The Evolution of Cyber-Insurance Industry and Market: An Institutional Analysis

By: Nir Kshetri

Kshetri, Nir (2020). "The Evolution of Cyber-Insurance Industry and Market: An Institutional Analysis", *Telecommunications Policy*, September, 102007.
https://doi.org/10.1016/j.telpol.2020.102007

Abstract:

The *cyber-insurance (*CI) market is at a nascent stage. This paper investigates how the contexts provided by formal and informal institutions affect the development of the CI industry. It highlights the nature, origin, and implications of CI-related institutions and provides insights into the mechanisms and forces that can lead to institutional changes. It offers an explanation as to how different institutional pillars related to CI progressively evolve and reinforce one another. Such a mechanism is likely to influence a range of demand and supply side factors and create a system that can accelerate the growth of the CI industry and market. The paper also investigates how contradictions generated by CI, the formation of dense networks and changing power dynamics can trigger regulative normative and cognitive changes. Since the current analysis of the causes and consequences of institutions and institutional change is mainly concerned with more established economic sectors, this paper is expected to provide insights into institutions surrounding to this new and rapidly evolving industry.

Keywords: Cyber-insurance | Cybersecurity | Institutional change | Institutional fields | Institutions | Standardization

Article:

1. Introduction

Cyber-insurance (CI) is emerging as an important tool to protect organizations against future cyberattack-related losses. Some recent observations have highlighted many complexities and challenges in the CI market. Different insurers' CI products often include different combinations of alternative features. This makes difficult for buyers to compare values of policies they are getting and price (Insurance Journal, 2017).

Most businesses have not yet realized the importance of CI. An estimate indicated that in 2017, while over 75% large businesses in certain categories had CI compared to less than 5% of small and medium-sized enterprises (SMEs) (Aon Benfield, 2017). A survey conducted among businesses in the U.K. in the early 2020 found that 32% of had CI (MacRae, 2020). Likewise, as of 2020, less than 20% of small businesses in the U.S. had bought CI (Grzadkowska, 2020).

At the root of these problems is a lack of standardization and common vocabulary and language in the CI industry. An additional problem is that some insurers underwrite only specific types of cyber-risks. However, the types of liability policyholders are facing is rapidly changing (O'Nell, 2018).

The newness and associated uncertainties have contributed to misunderstanding and confusion among insurers and policyholders. Consider the following example of an insurer-policyholder dispute: In June 2017, the international food company, Mondelez International was victimized by the NotPetya cyberattack, which is an encrypting ransomware first found in 2016. The attack affected Mondelez's 1700 servers and 24,000 laptops, which became permanently dysfunctional. Mondelez claimed that its loss due to property damage, disruption in commercial supply and distribution, inability to fulfill customer orders, reduced margins, and other losses exceeded US$100 million (https://tinyurl.com/y8yn7yuq). Mondelez filed a claim with its insurer-- Zurich American Insurance Company-- for these damages.

Zurich offered an initial payment of US$10 million but later rejected the claim altogether. It argued that NotPetya ransomware was an act of "cyber war" and thus was not covered by the policy (Lindsey, 2019). According to Zurich, the policy excludes "hostile or warlike action in time of peace or war" by a "government or sovereign power" (McCarthy, 2019).

An upshot of disputes such as this is the involvement of legislative, regulatory and judiciary agencies. Mondelez sued Zurich for breach of contract (Ferland, 2019). As of March 2020, the litigation had been ongoing (Clarke, 2020).

Recent newspaper editorials have also asked policymakers to reflect on the need of CI. When a ransomware attack disrupted software company Talman Software's operations in March 2020, which processed 75% of wool sales in Australia and New Zealand, an editorial argued that regulations that make it mandatory for companies to have CI could be a way to minimize the disruption (Musotto & Naser, 2020).

Just like the practices of industry bodies such as the American Insurance Association in traditional insurance products (Holyoke, 2003), trade groups representing insurers offering CI have engaged in lobbying strategies and tactics to secure policy outcomes that favor their interests. As an example, the Insurance Council of New Zealand (ICNZ) lobbied for better reporting and more access to data. In a hearing to Parliament's Justice Select Committee on the Privacy Bill, its Chief Executive argued that a register of data breaches with aggregated, anonymized data would help businesses and insurers better understand the issues (Walters, 2018).

