Law & Social Inquiry
Journal of the American Bar Foundation

Law & Social Inquiry
Volume ••, Issue ••, ••–••, •• 2017

Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses

Shauhin A. Talesh

While data theft and cyber risk are major threats facing organizations, existing research suggests that most organizations do not have sufficient protection to prevent data breaches, deal with notification responsibilities, and comply with privacy laws. This article explores how insurance companies play a critical, yet unrecognized, role in assisting organizations in complying with privacy laws and dealing with cyber theft. My analysis draws from and contributes to two literatures on organizational compliance: new institutional organizational sociology studies of how organizations respond to legal regulation and sociolegal insurance scholars' research on how institutions govern through risk. Through participant observation at conferences, interviews, and content analysis of insurer manuals and risk management services, my study highlights how insurers act as compliance managers for organizations dealing with cyber security threats. Well beyond pooling and transferring risk, insurance companies offer cyber insurance and unique risk management services that influence the ways organizations comply with privacy laws.

INTRODUCTION

This article explores the rise of the insurance industry as a regulatory intermediary of corporate behavior. Whereas recent insurance law and society research has examined the role that insurance and insurance companies play in shaping the meaning of compliance in corporate governance (Baker and Griffith 2010), employment (Talesh 2015a), and policing settings (Rappaport forthcoming), I explore how the insurance field, through cyber insurance, responds to and influences the meaning of compliance among organizations that are dealing with privacy laws and a burgeoning global problem: cyber security.

Cyber risks, that is, loss exposure associated with the use of electronic equipment, computers, information technology, and virtual reality, are among the biggest

Shauhin A. Talesh is a Professor of Law, Sociology, and Criminology, Law & Society at the University of California, Irvine. Please direct all correspondence to Shauhin Talesh, University of California, Irvine, School of Law, 401 E. Peltason Drive, Ste. 4800L, Irvine, CA 92697; e-mail: stalesh@law.uci.edu. Thanks to John Cioffi, Max Helveston, Claire Hill, Dan Schwarcz, and Cathy Sharkey for providing helpful feedback on earlier drafts. Thanks also to Itohan Okogbo and Elad Shem-Tov for outstanding research assistance on this project. An earlier version of this article was presented at the American Bar Foundation Faculty Workshop, University of California, Berkeley School of Law, Center for the Study of Law and Society Speaker Series, the University of Minnesota Faculty Workshop, the University of California, Hastings Faculty Workshop, the Drexel Law School Faculty Workshop, and the 2016 Society for the Advancement of Socio-Economic Studies Conference. The University of California, Irvine School of Law is thanked for providing funding to support this research.

new threats facing businesses and consumers. Cyber security risks are crucial as consumer, financial, and health information are increasingly stored in electronic form. Hackers, malware, viruses, tracking software, wiretapping, eavesdropping, robocalls, and solicitation lead to identity theft and compromised personal, financial, and health information. These breaches affect virtually every major industry, including, but not limited to, financial services, health care, government, entertainment, online gaming, retail, law, insurance, social networking, and credit card processing.

As people become more reliant on electronic communication and organizations collect and maintain more information about their consumers, the opportunity for bad actors to cause problems for organizations and the public is growing exponentially. The number of data breaches tracked by the Identity Theft Resource Center (ITRC) in 2015 was 781, the second highest year on record since the ITRC began tracking breaches in 2005 (ITRC 2016). The Ponemon Institute, an independent research organization on privacy, data protection, and information security policy, notes that 75 percent of organizations surveyed experienced data loss or breach since 2014 (Ponemon Institute 2016). The Office of Civil Rights indicated that 112 million health-care-related records were lost, stolen, or inappropriately disclosed via data breaches in 2015 (Munro 2015). According to recent reports, the average cost of a data breach event for an organization is between 3 and 7 million dollars (Podolak 2015; Lovelace 2016).[1]

In addition to financial and public relations damage, data breach events often threaten an organization's survival. Organizations also face compliance hurdles as they navigate between various, sometimes overlapping, federal and state laws and regulations concerning the collection and use of personal data.[2] The proliferation of security breaches in the last five years has resulted in an expansion of privacy laws, regulations, and industry guidelines. The increased flow of data across state boundaries, coupled with the increased enactment of data-protection-related statutes, creates significant challenges for organizations operating at a national level to comply with the state and federal legal requirements.

Even when there is no evidence that compromised data were used or otherwise disseminated, companies are still potentially subject to notification requirements, resulting in significant costs. Forty-seven states have notification statutes that require prompt notice of data breaches to those affected and to the state attorney general. Moreover, many statutes impose a significant daily fine for late notice or a

1. In addition, IBM's most recent report indicated that it costs approximately $158 for every lost or stolen record. In highly regulated industries such as health care, the cost of a breach can be as much as $355 per record (Lovelace 2016).

2. There is no single, comprehensive federal national law regulating the collection and use of personal data in the United States. Instead, the United States has a patchwork of federal and state laws that sometimes overlap. The major federal laws that regulate privacy in different ways include, but are not limited to, the Federal Trade Commission Act, the Financial Services Modernization Act, the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, and the Electronic Communications Privacy Act. There are many laws at the state level that regulate the collection and use of personal data. Some federal privacy laws preempt state privacy laws on the same topic. For example, the federal law regulating commercial e-mail and the sharing of e-mail addresses preempts most state laws regulating the same activities. However, there are many federal privacy laws that do not preempt state laws, which means that a company can find itself in the position of trying to comply with federal and state privacy laws that regulate the same types of data or types of activity in slightly different ways.

private right of action for failure to comply. Finally, as the number of data breaches grows, so does the number of individuals pursuing legal action to remedy their injuries.[3]

Despite legal, reputational, financial, and survival threats, prevailing research suggests that private organizations are not significantly changing their behavior. Although many organizations do have formal policies in place, the majority of organizations do not believe they are sufficiently prepared for a data breach, have not devoted adequate money, training, and resources to protect consumers' electronic and paper-based information from data breaches, and fail to perform adequate risk assessments (Business Wire 2015; Ponemon Institute 2015, 2016). In fact, because complying with multiple security frameworks is difficult, time consuming, and expensive, many organizations express "compliance fatigue" (Armerding 2015).

Recognizing this underpreparation and undercompliance gap, the insurance field stepped in during the last decade and began offering cyber insurance. Cyber insurance is insurance designed to provide both first-party loss and third-party liability coverage for data breach events, privacy violations, and cyber attacks. Although there is variation in the types of policies being offered, insurers offering cyber insurance provide some risk shifting for the costs associated with having to respond, investigate, defend, and mitigate against the consequences surrounding a cyber attack.

Compared to other lines of insurance, cyber insurance is in its infancy. Therefore, there is limited data on how competitive the cyber market is. However, we do know the cyber insurance market is growing rapidly as organizations become more aware of its potential usefulness. Whereas most companies did not have cyber insurance a decade ago, one in three organizations now has insurance specifically protecting against cyber and data theft losses (Fernandes 2014; Business Wire 2015).[4] The insurance industry's most recent reports, issued in 2015, indicate that 120 insurance groups are writing cyber insurance in the United States, totaling approximately $1 billion in direct written premiums with a loss ratio of 65 percent (Business Wire 2016).[5] Recent estimates suggest that the global insurance market collected approximately $2 billion in cyber insurance premiums and that this will rise by a magnitude of three to five times by 2020 (Business Wire 2016). Cyber insurance, therefore, is one of the biggest areas of growth among insurers, and organizations, in turn, are increasingly purchasing cyber insurance to deal with these new risks.

---

3. Different legal theories used by victims of data breach include (1) common law tort and contract claims, (2) constitutional privacy claims, (3) state and federal statutory claims, and (4) failure to notify claims under state data breach notification statutes.

