harrison RM, Herr T (eds) *Cyber Insecurity: Navigating the Perils of the Next Information Age* (1st ed., pp. 155–170). Rowman & Littlefield Publishers, Lanham, MD.
Mosley L (2009) Private Governance for the Public Good? Exploring Private Sector Participation in Global Financial Regulation. In: Milner HV, Moravcsik A (eds) *Power, Interdependence and Nonstate Actors in World Politics*, pp. 126–146. Princeton University Press, Princeton, NJ.
Newman, C. (2016) *Target's Cyber Insurance: A $100 Million Policy Vs. $300 Million (So Far) in Costs*. Patterson Belknap Data Security Law Blog, 7 Apr. [Last accessed 5 August 2018.] Available from URL: https://datasecuritylaw.com/targets-cyber-insurance-a-100-million-policy-vs-300-million-so-far-in-costs/.
Odell LA, Fauntleroy JC, Wagner RR (2015) *Cyber Insurance – Managing Cyber Risk (No. D-5481)*. Institute for Defense Analyses, Alexandria, VA. [Last accessed 5 August 2018.] Available from URL: https://www.ida.org/~/media/Corporate/Files/Publications/IDA_Documents/ITSD/2 015/D-5481.ashx.
Pal R (2014) *Improving Network Security through Cyber-Insurance*. University of Southern California. [Last accessed 5 August 2018.] Available from URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.717.6362&rep=rep1&type=pdf.
Pattberg P (2006) Private Governance and the South: Lessons from Global Forest Politics. *Third World Quarterly* 27(4), 579–593.
Ponemon Institute. (2013) *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age*. Ponemon Institute 22 Aug. [Last accessed 5 August 2018.] Available from URL: https://www.ponemon.org/blog/managing-cyber-security-as-a-business-risk-cyber-insurance-in-the-digital-age.
Porter T (1995) *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton University Press, Princeton, NJ.
Rayner J, Howlett M, Wilson J, Cashore B, Hoberg G (2001) Privileging the Sub-sector: Critical Sub-sectors and Sectoral Relationships in Forest Policy-making. *Forest Policy and Economics* 2(3), 319–332.
Romanosky S (2016) Examining the Costs and Causes of Cyber Incidents. *FTC Privacy Con*, Washington, D.C. p. 23.
Romanosky, S., Ablon, L., Kuehn, A., Jones, T. (2017) Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk? In Proceedings of the 16th Annual Workshop on the Economics of Information Security, 26–27 June, La Jolla, CA. [Last accessed 5 August 2018.] Available from URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2929137.
Romanosky S, Herr T (2016) Understanding Cyber Crime. *Cyber Insecurity: Navigating the Perils of the Next Information Age*, 1st edn, pp. 155–170. Rowman & Littlefield Publishers, Lanham, MD.
Schutzer, D. (2015) *CTO Corner: An Assessment of Cyber Insurance.* [Last accessed 31 Dec 2015.] Available from URL: http://fsroundtable.org/cto-corner-assessment-cyber- insurance/.
Securities and Exchange Commission. (2011) *CF Disclosure Guidance: Topic No. 2.* [Last accessed 5 August 2018.] Available from URL: https://www.sec.gov/divisions/corpfin/guidance/cfguidance- topic2.htm.
Spar DL (1999) Lost in (Cyber)Space: The Private Rules of Online Commerce. In: Cutler AC, Haufler V, Porter T (eds) *Private Authority and International Affairs*, pp. 31–52. Suny Press, Albany, NY.
Spruyt H (2001) The Supply and Demand of Governance in Standard-setting: Insights from the Past. *Journal of European Public Policy* 8(3), 371–391.
Stoker G (1998) Governance as Theory: Five Propositions. *International Social Science Journal* 50(155), 17–28.
Strange S (1996) *The Retreat of the State: The Diffusion of Power in the World Economy*. CUP, Cambridge, UK.

Stults, G. (2004) An Overview of Sarbanes-Oxley for the Information Security Professional. [Last accessed 5 August 2018.] Available from URL: https://www.sans.org/reading- room/whitepapers/legal/overview-sarbanes-oxley-information-security- professional-1426.
Talesh S (2015) A New Institutional Theory of Insurance. *University of California-Irvine Law Review* 5(3), 617–650.
Talesh S (2018) Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. *Law & Social Inquiry* 43(2), 417–440.
Thomason JS, Morgeson JD, Fitzsimmons MF (2013) *Integrated Risk Assessment and Management Model (IRAMM) (No. NSD-4883)*. Institute for Defense Analyses, Alexandria, VA. [Last accessed 5 August 2018.] Available from URL: https://www.ida.org/~/media/Corporate/Files/Publications/IDA_Documents/SFRD/ NS D-4883.ashx.
Thoyts R (2010) *Insurance Theory and Practice*. Routledge, Oxford.
Tollefson C (1999) *The Wealth of Forests: Markets, Regulation, and Sustainable Forestry*. UBC Press, Vancouver.
Tuttle B, Vandervelde SD (2007) An Empirical Examination of CobiT as an Internal Control Framework for Information Technology. *International Journal of Accounting Information Systems* 8(4), 240–263.
Urrico, R. U. J. (2015) Data Breaches on Record Pace for 2015. *Credit Union Times, 5 July*. [Last accessed 5 August 2018.] Available from URL: http://www.cutimes.com/2015/07/05/data-breaches-on- record-pace-for-2015.
Verbruggen PWJ (2014) Regulatory Governance by Contract. The Rise of Regulatory Standards in Commercial Contracts. *Recht der Werkelijkheid* 35(3), 79–100.
Walker C (2014) Organizational Learning: The Role of Third Party Auditors in Building Compliance and Enforcement Capability. *International Journal of Auditing* 18(3), 213–222.
Warren E (2010) Redesigning Regulation: A Case Study from the Consumer Credit Market. In: Balleisen EJ, Moss DA (eds) *Government and Markets: Toward a New Theory of Regulation*, pp. 391–418. CUP, New York.
Webel B (2014) Terrorism Risk Insurance: Issue Analysis and Overview of Current Program. *Congressional Research Service* 7-5700, 0-22. [Last accessed 5 August 2018.] Available from URL: https://www.fas.org/sgp/crs/terror/R42716.pdf.
Woo G (2002) Quantifying Insurance Terrorism Risk. *Manuscript, Risk Management Solutions*. Newark, CA. [Last accessed 5 August 2018.] Available from URL: http://www.rit.edu/cos/math/cmmc/conferences/2007/literature/Woo_2002b.pdf.
Wright A (2015) Cyber Market Dramatically Increases. *Risk & Insurance*. [Last accessed 5 August 2018.] Available from URL: http://www.riskandinsurance.com/cyber-market-dramatically-increases/.

Laws cited

The Clean Air Act, 42 U.S.C. § 7401 (1963)
Federal Information Security Modernization Act of 2002, FISMA, 44 U.S.C. § 3541 (2002)
General Data Protection Regulation (EU) 2016/679 (2018)
Health Insurance Portability and Accountability Act of 1996 (HIPAA) 42 U.S.C. § 300gg and 29 U.S.C § 1181 et seq. and 42 USC 1320d et seq. (1996)
Health Information Technology for Economic and Clinical Health Act (HITECH), U.S.C § 139w-4(0)(2) (2009)
Sarbanes-Oxley Act of 2002, 15 U.S.C. 7201 (2002)
Terrorism Risk Insurance Act (TRIA) (H.R. 3210, Pub.L. 107–297 (2002)