Examples such as the above show clearly that CI-related rules, norms and standards are not well developed. Indeed, many examples exist of such confusion and disagreements regarding what a given CI premium would cover (Table 1). The participation, discourses and practices of diverse actors such as policymakers, insurers, trade/industry associations, and policyholders are shaping, and are likely to continue to shape the evolution of CI. Institutional theory can provide important insights into this phenomenon. Specifically, this theory helps us understand, explain and

contextualize the interests, motivations and actions of various actors that participate in the CI industry and market.

Table 1. Some cases of cyberattack losses refused to be covered by cyber-insurers.

Organization	Cyberattack faced	Losses	Amount paid by insurer
The National Bank of Blacksburg (the U.S.)	Faced two separate cyberattacks (May 2016 and January 2017).	$2.4 million (unauthorized withdrawals at hundreds of ATMs).	Offered US$50,000 (Jdouri, 2018).
Equifax	2017: 147 million consumers' data stolen	US $242.7 million by April 2018 (digin, 2018). (expenses including customer support and legal fees)	US$50 million covered by insurance (Condon, 2018).
Target	December 2013: cyberattacks compromised 40 million credit and debit-card accounts and 70 million customers' personal data (Yadron, 2014).	Costs exceeded US$450 million (DeFranco, 2017).	Insurance covered US$100 million.
Merck	June 2017: NotPetya cyberattack	Lost US$260 million of sales (2017) US$320 million for additional marketing and production. Expected to lose another US$200 million of sales in 2018	Received US$45 million from its insurers by March 2018 (the final total could be up to US$275 million (Ralph, 2018).
P·F. Chang's	2014: Hackers gained access to the payment systems and breached 60,000 credit card numbers, which were posted online (Baukes, 2016).	Costs of the breach: US$1.7 million, paid US$1.9 million to Bank of America Merchant Services Payment Card Industry's (PCI) assessment (McDaniels, 2017).	Insurer Chubb paid US$1.7 million to cover costs from the breach but not the PCI fine. The court ruled in favor of Chubb (Baukes, 2016).
Ameriforge Group	May 2014: lost US$480,000 in an email scam that impersonated the firm's CEO.	Asked insurer, Chubb to cover the entire loss	Chubb refused to cover (Boddy, 2017).

This paper thus attempts to provide an institutional explanation for the currently nascent but rapidly growing CI industry and market. Specifically, it addresses the following research question: What are the mechanisms and nature of the evolution of institutions that shape the CI industry and market?

A main contribution of this paper is that it increases our understanding of CI, which is an under-investigated research area. Such an understanding would help organizations navigate the complex, and rapidly evolving CI landscape and manage cyber-risks more effectively. Another contribution is to make a connection between CI and institutional theory. It provides an understanding of various institutional actors, their actions as well as how they are shifting from the standpoint of CI.

The paper is structured as follows. It proceeds by first providing a brief overview of CI. Then it looks at institutions and institutional field in the context of the CI industry and market. Next, key mechanisms of institutional changes in the CI industry and market are discussed. It is followed

by a section on discussion and implications. The final section provides concluding comments on institutions' effects on the CI industry and market.

2. A brief overview of CI

CI provides coverage for the theft or loss of first-party and third-party data. As to the first-party data, an insurer may cover expenses related to notifying customers regarding a data breach, purchasing credit monitoring services for affected customers and launching a public relations campaign to restore the company's reputation. Third-party coverage includes claims related to unlawful disclosure of a third-party's information and infringement of intellectual property rights (IPR) (natlawreview.com, 2014). This type of CI protects businesses that are responsible for a client's cybersecurity. CI helps them to pay for lawsuits if their actions or the lack of an action leads to a data breach on a client's system (techinsurance.com, 2020). Some examples of companies that need third-party CI include web hosting businesses, IT consultants, software and app developers, security consultants and website designers (insureon.com, 2020).

CI expresses a cyber-risk in terms of a dollar value. The CI underwriting process can thus help identify CS gaps and provide opportunities for improvement. Understanding how CI functions and the costs of CI premium will help organizational decision makers increase the effectiveness of cybersecurity budgeting process (National Conference of State Legislatures, 2020).