4. In 2013, cyber insurance policies sold to retailers, hospitals, banks, and other businesses rose 20 percent according to Marsh LLC, a New York insurance brokerage firm that tracks the market (Fernandes 2014).

5. For insurance, the loss ratio is the ratio of total losses incurred (paid and reserved) in claims plus adjustment for expenses divided by the total premiums earned. Thus, if the loss ratio is 65.2 percent, it means that for every $100 million collected in premiums, the insurance companies are paying out approximately $65 million to policyholders.

Despite the increased attention on data theft and cyber insurance, there has been little research directed toward the role that insurance and, in particular, insurance institutions play in constructing the meaning of compliance with privacy laws and dealing with data breach. Drawing from participant observation and ethnographic interviews at cyber insurance conferences across the country, in addition to content analysis of cyber insurance policies, loss prevention manuals, cyber insurance risk management services, and webinars, my data suggest that insurance companies and institutions, through cyber insurance, go well beyond simply pooling and transferring an insured's risk to an insurance company or providing defense and indemnification services to an insured; rather, my data suggest that cyber insurers are also acting as *compliance managers*.

By offering a series of risk management services developed within the insurance field, insurance institutions actively shape the way organizations' various departments tasked with dealing with data breach, such as in-house counsel, information technology, compliance, public relations, and other organizational units, respond to data breaches. Cyber insurance provides a pathway for insurance institutions to act as external compliance overseers and managers of organizational behavior with respect to data theft. Given the underpreparation and compliance by businesses, I conclude that institutionalized risk management techniques developed within the insurance field can potentially improve organizational practices and compliance concerning data breach, but may have some potential drawbacks as well.

RISK-BASED AND NEW INSTITUTIONAL APPROACHES TOWARD STUDYING ORGANIZATIONAL COMPLIANCE WITH LAW

Consistent with the global turn away from command-and-control regulation and toward more public-private partnerships and self-regulation, insurance scholars are increasingly discussing the role of private insurance as a form of regulation over individuals and organizations (Ben-Shahar and Logue 2012; Talesh 2015b). Insurance policies often take the form of private legislation or regulation through a wide variety of exclusions and conditions. To that end, insurance companies play an important role by shaping policy language and also communicating ideas about what law means to organizations tasked with complying with and implementing various legislative and regulatory mandates. Broadening this frame, Baker and Simon explore how institutions address compliance concerns by "governing through risk" or "[using] formal considerations about risk to direct organizational strategy and resources" (Baker and Simon 2002, 11). This concept includes not only the use of risk-based principles by insurance companies, but also the use of insurance technologies and concepts to govern risk outside of insurance institutions (Baker and Simon 2002; Ewald 2002; Heimer 2002).

In particular, scholars examining these issues across a variety of contexts note that insurance develops templates to regulate behavior in ways that are potentially more precise than some forms of governmental control (Ben-Shahar and Logue 2012). Through policy language, pricing, and risk management services, liability

insurance companies actively engage in loss prevention and try to influence the behavior of actors and organizations (Heimer 2002; Ericson, Doyle, and Barry 2003; Baker 2005; Baker and Griffith 2010; Ben-Shahar and Logue 2012; Abraham 2013). Insurers, and insurer risk management techniques, manage moral hazard in property and fidelity relationships (Heimer 1985), govern security in the home (O'Malley 1991), impact the motion picture industry in the United States (Hubbart 1996–1997), influence risk management approaches toward campus drinking (Simon 1994), and encourage better policing practices (Rappaport forthcoming).

Recent work in this area pivots away from how policy language acts as a form of regulation to focusing on the processes and mechanisms through which insurers engage in risk regulation and the extent to which insurance institutions influence or induce compliant behavior with laws and regulations. Here, empirical findings are much more mixed; although insurers offering directors and officers insurance have an opportunity to influence the behavior of directors and officers and discourage wrongful or even illegal behavior, they seldom do (Baker and Griffith 2010).[6]

More recently, insurance scholars have drawn from new institutional organizational sociology studies to explain how insurance institutions mediate the meaning of compliance through a logic of risk operating within the insurance field. Prior new institutional research reveals how managerial conceptions of law anchored around concepts of rationality, efficiency, and discretion broaden the term *diversity* in a way that disassociates the term from its original goal of protecting civil rights (Edelman, Fuller, and Mara-Drita 2001), transform sexual harassment claims into personality conflicts (Edelman, Erlanger, and Lande 1993), deflect or discourage complaints rather than offering informal resolution (Marshall 2005), and even shape the way public legal institutions such as legislatures (Talesh 2009, 2014), courts (Edelman, Uggen, and Erlanger 1999; Edelman 2005, 2007; Edelman et al. 2011), and arbitration forums (Talesh 2012) understand law and compliance. Drawing from new institutional studies, I show how the insurance field frames the legal environment of employers around concerns of risk (Talesh 2015a,b).

For example, through employment practice liability insurance (EPLI), insurance companies play a critical and as yet unrecognized role in mediating the meaning of antidiscrimination law (Talesh 2015a,b). Faced with uncertain legal risk concerning potential discrimination violations, insurance institutions elevate the risk and threat in the legal environment and offer EPLI and a series of risk management services that build discretion into legal rules and mediate the nature of civil rights compliance. In this setting, risk and managerial values work in a complementary manner because the insurance field uses risk-based logics to encourage employers to engage in managerial responses such as developing policies and procedures.[7]

6. Directors and officers liability insurance (often called "D&O") is liability insurance payable to the directors and officers of a company, or to the organization itself, as reimbursement for losses or advancement of defense costs in the event an insured suffers such a loss as a result of a legal action brought for alleged wrongful acts in his or her capacity as a director and/or officer.

7. Although there are a few new institutional studies in this area that frame risk in terms of litigation threat, new institutionalists have yet to engage in a comprehensive exploration of the processes through which risk narratives influence the meaning of compliance (Edelman, Abraham, and Erlanger 1992; Dobbin et al. 1993; Schneiberg and Soule 2005; Edelman 2016).

This study continues in this recent tradition of marrying new institutional studies of compliance and sociolegal studies of risk and moves into an area largely unexplored by scholars: privacy law and data theft. Prior research in this area focuses on the role that privacy officers play in shaping compliance with privacy law without focusing on cyber insurance and the role that insurance companies play as managers of the compliance behavior of organizations (Bamberger and Mulligan 2015). My study bridges the new institutional and insurance and risk literatures. In particular, I import the governing through risk approach into new institutional studies of law and organizations by revealing how risk management services and risk-based logics that are institutionalized within the insurance field influence what organizations are told privacy laws mean and how they are told to respond to data breaches.

METHODOLOGY

My research design evaluated how, through cyber insurance, participants in the insurance field, that is, insurance companies, claims administrators, brokers, agents, risk management consultants, underwriters, product managers, in-house counsel, and insurance attorneys, respond to data breach issues and influence the meaning of compliance with cyber security and privacy laws. A series of subquestions guided my inquiry: (1) How does the insurance industry shape the way that organizations respond to data theft breaches and the accompanying privacy laws? (2) How does the insurance industry characterize the objectives of privacy laws? (3) How does the insurance industry characterize the problem of data theft (cyber security)? and (4) How do formal considerations of risk impact the way that the insurance field responds to cyber security threats?

To answer these questions, I gained entry into the emerging field of cyber insurance, which is not easily accessible to social science research. I used different sources of data from a variety of locations.[8] Obtaining data from a variety of sources (participant observation, interviews, and content analysis) was particularly important because I was trying to map an aspect of the insurance field, cyber insurance, that is largely nascent and in its early stages of development. Because I do not have data on how cyber insurance impacts actual organizational behavior, or whether cyber insurance and the risk management services that insurers offer lead to less data theft, my data focus is on how the insurance field frames compliance with privacy laws and how it attempts to prevent data theft from organizations.[9]

8. Because unfettered access was unrealistic and preliminary inquiries revealed that industry officials were resistant to formal in-depth interviews, I triangulated through participant observation, ethnographic interviewing, and extensive content analysis.

9. Despite these limitations, the increasing purchase of cyber insurance by organizations and the plethora of insurer risk management tools that are emerging and examined by this study and my fieldwork suggest, at least preliminarily, that organizations are finding insurer-based compliance management useful.

Participant Observation at Cyber Conferences

I attended four national conferences on cyber insurance over a period of two years. Cyber conferences are three days long, occur two to three times a year, and bring together various actors engaged in employment practices liability to discuss important issues in the field. These conferences have been occurring for approximately ten years. Cyber conferences are where the majority of actors involved in drafting, marketing, buying, and selling cyber insurance engage one another. Cyber conferences allowed me to observe the field and to explore how various organizational actors think about data breaches and privacy laws, to document what logics or frames were dominating the discourse as participants discussed cyber insurance, and to explore how field actors use and market cyber insurance as a mechanism through which organizations can better comply with privacy laws.

Cyber liability insurance conferences were typically held at hotels. Approximately fifty to seventy-five insurance field actors attended these conferences. Panel sessions occurred daily and brought attendees together in one conference room.[10] I observed approximately thirty-one panel sessions on cyber insurance. Conference rooms were set up much like classrooms, with a podium and table for discussants in the front of the room and rows of tables and chairs for audience members.

Webinars

I also observed, transcribed, and coded cyber insurance webinars administered by risk management consultants and brokers, insurance industry and cyber security experts, and attorneys. These webinars simultaneously market cyber insurance and educate webinar participants on what cyber insurance is, educate participants on how cyber insurance is used, and highlight the various risk management services that are provided to organizations that purchase cyber insurance. Similar to conferences, cyber insurance webinars allowed me to explore how various organizational actors discuss the interplay between insurance, data theft, and privacy laws.

Content Analysis from Primary Sources: Cyber Insurance Policies and Risk Management Services

Unlike most lines of insurance, insurance companies offering cyber liability insurance also offer accompanying risk management services to address a wide variety of problems that organizations experience when data breaches occur. Cyber insurers rely heavily on offering organizations either the risk management services they have or the services of third-party vendors with whom they contract. I reviewed over thirty different risk management services offered by insurers and third-party vendors. These data proved to be a key area of focus for this research project. Researching the risk management services was important because it

10. There was never more than one panel session going on at a time.

revealed how the insurance industry acts as a compliance manager well beyond the traditional services that the insurance industry offers. I also reviewed industry reports and executive summaries by risk management consultants who conduct research on the kinds of cyber liability insurance coverage offered by insurers. In addition to these reports, I also obtained and evaluated cyber insurance policies. While most EPLI policies have similar provisions, some vary with respect to the type of specific first- and third-party coverage offered.

Ethnographic Interviews

My observations at the annual cyber conferences allowed me to identify various field actors and to pursue informal, ethnographic interviews. Ethnographic interviewing is a type of qualitative research that combines immersive observation and directed, one-on-one interviews (Spradley 1979). Because these interviews occur in the interviewees' natural settings while they are performing their normal tasks, the interviews are less formal. While at the conferences, I conducted twenty-two ethnographic interviews with field actors. These interviews varied in length from five to thirty minutes and generally involved eliciting opinions about the interplay between cyber insurance and various privacy laws from (1) insurance agents, (2) brokers, (3) claims administrators, (4) insurance company executives, and (5) attorneys.

Coding

Following standard procedures and protocols for qualitative research, data analysis proceeded from coding, to developing conceptual categories based on the codes, to defining the conceptual categories, and, finally, to clarifying the links between the conceptual categories (Fielding 1993; Charmaz 2001; Lofland et al. 2005). I first open coded (Lofland et al. 2005). Under this coding approach, written data from field notes and insurance industry documents were coded line by line (Charmaz 2001). I initially created some preliminary substantive coding categories around actors encountered in the field, activities observed in the field, and variation in written cyber security materials produced by insurance actors. Focused coding (Charmaz 2001) led me to refine my coding into analytic categories and to identify how risk-based principles and values filter the way that insurance actors discuss compliance with privacy laws. To add a layer of formality, transparency, and systematization to my coding process, I used qualitative coding software (ATLAS.ti) to code my written materials, interviews, and field notes (Fielding 1993).

While no one method used in this study provides enough data to reveal conclusive findings, I am confident that triangulating across multiple sites and examining different data points led to reliable findings. Unlike prior studies of insurance as regulation and insurer risk management, I am studying a field that is largely immature and changing in real time. Insurance scholars, therefore, would benefit from

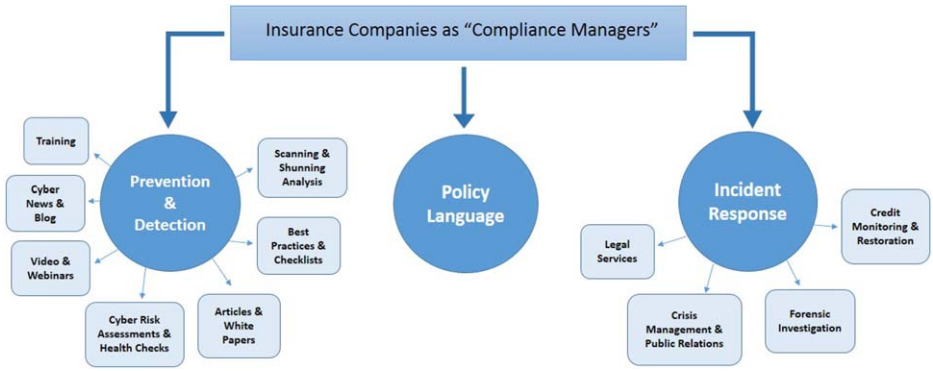

FIGURE 1.
How the Insurance Field Influences the Meaning of Compliance with Privacy Law and Cyber Security Threats [Color figure can be viewed at wileyonlinelibrary.com]

replicating this study in another ten years to see to what degree insurer risk management in this area has evolved and to what degree such techniques are impacting organizational responses to data breaches and privacy law more generally.

INSURANCE INSTITUTIONS AS COMPLIANCE MANAGERS OF DATA THEFT BREACHES AND PRIVACY LAWS

The following explores how insurance companies and institutions, through cyber liability insurance, actively shape the way an organization's various departments tasked with dealing with data breach, such as in-house counsel, information technology, compliance, public relations, and other organizational units, respond to data breach. I find that cyber insurers are acting as compliance managers aimed at preventing, detecting, and responding to data breaches and complying with various privacy laws. Through policy language and risk management services, insurance companies and the third-party vendors with whom they contract to assist insureds absorb the responsibilities of the legal counsel, compliance, public relations, and information technology departments for organizations with a series of additional risk management services. Figure 1 highlights how insurance companies shape the nature of compliance through expansive policy coverage and risk management services. In addition to policy language, the insurance field uses a series of mechanisms aimed at preventing, detecting, and responding to data theft.

Cyber Insurance—Beyond Risk Transfer of Defense and Expenses

Analysis of various cyber insurance policies reveals that this insurance is an important intervention in the insurance market because it expands coverage to insureds for losses specifically excluded by other lines of insurance. When data breach issues arose about a decade ago, policyholders fought, largely

unsuccessfully, with commercial general liability (CGL) and property insurers over coverage.[11] Modern CGL policies specifically exclude electronic data from the definition of property damage, which means that the only form of coverage that CGL policies can provide is associated with liability from physical damage to hardware, which is unusual in most cyber incidents. Property insurance and other lines of insurance also exclude coverage for losses associated with data breach.