CI is offered as a standalone service and as well as add-ons to other insurance policies. For instance, insurers such as American International Group (AIG) sell personal CI policies as add-ons to homeowners' and renters' insurance. AIG also offers a standalone CyberEdge policy. In 2019, 46 insurers wrote standalone CI products worth US$1.11 billion in direct premiums (Grones, 2019). Likewise, a survey conducted by insurance broker Gallagher found the proportion of businesses in the U.K with standalone CI policy to be 18% (Gangcuangco, 2020b).

2.1. Rapidly growing and maturing CI market

The global market research company Allied Market Research put the size of global CI market at US$4.85 billion in 2018, which is expected to reach US$28.60 billion by 2026 (Allied Market Research, 2020). Likewise, according to the investment bank, RBC Capital Markets, the global CI market was US$6 billion in 2019, which will reach US$15 billion by 2022 (Ralph, 2019).

CI differs from more established insurance products in terms of regulatory, industry, and market factors. The CI market is currently thin in the sense that there are lower numbers of buyers and sellers and fewer transactions compared to more traditional insurance products such as home and auto. The number of carriers offering CI worldwide was fewer than 50 in 2015 (Meckbach, 2019). By 2017, about 50 companies offered CI only in the EU (Stupp, 2017). In the U.S., about 200 insurers offered CI in 2019 (Ralph, 2019). Nonetheless this number is much lower compared to over 900 insurers that offered medical coverage (Price, 2020).

The CI market is developing toward higher maturity levels. For instance, management's awareness of cyber-risk has increased. There is less confusion and a higher degree of clarity regarding what is covered in a CI. Companies are also addressing so-called silent cyber-risk. An

increasing number of insurance contracts explicitly include cyber coverage, which used to be "silent" under other policies before (Trice, 2019). Consequently, the overlap between cyber coverage and more traditional policies is decreasing. Underwriters and brokers are also more clearly outlining protection from different types of cyberattack losses (spglobal.com, 2020).

3. Institutions and institutional changes

Institutions are "macro-level rules of the game" (North, 1990, p. 27), which include: a) formal institutions such as rules, laws, constitutions; and b) informal institutions such as social norms, conventions and self-imposed codes (North, 1996).

Scott (2001) proposed three institutional pillars: (i) regulative; (ii) normative and (iii) cultural-cognitive. The normative and cultural-cognitive pillars can be mapped to North's (1990) informal institutions whereas regulative pillar is related to formal institutions.

3.1. Institutional pillars

In this section, Scott's (2001) three pillars are first explained and illustrated with some CI-related examples.

3.1.1. Regulative institutions

Regulative institutions consist of "explicit regulative processes: rule setting, monitoring, and sanctioning activities" (Scott, 1995, p. 35). In the context of this paper, regulative institutions consist of existing laws and rules that affect CI. To take an example, the rapid growth in the European CI market can be primarily attributed to the risks associated with European Union's General Data Protection Regulation (GDPR) compliance (Cohn, 2018). Some jurisdictions such as the state of California are moving towards making CI as a legally sanctioned requirement.

Prior research conducted in complex problems has indicated that policy measures play a key role in shaping the trajectory of an industry (Ericson & Kessler, 2013, 2016; Van der Veen & Tagel, 2011). In developmental and socio-economic issues such as food security, policy measures can be applied to ensure the affordability of products and services and increase the availability of inputs (Van der Veen & Tagel, 2011). Governments can achieve similar outcomes in CI industry as well. For instance, the government can make it mandatory for all insurers to offer CI. The increased competition is likely to have positive effects on the availability and affordability of CI. Government policies can also help increase the availability manpower, data and other key inputs required for the CI sector.

3.1.2. Normative institutions

Normative institutions introduce "a prescriptive, evaluative, and obligatory dimension into social life" (Scott, 1995, p. 37). This component is linked to morality and social conventions (Scott et al., 2000). The basis of compliance in the case of normative institutions is related to professional and social obligations.

Normative institutions also include trade/professional associations (e.g., the ICNZ), industry groups or non-profit organizations that can use social/professional obligation requirements (e.g., ethical codes of conduct) to induce certain behaviors in the CI industry and market. An association's norms, informal rules, and codes of behavior can create order, without the law's coercive power, by relying on a decentralized enforcement process where noncompliance is penalized with social and/or economic sanctions (North, 1990). For instance, non-adherence to codes of trade associations may result in sanctions such as losing membership in a trade association (Kshetri & Dholakia, 2009).