Cyber insurance eliminates potential denials of coverage that often occur under other lines of insurance and provides a source of risk transfer. Cyber insurance is similar to homeowner and automobile insurance and some other lines of insurance because it covers a very broad scope of losses. In particular, cyber insurance policies provide both first-party coverage (the policyholder insures her own interest in her body or property) and third-party coverage (which pays proceeds to a third party to whom an insured becomes liable) for data breach events. Thus, cyber insurance often covers the loss of personal information regardless of how the data were lost or stolen. Although the scope and breadth of coverage varies among insurers, this insurance tries to shift risks for the costs associated with having to respond, investigate, defend, and mitigate against the consequences surrounding a cyber attack.

Cyber insurance covers the liability that flows from the loss, such as lawsuits filed by individual victims or from business partners that experience harm as a result of the data breach. In other words, cyber liability insurance protects the insured from actual or potential liability and litigation defense expenses to a third party as the result of a cyber event, such as damages arising from the theft of personal identification information, identity theft, third-party network interruption, third-party security failures, and cyber extortion. Cyber liability insurance also covers the insured's own costs to notify and monitor the credit of the victims, perform a forensic investigation, and handle the public relations campaign to maintain and restore the public's trust in the organization. Figure 2 highlights the broad coverage provided in most cyber insurance policies.

Although cyber insurance provides defense and indemnification for a broader scope of coverage, cyber insurance is not all-encompassing. Because the cyber insurance market is so new, brokers and underwriters struggle with evaluating how to price and evaluate the risk of loss.[12] As a result, some insurers offering cyber insurance limit their coverage to under $20 million and often insist on sizable deductibles. Moreover, cyber insurance does not cover all harms associated with cyber attacks, such as payments of ransom to unlock malware, the direct costs to reputation, and the direct costs of data destruction. Nonetheless, my fieldwork reveals that organizations view cyber insurance policies favorably because far more coverage is provided now than previously existed when insureds were forced to try to claim coverage under other lines of insurance. As the next section shows, the expansive coverage creates space for insurers to offer their risk management services to combat the various risks that they insure.

11. A CGL insurance policy is often issued by business organizations to protect them against liability claims for bodily injury and property damage arising out of premises, operations, products, and completed operations. Property insurance provides protection against most risks to property, such as fire, theft, and some weather damage. This includes specialized forms of insurance such as fire insurance, flood insurance, earthquake insurance, home insurance, or boiler insurance.

12. Specifically, underwriters that I spoke with indicated that they do not have enough data to make educated determinations on payout estimates.

Third-Party Coverage: The third-party insurance component typically covers:

- Wrongful disclosure of personally identifiable information, protected health information, or confidential corporate information in the client's care, custody, or control via a computer network or offline via laptop, paper, records, and disks
- Failure of computer network security to guard against threats such as hackers, viruses, worms, Trojan horses, and denial of service attacks, whether or not resulting from the provision of professional services
- Content liability risks such as defamation and infringement of intellectual property rights arising out of Web site, marketing, and advertising activities
- Security or privacy breach regulatory proceedings, including associated fines and penalties
- Media content coverage, addressing claims related to the creation and distribution of material
- PCI fines and penalties resulting from noncompliance with PCI data security standards

First-Party Coverage: The first-party insurance component typically covers:

- Network business interruption: loss of income and extra expense due to network security failure
- Intangible property: costs to restore or re-create data or software resulting from network security failure
- Loss of income due to failure of network security
- Breach response and associated management costs

Legal Fees: Costs to hire lawyers to assist with notification in the event of a data breach and to defend lawsuits following such notification

Forensic Investigation and Restoration Costs: Cost to investigate and contain the extent of a data breach, including the costs to retain information security forensics experts; in particular, most policies cover the costs incurred by the policyholder to identify the source of the breach, to contain the breach, and ultimately to restore network processes that may have been damaged as a result of the breach event

Crisis Management and Public Relations: Covers the costs to retain the services of a public relations firm and crisis management firm for advertising or related communications to protect and to restore the policyholder's public reputation following a breach event

Business Interruption: Covers lost income and related costs where a policyholder is unable to conduct business due to a data breach event beyond a specified waiting period

Credit Monitoring/Call Center Expenses: Covers the costs of credit monitoring, fraud monitoring, or other related services to customers affected by a data breach event; in addition, it covers the cost to set up call centers to respond to customer concerns and inquiries

Cyber Threat Extortion Expenses: Covers the reasonable and necessary expenses incurred by the policyholder to protect against credible threats by hackers, including payment of monies demanded by extortionists

FIGURE 2.
Third-Party and First-Party Coverage Under Cyber Insurance

Risk Management Services: Mechanisms Through Which Insurers Seek to Influence the Form of Compliance

My research in the field reveals that insurance institutions are doing something more than transferring risk—they are actively managing the underlying risk of data breach. The lack of organizational preparation for and response to data breaches and the overall undercompliance with privacy laws is a gap being filled by the insurance field and the various value-added services that cyber policies offer. Unlike in the directors and officers liability insurance context (Baker and Griffith 2010), where insurers had an opportunity to engage in loss prevention but failed to do so, cyber insurers actively engage in loss prevention and fill the roles previously held by internal departments within an organization such as legal, compliance, information technology, and crisis management.

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:

> Buyers of cyber insurance are purchasing accessibility to vendors that the insurance company has. It is a partnership as we connect to the relationship of the insurance company. We are not just buying [insurance] coverage. (Conference panel, insurance consumer, lines 56–59)
>
> We've partnered with vendors to bring expertise to our insureds and make sure that they have the most current tools available to help keep them ahead of the curve. (CyberEdge Strategic Partnership Series, introduction, lines 16–18)
>
> We offer a proposition, a package [of services] that the insured gains access to. (Interview, insurance agent, line 87)
>
> We see this as a mutually beneficial relationship. The insurance company gets the business and the insured becomes a better risk. (Interview, insurance company official, lines 78–80)

Twenty-two of the thirty-one panels I observed at cyber insurance conferences mentioned or discussed the value of the various risk management services that accompany the cyber insurance policy. Thus, cyber insurance—through the risk management services that come with the insurance—provides a pathway for insurance institutions to gain influence over organizational decision making relating to compliance issues surrounding data breach and privacy. As one insurance industry official noted, "We act like a quarterback of the data breach response and try to steer the response in the right direction" (Insurance official, Panel 8, lines 125–26). The following highlights in more detail the mechanisms through which the insurance field attempts to shape and influence how organizations deal with data loss and the accompanying privacy laws.

Insurer Risk Management Services Focus on Preventing and Detecting Data Breaches and Influencing the Form of Compliance

Unlike in the directors and officers professional liability context (Baker and Griffith 2010), cyber insurers engage in considerable risk and loss *prevention*.

Insurance companies either have in-house departments or contract with third-party organizations that offer a series of services aimed at preventing data breaches and violations of privacy laws from ever occurring. In doing so, insurers absorb many of the functions of the organizations in terms of preventing these risks.

Risk prevention begins with a series of assessments, or what one insurer calls "cyber health checks." The goal of these checks is to "give organizations a 360 degree view of their people, processes and technology, so they can reaffirm that reasonable practices are in place, harden their data security, qualify for network liability and privacy insurance, and bolster their defense posture in the event of class action lawsuits" (NetDiligence 2015). Another risk management assessment tool focuses on cyber security best practice standards for categories such as (1) current events, (2) security policy, (3) security organization, (4) asset classification and control, (5) personnel security, (6) physical and environmental security, (7) computer and network management, (8) system development and maintenance, (9) business continuity planning, (10) security compliance, (11) Internet liability, and (12) privacy and regulatory compliance (NetDiligence 2015). This particular intervention assesses data security strengths and weaknesses, and includes a data security score for each practice area. The goal is to measure the organization's practices and make sure they are consistent with the prevailing security standards. The health check is often followed by an independent, objective review of the organization's security and privacy practices.

Another insurer offers a risk prevention service called *scanning*, which analyzes the risks that an organization's security poses: "Scanning . . . detects and prioritizes hidden risks on public-facing infrastructures, provides a detailed view of a company's vulnerability status, priority vulnerabilities, and more" (AIG, CyberEdge Strategic Partnership Series, IBM security, lines 6–9). Typically, the insurer or the affiliated third-party vendor performs a remotely delivered scan of the organization's perimeter network devices such as the firewall, web server, and e-mail servers to mitigate vulnerabilities and stave off potential attacks. They also test the effectiveness of existing firewalls and web servers. Insurers framed these services as unique and value added, well beyond what many existing organizations had in terms of detecting cyber security breaches.

These risk prevention tools and security ratings play an important regulatory role over organizations. First, the scans and health checks are sometimes used as a precondition for determining whether a potential company is eligible for cyber insurance. Organizations interested in insurance protection, therefore, are often interested in becoming more cyber secure. Second, the better a company scores on its health check, the greater the likelihood the insurance company will lower its premiums.[13]

Coupled with risk prevention strategies, the insurance field also offers a series of services aimed at *detecting* data breaches before they are completed. These

13. To be fair, the market for cyber insurance is not mature enough to have the refined premium setting standards that exist with more established lines of insurance. Insurers, brokers, and underwriters simply do not have enough claims history. That said, brokers I spoke with indicated that the more cyber secure organizations are with good preventative tools in place, the more likely organizations would be issued insurance and receive a favorable pricing arrangement.

services include managing and tuning intrusion detection system technologies, managing host and network-based firewall technologies, managing security information and event management correlation technologies, and managing security service providers. Insurers often use third-party vendors that offer "shunning" services. This service uses intel and security technology to isolate and shun communications to and from IP addresses currently being used by criminals. The entire cyber security community that I studied repeatedly described these services as invaluable.

The insurance field also helps extend its preventive approach toward subcontractors and outside vendors with whom organizations contract to perform services. Here, the insurance field positions itself as an intermediary between formal privacy law and the need for organizations to interpret, implement, and comply with privacy laws properly. Panelists reminded attendees that an organization is potentially legally liable for its subcontractor's or vendor's data loss. Thus, organizations are increasingly trying to contract with vendors who are cyber secure. To ameliorate this legal risk, insurers offer services that help measure and monitor the networks of vendors with which an organization works. Insurers provide reports of the security practices of vendors and allow an organization to compare the practices of other vendors when the organization is considering using new or different vendors. Thus, insurers' services allow organizations to have continuous visibility into their vendors' security practices to ensure company data are safe, even when they are outside the organization's network.

Panelists at conferences suggest that the goal of the health check assessments is to evaluate the people, processes, and technology and to ensure that organizations have a foundation upon which to develop a stronger cyber risk management program. In doing so, the insurance company absorbs many of the functions of the information technology department and actively engages in loss prevention. In this vein, cyber insurers are similar to insurers offering EPLI (Talesh 2015a,b), but different than directors and officers insurance (Baker and Griffith 2010). Whereas directors and officers have an incentive to have defense and indemnification liability coverage, they are less eager to have outside actors and institutions (such as insurers) interfering with their day-to-day decision making and at times risky behavior. However, with cyber insurance, the incentives are better aligned. Given the financial, legal, and reputational harm, no organization benefits from a cyber attack. Thus, policyholders purchasing cyber insurance are interested in using these risk management tools to prevent and detect risks.

Insurer Risk Management Services Influence the Form of Compliance Through Written Training Materials and Telephone Hotlines

In addition to risk assessments and audits, insurers construct what compliance with privacy laws means through a series of written, value-added services. These documents also advise organizations on how to prevent and detect data breaches. Cyber insurers offer organizations hundreds of forms and documents, including access to cyber news and blogs, best practice checklists, monthly newsletters,

articles, whitepapers, videos, webinars, and legal summaries, including some that address new and amended privacy laws.

Like trainings conducted by employers (Bisom-Rapp 1996, 1999), cyber insurer loss prevention manuals and training sessions specifically guide organizations on how to avoid regulatory fines and liability for data breach. Creating and maintaining an incident response plan and team—many members of which are third-party vendors in contractual relationships with insurers—is reiterated repeatedly at conferences and in written materials provided to organizations. Cyber insurers also audit an organization's written policies, procedures, forms, and handbooks to determine whether they comply with federal, state, and local laws. These audits focus on interpreting and implementing privacy laws and preventing breaches and the resulting fines that are triggered by failing to comply with laws. In addition to these services, insureds have access to a website filled with tools and training to identify exposure to loss, develop and implement policies and procedures, train staff, and stay informed as the compliance issues continue to evolve. Like EPLI, cyber insurance tries to shape the nature of compliance (Talesh 2015a).

These written, value-added services can have potential positive and negative impacts on compliance. On the one hand, offering these services may reflect some best practices, prevent data theft breaches, and lead to improved compliance. More specifically, unlike in the EPLI context (Talesh 2015a), insurance company guidance on these issues does not largely focus on how to avoid litigation—but on how to prevent data theft losses in the first instance. On the other hand, these services make it easy for organizations to develop policies and procedures without actively drafting them.

Insurers also offer incident response hotlines aimed at identifying and preventing risk. These hotlines are made up of subject matter experts who know the latest vulnerabilities and the cyber risk landscape and are able to provide specialized knowledge to clients to ensure that their cyber infrastructure is secure. Whereas EPLI insurers offer a *legal* hotline that administers legal advice to employers that call (Talesh 2015a), cyber insurer hotlines focus on heightening the security systems of companies and preventing any data loss. As one insurer notes, the hotline is "where subject matter experts may be reached instantly to discuss potential indicators of compromise to determine if, and how, a compromise may have occurred, with advice on what immediate steps to take to address vulnerabilities and contagion" (AIG, CyberEdge Strategic Partnership Series, IBM security, lines 10–18). Cyber insurer risk management services, unlike EPLI insurer risk management services, are more focused on helping organizations avoid data breach and comply with privacy laws than mediating the meaning of law. Insurers are stepping into this vacuous space and trying to provide compliance guidance to organizations that have security systems unprepared for the latest cyber threats.

Thus, with respect to the cyber insurer's risk management services, risk and managerial logics complement one another. The insurance field adopts a managerialized conception of privacy law, which highlights the elaboration of organizations' formal structures that demonstrate compliance and rational governance. The insurance industry sells this vision by highlighting the risk of not developing policies and procedures as well as providing a safety net for organizations that includes a

series of risk management services in addition to defense and indemnification insurance coverage.

Cyber Insurance Provides a Pathway for Insurers to Manage the Legal Process, Forensic Investigation, and Credit Monitoring When a Data Breach Occurs

Perhaps the biggest intervention the insurance field makes is the array of risk management services it offers to shape the way that organizations *respond* in the event of an actual data breach. Traditionally, insurance covers legal defense and indemnification costs associated with a covered loss. In the cyber insurance context, insurers cover the legal, forensic, restoration, business interruption, crisis management, and credit monitoring expenses. I was surprised to learn, however, that cyber insurance goes beyond risk transfer in the defense and indemnification context because it also provides access to services aimed at responding to, investigating, defending, and mitigating against the consequences surrounding a data breach event or privacy law violation. Cyber insurers provide these risk management services, which organizations use to respond to data loss. Insurers either have departmental units that deal with various cyber-related problems or contract with third-party vendors that the insured can use. Typically, the insured receives a reduced premium to use the insurer's vendors. In this respect, cyber insurance provides not only risk transfer, but also risk response well beyond the scope of what insurers typically handle.