Trade and professional associations also engage in activities to create awareness of CI and provide insights about the CI industry and market. The Council of Insurance Agents & Brokers, which is an association for regional, national and international commercial insurance and employee conducts *Cyber Insurance Market Watch Survey* on a bi-annual basis. The survey is designed to provide insights into factors affecting the CI market's growth (Ciab, 2018).

These associations may also engage in lobbying and related activities. As noted above, the ICNZ which represents 28 members that collectively write more than 95% of all fire and general insurance in New Zealand, argued that better reporting and more access to data would help the CI industry's growth. In order to understand this better, the idea of “subject positions” of an institutional actor is helpful (Maguire et al., 2004). Compared to industry bodies such as ICNZ, the government's “subject positions” is more dominant, which can allow it to take measures to require organizations to report cyberattacks and develop cyber-threat databases.

Professional and trade associations also play an important role in strengthening the regulative institutions (Kshetri & Dholakia, 2009). For instance, they can work with the state to develop new regulatory framework appropriate for the growth of the CI market.

3.1.3. Cultural-cognitive institutions

Cultural-cognitive institutions are ‘‘the shared conceptions that constitute the nature of social reality and the frames through which meaning is made’’ (Scott, 2001, p. 57). They deal with “recognizable, taken-for-granted” behaviors (Scott et al., 2000, p. 238).

In this paper's context, the most relevant issue concerns organizational decision makers' assumptions and beliefs about CI. In this regard, Table 2 provides the findings of some representative surveys regarding the perception of CI. According to a survey conducted by Deloitte, the lack of understanding of CI options and the perceived unaffordability have acted as key barriers for CI adoption (Friedman, 2017). In addition, most companies have never filed CI claims. They thus exhibit limited understanding of the processes to file a claim. They might be concerned and worried about the lack of sufficient “due care” leading to a fear that their claim could be denied (Covington, 2016).

Another relevant aspect is that most brokers lack CI-related expertise (Gerhards, 2018). Compared to other insurance products, for CI brokers, technical understanding of cyberattacks is more important than selling skills (Grzadkowska, 2019).

Table 2. Organizations' perceptions of CI: Some representative surveys.

Survey conducted by	Conducted/ released in	Major findings
Marsh & McLennan Companies conducted in Asia-Pacific including East Asia, South Asia, Southeast Asia and Oceania	2017	49% of respondents had "insufficient knowledge" about their cyber risk exposures to assess the type and coverage of insurances they need (Marsh & McLennan Companies, 2017).
Ponemon Institute with 2168 individuals in North America, Europe, the Middle East, Africa, Asia Pacific, Japan and Latin America. The respondents are involved in their company's cyber risk management and enterprise risk management activities	2017	Only 24% had CI. Main reasons for not purchasing CI: premiums too expensive (36%), inadequate coverage (36%), property and casualty policies sufficient (30%); too many exclusions, restrictions and uninsurable risks (27%) (aon.com, 2017)
Research firm Ovum for Silicon Valley analytics firm FICO with 350 c-suite executives and senior security officers from financial services, telecommunications, healthcare, retail, e-commerce and media service providers in the U.S.	Mid-2017	50% lacked CI and 27% had no plans to buy CI. Only 25% believed CI premiums rightly reflect the risk profile of organizations, only 23% believed that insurers are clear and transparent in their approaches to pricing; 29% wanted insurers to provide clear guidelines about the choice of premiums, 28% want clearer communications regarding premium adjustments, 23% would like to see an industry standard for benchmarking cyber-risks (Insurance Journal, 2017).
Fox Rothschild LLP	2018	70% of executives said their companies had CI but only 21% had ever filed a claim (Gerhards, 2018).
U.K. legal expenses insurer DAS UK Group, and HSB Engineering (March 2018 with 250 brokers)	Mid-2018	31% admitted that they had a "poor" or "very poor" understanding of cyber-risks and CI. Most important thing insurers can do to support them: making policies simpler (23%), providing better explanation of policies (19%) and better training for brokers (15%). (Insurance Journal, 2018).
IT industry networking organization Spiceworks.	Early 2019	Only 7% with CI had filed a claim. 62% lacked CI. Top reasons for not carrying CI: not a priority at their organization (41%), lack of budget (40%), lack of knowledge about CI (36%), and CI not required by regulations (34%), not sold on the benefits of CI (33%), insufficient use cases (20%), not confident claims would be paid out 12% (Ashford, 2019).
UK Government's survey of 1/566 businesses and 514 registered charities in the U.K.	April 2019	Those with CI that have made an insurance claim (3% of businesses and 12% of charities). Reasons for not having CI: already covered by external cyber security providers: 23% businesses, 26% charities; lack of awareness of CI: 23% businesses and 15% charities; considered themselves as being at too low of a risk: 29% charities and 22% businesses (Ross, 2019).