Typically, organizations facing a cyber violation have incident response teams that try to manage and coordinate the data security event investigation, response, reporting, and the corrective action taken. Panelists repeatedly describe the numerous voices that are part of the process:

> The incident response team is made up of the incident response team leader, the privacy officer, legal and risk management services department, information security, human resources, employee relations, patient relations, outside legal counsel who is often the breach coach, crisis management and public relations person, the forensics person and the insurance company or broker. The external team members such as outside vendors, privacy breach coach, forensics and outside counsel are part of the internal response. (Insurance official, Panel 21, lines 123–29)

My research reveals that the insurance company, through the risk management services it offers with cyber insurance, largely drives the company's incident response when a data loss occurs. Many of the members of the incident response team have direct relationships with the insurance company.

In particular, many organizations purchasing this insurance express how efficient it is to have one-stop shopping in the event of a data breach (cf. Talesh 2015a). Through this close partnership with the insured, insurers gain influence over the organization's compliance process. In particular, the insurance company

offers a menu of services that an organization can quickly access in the event of a data breach. According to private organizations, the most helpful aspects of cyber insurance are the risk management services:

> These services can actually be quite robust and innovative. Finally, insureds are able to tap into a built-in network of IT experts, PR firms and legal counsel experienced in cyber matters, which brings an enormous amount of value to the coverage. (Andrews interview, ABA, April 1, 2015)

> We use the insurance company as a resource for our decision making. (Insured, Panel 6, line 10)

Insurers offer insured organizations access to a designated panel of lawyers and law firms that can assist in managing the legal issues that arise when a data loss incident occurs. These law firms help organizations to prepare for and respond to data security incidents. In addition to defending lawsuits, lawyers are particularly important because they assist with complying with various privacy laws and regulatory provisions largely geared toward making sure consumers are notified in a timely manner that there is a data breach. Because of the variation in consumer notification laws in forty-seven states, lawyers assist policyholders in evaluating which state laws have been triggered and what steps the insured must take following a data breach event.

Lawyers are clearly viewed as leaders for data breach response. Panelists repeatedly refer to the lawyer who is retained as the "breach coach." In particular, policyholders participating on panels indicate that they like being able to contact a lawyer who has been vetted by the insurer: "Cyber insurance is a great product because of the pre and post breach services. My first [phone] call is to the breach coach" (Insured, Panel 6, line 112). They also like that communications thereafter concerning the breach are privileged. Typically, panelists noted that the breach coach plays a critical and primary role in developing and managing the incident response team that is formed when a data breach occurs. Moreover, these lawyers provide twenty-four-hour access to the organization's incident response lawyers through an 800 number. While I am not suggesting that in-house counsel does not play any role, it appears that the insurance-sponsored law firm retained by an organization plays a greater role in many instances. These lawyers and law firms are relied on in part because they are repeat players and have developed significant experience handling clients experiencing data loss.

When a company's cyber security system is breached, an immediate concern is identifying the source and cause of the data breach, containing the breach, and ultimately restoring network processes that may have been damaged as a result of the breach. Addressing these problems often requires an information security cyber expert. Cyber insurers or their third-party vendors offer forensic experts to organizations. My fieldwork reveals almost unanimous support for the insurer's ability to provide rapid access to these forensic services: "A key post-breach service includes mitigating harm and having a forensic investigator help the firm" (Hudson 2015). One forensic investigator I interviewed highlights how insurers provide access to

key forensic services: "Firms really want us to come in and clean things up when a breach occurs and our relationship with the insurer makes it easier for the firm to access our services" (Forensic investigator interview, lines 43–45). Cyber insurers not only provide the insured access to these vendors, but they also cover the costs to investigate the cause of the data breach, restore the network processes to normal, and retain information security forensics experts. Similar to the legal expertise coming from the insurance company, insurance companies are also the primary source for forensic expertise.

As noted earlier, another big threat organizations face when a breach occurs is damage to its reputation. A study conducted by the Economist Intelligence Unit in 2013 found that more than one-third of customers of companies that suffer a data breach refuse to continue doing business with that company in the future (Beazley 2016). Cyber insurance addresses this risk by covering the costs to retain the services of a public relations and crisis management firm. However, cyber insurers go beyond providing coverage by offering a series of preapproved public relations and crisis management firms that the insured can retain at a reduced premium. These crisis management and public relations firms play a crucial role in developing and providing advertising or related communications to protect and restore the insured's reputation following a data breach event. The experience of the public relations vendor the insurer is able to provide under tense circumstances was repeatedly touted as value-added at conferences: "When a breach occurs, an organization needs to respond really quickly. Look at Target. So much damage to their reputation. The public relations people know how to manage and finesse those situations" (Insurance industry official interview, lines 110–13).

Finally, the other major response organizations often face when a data breach violation occurs is dealing with consumers whose financial information is stolen. In such situations, millions of people are at risk of credit card and identity theft by hackers. Financial institutions, retail stores, and credit card companies that experience breaches of consumer information often have to set up credit monitoring and restoration services for consumers. This typically includes establishing a call center for consumers to respond to customer concerns and inquiries concerning the data breach event. Cyber insurance provides access to companies experienced in credit monitoring and restoration that organizations can use for a reduced fee. Cyber insurance also covers the costs of credit and fraud monitoring and costs associated with setting up call centers to respond to customer concerns and inquiries as a result of data loss.

In sum, in an environment in which organizations are undercomplying with privacy laws and underprepared for potential data breach events, cyber insurers have stepped in as intermediaries and are acting as compliance managers. Cyber insurers are doing much more than pooling and spreading risk. Cyber insurers heavily influence organizations' data breach and privacy law response teams. In addition to providing defense and indemnification for losses resulting from data breaches, insurers are involved in the legal, forensic, information technology, credit monitoring, and public relations decisions relating to a data breach event. Insurers either offer the insured their risk management services or access to their networks of third-party vendors that specialize in dealing with these issues. By offering a

series of risk management services developed within the insurance field that are aimed at preventing, detecting, and responding to cyber security breaches, insurance institutions actively shape the way organizations respond to data theft.

CONCLUSION

This study elaborates the literature on the relationship between organizations and law by blending new institutional organizational sociology studies of how organizations respond to legal regulation and sociolegal insurance scholars' studies of how institutions govern through risk. In particular, my study bridges these two theoretical frameworks by revealing how in the context of cyber insurance, insurers go well beyond pooling and spreading risk and act as compliance managers for organizations dealing with cyber security threats. Although prior new institutional studies of law and organizations emphasize the way that managerial values influence the nature of law and compliance among organizations, governing through risk provides an alternative framework by showing how risk management services and risk-based logics that are institutionalized by the insurance field influence what organizations are told privacy laws mean and how they are told to respond to data breach. Consistent with prior studies that blend governing through risk and the managerialization of law, concerns over risk and the need for adequate policies and procedures drive the process at every stage. Thus, risk and managerialized values work in tandem.

My multisite, multimethod approach also enhances prior studies of insurance as regulation by revealing *how* the insurance field governs through risk and uses considerations of risk and insurance services to influence organizational strategy and decision making. Whereas early work celebrates insurance as regulation and focuses on the forms and functions of insurance, more recent studies of directors and officers, employment practices liability, and cyber insurance focus on the conditions under which insurance shapes regulatory behavior in positive and negative ways.