It is important to understand that cognitive programs are built on mental maps of potential policyholders. Put differently, cognitive systems influence the lens (Scott, 2001) through policyholders view and interpret CI and its benefits as well as different aspects of CI such as fairness of premiums charged, complexity/clarity of CI policies, and the level of confidence that claims would be paid out (Table 2). For instance, surveys conducted by research firms such as Ponemon Institute and Ovum found that it is a common perception among many policyholders that CI premiums are higher than could be justified based on the cyber-risks they face (Table 2).

3.2. Institutional field

An institutional field is “formed around the issues that become important to the interests and objectives of specific collectives of organizations” (Hoffman, 1999, p. 352). For the CI industry, this institutional field includes **issues raised by** national governments, industry bodies, trade and professional associations as well as insurers, and organizations that are concerned about cyberattacks directed against their networks. The “content, rhetoric, and dialogue” (Hoffman, 1999, p. 355) among these constituents influence the field related to CI.

Regarding a field's evolution, institutional theorists argue that a field is a dynamic system characterized by the entry and exit of various players and constituencies with competing interests and disparate purposes and a change in interaction patterns among them (Barnett & Carroll, 1993). These players continuously negotiate over issue interpretation and engage in what is referred to as “institutional war” (Greenwood & Hinings, 1996).

As an example, regulators and consumers have emphasized the importance of standardization. Industry bodies, on the other hand have been pointing out difficulties associated with standardization efforts. The Association of British Insurers (ABI), the voice of the U.K.‘s insurance and long-term savings industry, argued that it is “misguided … to attempt to impose standards on CI, especially one that is in its relative infancy and one that needs flexibility to respond to an ever-changing cyber risk landscape” (professionalsecurity.co.uk, 2019).

Likewise, some insurers have refused to cover social engineering frauds (Row, 2018). Note that in social engineering frauds, cybercriminals use emotional appeals such as fear, pity or excitement to victimize Internet users by luring them to give their credentials, click malicious links or download files containing malware. They may establish interpersonal relationships or create a feeling of trust and commitment in order to achieve these goals.

Similarly, in a 2013 cyberattack case, an insurer refused to cover losses because the policy arguably applied only to property damage and the insurer argued that electronic data was not “tangible property” (Boddy, 2017). A 2019 report also noted that most CI policies only cover losses of “tangible assets” such as damaged or stolen hardware and costs associated with forensic investigations (McIntosh, 2019). Over time, insurers are likely to have an increased understanding and appreciation of cyber-risks. Moreover, needs of policyholders may change, which is likely to change this discourse.

Many CI policies contain a condition that requires the policyholders to be payment card industry data security standard (PCI DSS) compliant at the time the breach (businessinsurance.com, 2014). Note that the PCI DSS is an information security standard intended for organizations handling branded credit cards such as Visa, MasterCard, American Express, JCB and Discover. A major goal of the standard is to reduce credit card fraud. It is administered by the Payment Card Industry Security Standards Council. Being fully compliant with the standard is a difficult task, which makes it hard to obtain a full reimbursement of losses (Hare-Brown, 2019; ITIJ, 2018). Indeed, this has been a major source of dispute between insurers and policyholders (e.g., P.F. Chang's and Chubb, Table 1).

Prior researchers have noted that fields evolve through three stages (Purdy & Gray, 2009, Table 3). The CI industry is probably in mobilization stage. For instance, insurance companies are promoting fear and anxiety about possible cyberattacks to sell CI products. They claim that they would cover losses associated with cyberattacks.

Table 3. Evolution of institutional field around CI.