Given the range of findings from these studies, scholars need to think of the benefits of insurance as regulation on a continuum. Insurance as regulation does not always work, nor does it always fail. Although more research is clearly needed, it appears there are a couple of distinctions between EPLI, directors and officers insurance, and cyber insurance. For example, prior work in the directors and officers context shows how the insurance industry has the ability to engage in loss prevention behavior but does not try to engage in such behavior (Baker and Griffith 2010). In the cyber context, the insurance industry does try to engage in loss prevention and does so in a manner that is focused on managing and averting the risks associated with data breach. One likely difference is that in the directors and officers context, directors and officers are less eager to be told how to engage in risk-averse behavior. Policyholders in the cyber context, however, are interested in the insurance defense and indemnity coverage, but also the accompanying risk management services that can prevent, detect, and respond to a data breach event. The risk management services that accompany cyber insurance also fill a competency or knowledge gap for the organization. Organizations are willing to use risk

management tools that deal with the latest cyber threats that they lack internal tools to defend against. Conversely, directors and officers believe they possess the requisite knowledge and experience to manage a corporation responsibly and are less eager to receive insurance risk management recommendations.

Moreover, whereas prior research shows that EPLI insurers spend considerable time trying to shape the meaning of law for employers tasked with dealing with discrimination laws (Talesh 2015a), here, cyber insurers spend far less time mediating law's meaning and far more time trying to enhance an organization's ability to detect and respond when faced with a data breach. Thus, unlike in the EPLI context, the insurance risk management tools are less about simply avoiding being sued and more about developing processes to prevent or limit any data breach problem from occurring. Therefore, the conditions under which insurance as regulation works depends on a variety of factors. Taken collectively, however, research on directors and officers insurance, EPLI, and the cyber liability insurance context reflect a significant shift in the manner in which insurers actively shape the nature of compliance.

From a policy standpoint, this study raises important questions about the role of insurance in regulating cyber security theft. Although prior research highlights how insurance acts as a form of social control on society (Baker and Simon 2002; Baker and Griffith 2010; Ben-Shahar and Logue 2012; Abraham 2013), important questions remain concerning whether insurers should regulate organizational behavior and if they do regulate behavior, how that authority is exercised. Similar to human resource officials, in-house counsel, and managers (Edelman, Erlanger, and Lande 1993; Edelman, Fuller, and Mara-Drita 2001), my data suggest that the insurance field's involvement as an intermediary may be a mix of benefits and disadvantages.

On the one hand, to the extent organizations remain underprepared for cyber risks and undercompliant with privacy laws, insurance industry intervention in this area is very valuable. The risk management tools offered encourage and, to some extent, force stronger detection and security protocols in organizations and nudge organizations toward greater safety and security. In turn, this makes consumer information less likely to fall into the hands of wrongdoers. Cyber insurance and risk management services such as the audits, hotlines, and online portals of handbook materials provide substantive guidance on privacy law and on organizations' responsibilities. To the extent that the information provided to organizations is accurate in these settings, these services could be compatible with compliance and could even induce greater compliance. Moreover, the postbreach services allow organizations to turn to one place and address all their concerns. Unlike other financial institutions that also offer risk management services related to data breach, insurance companies are able to package these services with insurance litigation defense and indemnification in the event of an actual breach.

On the other hand, overreliance on cyber risk management systems may allow organizations to avoid more active engagement with the design, content, enforcement, and maintenance of their policies. By encouraging organizations to use insurer-sponsored forensics, information technology, public relations units, and hotlines, the insurance field shifts or decouples responsibility for hard normative

judgments to others (such as insurance companies) operating outside the organization (cf. Bisom-Rapp 1996, 1999; Edelman, Fuller, and Mara-Drita 2001). Insurance companies have an obvious financial incentive in seeing more customers purchase cyber insurance and the accompanying risk management services. Insurance industry services that diminish an organization's individual responsibility to design its cyber security policies and procedures may diminish organizational responsibility for making moral, ethical, and legal choices involved with compliance (cf. Baker and Simon 2002). To the extent organizations can simply delegate their data breach events to the insurers and accompanying risk management vendors, cyber insurers may enhance the possibility that organizations are lethargic in taking ownership of compliance policies and procedures and, consequently, preventing privacy laws from making a greater impact.

Obviously, future research on whether cyber insurance leads to less data theft would help to gauge the value of these insurer-sponsored risk management services. Assuming insurer risk management services reduce the likelihood that data breach events will occur, my data suggest, at least preliminarily, that there is a net benefit. Existing research suggests that organizations are currently unable to keep up with cyber threats. Thus, despite insurers' financial incentives, insurer-sponsored help is greatly appreciated by organizations and the consumers whose information is potentially exposed.

At a minimum, this study highlights the processes and mechanisms through which insurers act as private risk regulators (Ben-Shahar and Logue 2012). Regulation over privacy and cyber security issues in the United States remains fragmented and incomplete. The insurance industry is stepping in and trying to offer organizations a pathway for dealing with cyber threats and the abundance of privacy laws. Law is typically thought of as top down, coming from public legal institutions such as courts, legislators, and regulatory institutions. However, consistent with new legal realist and the law and society studies, how organizations implement laws and comply with various rules is shaped by intermediary institutions such as insurance companies.

Cyber risk management services do not just reduce risk; they actively construct the meaning of compliance. As shown in the employment and consumer protection contexts (Edelman, Uggen, and Erlanger 1999; Talesh 2009, 2012), these responses are becoming institutionalized and gaining legitimacy. In particular, public legal institutions are deferring to and encouraging organizations to purchase cyber security insurance.

The Department of Homeland Security's National Protection and Programs Directorate recently convened working sessions and roundtables with the insurance industry to discuss ways to make public and private institutions more cyber secure. While acknowledging that the cyber insurance market is relatively nascent as compared to other lines of insurance, the Department of Homeland Security's report concluded that cyber insurance is vital: "A robust cybersecurity insurance market could help reduce the number of successful cyberattacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection" (DHS 2017). Moreover, the report devoted extensive attention

toward improving risk management within organizations, the very kinds of services cyber insurance companies are offering (Department of Homeland Security 2014). Thus, it appears that insurance institutions are shaping the content and meaning of cyber security compliance.

Moving forward, this article suggests that there is great potential for constructive linkages between studies on risk management and law and organizations. More research on how risk-based logics are mobilized by intermediaries and mediate the way organizations deal with cyber security threats and comply with privacy laws would help strengthen organizational theory and reveal how, in action, the meaning of compliance is often constructed by legal intermediaries.

REFERENCES

Abraham, Ken. 2013. Four Conceptions of Insurance. *University of Pennsylvania Law Review* 161: 653–98.

Armerding, Taylor. 2015. "Compliance Fatigue" Sets In. *CSO Online*. http://www.csoonline.com/article/2899612/compliance/compliance-fatigue-sets-in.html (accessed December 11, 2015).

Bamberger, Kenneth, and Deirdre Mulligan. 2015. *Privacy on the Ground*. Cambridge, MA: MIT Press.

Baker, Tom. 2005. *The Medical Malpractice Myth*. Chicago: University of Chicago Press.

Baker, Tom, and Sean J. Griffith. 2010. *Ensuring Corporate Misconduct: How Liability Insurance Transforms Shareholder Litigation*. Chicago: University of Chicago Press.

Baker, Tom, and Jonathan Simon, eds. 2002. *Embracing Risk: The Changing Culture of Insurance and Responsibility*. Chicago: University of Chicago Press.

Beazley. 2016. *Data Breach*. https://www.beazley.com/specialty_lines/data_breach.html (accessed January 20, 2016).

Ben-Shahar, Omri, and Kyle D. Logue. 2012. Outsourcing Regulation: How Insurance Reduces Moral Hazard. *Michigan Law Review* 111:197–248.

Bisom-Rapp, Susan. 1996. Scripting Reality in the Legal Workplace: Women, Lawyers, Litigation Prevention Measures, and the Limits of Anti-Discrimination Law. *Columbia Journal of Gender and Law* 6:323–85.

——. 1999. Bulletproofing the Workplace: Symbol and Substance in Employment Discrimination Law Practice. *Florida State University Law Review* 29:959–1049.

Business Wire. 2015. HSB Study Shows 69 Percent of Businesses Experienced Hacking Incidents in the Last Year; Cyber Poll Finds Risk Managers Not Confident About Resources Dedicated to Combat Hacking. *Business Wire*, June 3.

——. 2016. Fitch: U.S. Cyber Insurance Premiums Total $1B per New Supplemental Filing. *Business Wire*, August 24.

Charmaz, Kathy. 2001. Qualitative Interviewing and Grounded Theory Analysis. In *Handbook of Interview Research: Context and Method*, ed. Jaber F. Gubrium and James Holstein, 675–94. Thousand Oaks, CA: Sage.

Department of Homeland Security. 2014. *Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues*. Insurance Industry Working Session Readout Report. Washington, DC: Department of Homeland Security.

DHS, 2017. Cybersecurity Insurance. https://www.dhs.gov/cybersecurity-insurance (accessed April 23, 2017).

Dobbin, Frank, John Sutton, John Meyer, and Richard Scott. 1993. Equal Employment Opportunity Law and the Construction of Internal Labor Markets. *American Journal of Sociology* 99: 396–427.

Edelman, Lauren B. 2005. Law at Work: The Endogenous Construction of Civil Rights. In *Handbook of Employment Discrimination Research: Rights and Realities*, ed. Laura Beth Nielsen and Robert L. Nelson, 337–52. Boston: Kluwer Academic Press.

——. 2007. Overlapping Fields and Constructed Legalities: The Endogeneity of Law. In *Private Equity, Corporate Governance and the Dynamics of Capital Market Regulation*, ed. Justin O'Brien, 55–90. London: Imperial College Press.

——. 2016. *Working Law: Courts, Corporations & Symbolic Civil Rights*. Chicago: University of Chicago Press.

Edelman, Lauren B., Steven E. Abraham, and Howard S. Erlanger. 1992. Professional Construction of the Legal Environment: The Inflated Threat of Wrongful Discharge Doctrine. *Law & Society Review* 26:47–83.

Edelman, Lauren B., Howard S. Erlanger, and John Lande. 1993. Employers' Handling of Discrimination Complaints: The Transformation of Rights in the Workplace. *Law & Society Review* 27:497–534.

Edelman, Lauren B., Sally Riggs Fuller, and Iona Mara-Drita. 2001. Diversity Rhetoric and the Managerialization of Law. *American Journal of Sociology* 106:1589–1641.

Edelman, Lauren B., Linda H. Krieger, Scott Eliason, Catherine Albiston, and Virginia Mellema. 2011. When Organizations Rule: Judicial Deference to Institutionalized Employment Structures. *American Journal of Sociology* 117:888–954.

Edelman, Lauren B., Christopher Uggen, and Howard S. Erlanger. 1999. The Endogeneity of Legal Regulation: Grievance Procedures as Rational Myth. *American Journal of Sociology* 105: 406–54.

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

Ewald, Francois. 2002. The Return of Descartes's Malicious Demon: An Outline of a Philosophy of Precaution. In *Embracing Risk: The Changing Culture of Insurance and Responsibility*, ed. Tom Baker and Jonathan Simon, 273–301. Chicago: University of Chicago Press.

Fernandes, Deirdre. 2014. More Firms Buying Insurance for Data Breaches. *Boston Globe*. http://www.bostonglobe.com/business/2014/02/07 (accessed February 17, 2014).

Fielding, Nigel. 1993. Ethnography. In *Researching Social Life*, ed. Nigel Gilbert, 154–71. London: Sage.

Heimer, Carol. 1985. *Reactive Risk and Rational Action: Managing Moral Hazard in Insurance Contracts*. Berkeley: University of California Press.

——. 2002. Insuring More, Ensuring Less: The Costs and Benefits of Private Regulation Through Insurance. In *Embracing Risk: The Changing Culture of Insurance and Responsibility*, ed. Tom Baker and Jonathan Simon, 116–45. Chicago: University of Chicago Press.

Hubbart, E. O. 1996–1997. When Worlds Collide: The Intersection of Insurance and Motion Pictures. *Connecticut Insurance Law Journal* 3:267–304.

Hudson, David L. 2015. Cyber Liability Insurance Is an Increasingly Popular, Almost Necessary Choice for Law Firms. *ABA Journal* April:22–23.

Identity Theft Resource Center (ITRC). 2016. Identity Theft Resource Center Breach Report Hits Near Record High in 2015. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html (accessed November 20, 2016).

Lofland, John, David Snow, Leon Anderson, and Lyn Lofland. 2005. *Analyzing Social Settings*, 4th ed. Belmont, CA: Wadsworth.

Lovelace, Berkeley. 2016. Cost of Data Breaches Hits $4 Million on Average: IBM. http://www.cnbc.com/2016/06/14/cost-of-data-breaches-hits-4-million-on-average-ibm.html (accessed June 15, 2016).

Marshall, Anna-Maria. 2005. Idle Rights: Employees' Rights Consciousness and the Construction of Sexual Harassment Policies. *Law & Society Review* 39:83–124.

Munro, Dan. 2015. Data Breaches in Healthcare Totaled Over 112 Million Records in 2015. *Forbes*. http://www.forbes.com/sites/danmunro/2015/12/31data-breaches-in-healthcare-total-over-112-Million-Records-in-2015. (accessed December 31, 2015).

NetDiligence. 2015. *Cyber Risk Assessments*. https://netdiligence.com/portfolio/assessment/ (accessed December 2015).

O'Malley, Pat. 1991. Legal Networks and Domestic Security. *Studies in Law, Politics and Society* 11:171–90.

Podolak, Gregory D. 2015. Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges. *Quinnipiac Law Review* 33: 369–409.

Ponemon Institute. 2015. *Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data*. Traverse City, MI: Ponemon Institute.

——. 2016. *Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations*. Traverse City, MI: Ponemon Institute.

Rappaport, John. Forthcoming. How Private Insurers Regulate Public Policy. *Harvard Law Review* 130.

Schneiberg, Marc, and Sarah Soule. 2005. Institutionalization as a Contested, Multi-Level Process: The Case of Rate Regulation in American Fire Insurance. In *Social Movements and Organization Theory: Building Bridges*, ed. Gerald F. Davis, Doug McAdam, W. Richard Scott, and Mayer N. Zald, 122–60. Cambridge: Cambridge University Press.

Simon, Jonathan. 1994. In the Place of the Parent: Risk Management and the Government of Campus Life. *Social & Legal Studies* 3:15–45.

Spradley, James. 1979. *The Ethnographic Interview*. Belmont, CA: Wadsworth Group/Thomas Learning.

Talesh, Shauhin. 2009. The Privatization of Public Legal Rights: How Manufacturers Construct the Meaning of Consumer Law. *Law & Society Review* 43:527–62.

——. 2012. How Dispute Resolution System Design Matters: An Organizational Analysis of Dispute Resolution Structures and Consumer Lemon Laws. *Law & Society Review* 46:463–96.

——. 2014. Institutional and Political Sources of Legislative Change: Explaining How Private Organizations Influence the Form and Content of Consumer Protection Legislation. *Law & Social Inquiry* 39:973–1005.

——. 2015a. Legal Intermediaries: How Insurance Companies Construct the Meaning of Compliance with Antidiscrimination Laws. *Law & Policy* 37:209–39.

——. 2015b. A New Institutional Theory of Insurance. *U.C. Irvine Law Review* 5:617–50.