Stage	Explanation	Meaning in the CI context
Stage 1: Innovation	New logics are introduced and are drawn into the debate.	CI was at this stage in the 1990s, when insurers started to provide CI as an add-on to existing policies mainly for technology, media and telecommunications companies and in 2000s when many insurers started explicitly adding clauses to exclude CI in existing policies (Verdict, 2020)
Stage 2: Mobilization	Complex power dynamics among institutional actors	Insurers. policyholders, regulators and other actors compete to validate and implement their logics.
Stage 3: Structuration	Logics are translated into practices (Reay et al., 2006). Norms and structures are standardized (Covaleski & Dirsmith, 1988).	CI not reached at this stage.

Some organizations, on the other hand, argue that insurers tend to take advantage of legal loopholes and look for excuses not to pay cyberattack-related losses. Many companies think that their limited resources may be better spent on backing up important data rather than paying for CI. Many chief information security officers (CISOs) complain that CI only gives a "false sense of control" and should not be "trusted at face value" (Boddy, 2017).

Policyholders have a tendency to switch insurance providers (Johns, 2017). In this regard, the competition is becoming more intense in the CI industry. Companies find it easier to change CI providers. In this way, policyholders' relative power vis-a-vis insurers is likely to increase. Policyholders can leverage this increased power to force providers to take measures to enhance CI services such as by providing coverages for new types of risks.

4. Institutional changes shaping the CI industry and market

4.1. Contradictions associated with CI and institutional changes

A simple approach to understand institutional changes would be to look at the various contradictions and dilemmas that CI produces with the existing institutional arrangements, which are likely to shape decision-making processes of key institutional actors. We first introduce the concept of organizational isomorphism, which is "a constraining process that forces one unit in a population to resemble other units that face the same set of environmental conditions" (DiMaggio & Powell, 1983). Isomorphism is positively related with legitimacy (Deephouse, 1996). Organizations thus try to exhibit isomorphism with respect to external institutional pressures by adopting structures and processes (Scott, 1987). If other institutional actors perceive that practices of an organization have strong similarities to industry norms, the organization is viewed as more desirable (Suchman, 1995). Organizations, however, often have multiple constituents and hence different types and sources of legitimacy. Each constituent may evaluate

the legitimacy of an organization based on the organizational activity most relevant to the concerns of the constituent (Deephouse, 1996; Suchman, 1995).

Institutional theorists view this as accumulated results of continuous isomorphic adaptations of organizations (Burns & Nielsen, 2006). If we look from this viewpoint, institutional changes can be seen as an outcome of the dynamic interactions of contradictions and "praxis" (Seo & Creed, 2002, p. 222). That is, institutional actors continuously engage in the process of enactment, embodiment and interpretation of theories, lessons and skills.

Table 4 presents how various contradictions and incompatibilities are leading to changes in actions of regulators and (potential) policyholders. First, conformance to the existing institutions may be at the expense of technical and functional efficiency (e.g., not being able to cover losses associated with a cyberattack due to the lack of CI), which is likely to act as a force of institutional changes. For instance, all the U.S. states except for two require car insurance (Bay, 2020). However, regulations requiring CI have not yet been developed. This situation is changing. In February 2020, a bill was introduced in the California State Assembly (Assembly Bill 2320), which would require any business that has access to personal information and contracts with the state to maintain CI coverage (Hobson & Adams, 2020). Lawmakers are thus realizing that the "status quo" is ineffective to fight the rapid rise in cyberattacks.

Table 4. Some examples of CI-related contradictions and incompatibilities leading to institutional changes.

Institutional actor	Current situation	Response favoring the growth of CI	Institutional change mechanism (Seo & Creed, 2002)
Regulators	The "status quo" (no laws requiring CI) is ineffective to fight the rapid rise in cyberattacks.	Some jurisdictions (e.g., the state of California in the U.S.) are introducing legislations that require CI. Newspaper editorials have asked policymakers to reflect on the need of CI (Musotto & Naser, 2020).	Legitimacy undermining functional efficiency.
Organizations/ policyholders	Organizations only facing smaller cyberattacks, may not realize the need for CI	Rapidly rising data breach costs may increase financial stress associated with cyberattacks: change in the perception of the importance of CI	Adaptation weakening adaptability
	Institutional pressures from shareholders: increasing profitability and lowering costs (no CI)	Pressures from business partners require them to buy CI (Harrington, 2017).	Isomorphism conflicting with divergent interest
	Businesses may carry limited or no CI coverage in jurisdictions that do not make CI mandatory.	new laws are being proposed in some jurisdictions, which require them to have CI	Intra-institutional conformity leading to inter-institutional incompatibilities

Some big companies attacked by Petya/NotPetya such as Maersk and FedEx lacked CI (reinsurancene.ws, 2018). They suffered significant economic losses. Maersk's loss exceeded

€350 million (Stupp, 2017). Cyber-incidents such as this would change decision-makers' cognitive lenses with which they view CI. For instance, organizations in which a discourse about efficiency and cost saving become taken for granted, there are possibilities of resistance for ideas related to buying CI products. Big losses such as this may change the way companies view CI. This means that what was considered to be logically compatible or congruent practice some years ago (e.g., not spending on CI) is viewed as incompatible or incongruent today. Seo and Creed (2002, p. 226) refer to this type of contradiction as "legitimacy that undermines functional efficiency". That is, not buying CI in an attempt to increase profitability to gain legitimacy with shareholders may actually **lead to more adverse** consequences in case of a big cyberattack.

A key point to note here is that what is currently taken-for-granted, which is embedded in practices, may change through time (Colyvas & Powell, 2006). An organization's understanding of the effectiveness of a practice (e.g., buying vs. not buying CI) may change. For organizations such as FedEx and Maersk, the economic ramifications of not being (fully) insured become well understood when they face cyberattacks.

When organizations only face smaller cyberattacks, they may not realize the need for CI. Data breach costs are rapidly rising. According to IBM Security's, 2019 Cost of Data Breach Report, the total average cost of a cyberattack on organizations was US$3.92 million (IBM Security, 2019). Over time, financial stress associated with cyberattacks can be large enough to exceed the threshold of tolerance.

A related point is that substantial economic losses have occurred due to cyberattacks on some big companies. For instance, cyberattacks on Equifax and Merck resulted in economic losses that were estimated to exceed US$1 billion (reinsurancene.ws, 2018). Organizations may find it difficult to cover such big losses and adapt to such changes without CI. Seo and Creed (2002, p. 226) refer this phenomenon as "adaptation that undermines adaptability" in which "adaptive moves make adopters less able to adapt over the long run".

Third, to gain legitimacy, organizations may need to appease multiple institutions that are conflicting and inconsistent. This type of contradiction is referred as "isomorphism that conflicts with divergent interests" which may act as a trigger for institutional change (Seo & Creed, 2002, p. 226). For instance, organizational decision makers face institutional pressures for legitimacy from shareholders, which would often require increasing profitability. Such pressures translate to organizational objectives such as lowering costs. However, they also need to gain legitimacy with business partners. In this regard, an increasing number of companies require their business partners to buy CI (Harrington, 2017). Likewise, when organizations face coercive pressures from regulators, discourses related to efficiency and cost saving may become less powerful.

Finally, businesses in a jurisdiction may carry limited or no CI coverage, which is consistent with institutional arrangements in the jurisdiction. Such measures could be in conflict with the frameworks adopted by other jurisdictions that are proposing stricter cybersecurity laws or making it mandatory to have CI (Hobson & Adams, 2020). Legislations such as the California Consumer Privacy Act (CCPA) and the GDPR are forcing companies to increase the scope of CI coverage. Following the enactment of the CCPA, which became effective on January 1, 2020, more and more companies were reported to be buying CI (Stoller, 2020).

Such inconsistencies are described as “intra-institutional conformity that creates inter-institutional incompatibilities”, which are likely to bring about pressures for changes in organizations’ approaches to CI (Seo & Creed, 2002, p. 226). For instance, the third-party CI has a number of components such as litigation, regulatory response, credit monitoring services, crisis management, privacy and security liability, and network security liability. Especially the GDPR and the CCPA are expected to stimulate CI coverage related to regulatory response (Market Research Future, 2019). Likewise, the first party CI is composed of categories such as theft/fraud, forensic investigation, business interruption, electronic restoration and ransom/extortion. Among these components, legislations such as the GDPR and the CCPA are expected to have the largest impact on forensic investigation. This is because, to comply with these legislations, victim companies are required to collect, analyze and report data in legally admissible ways (Market Research Future, 2019).

4.2. Reinforcing effects of institutional components

An institutional pillar both reflects and determines the nature of the other pillars (Hayek, 1979). North (1994) observes that informal rules provide legitimacy to formal rules. Likewise, Axelrod (1997, p. 61) comments on the relationship between regulative and normative institutions: “Social norms and laws are often mutually supporting. This is true because social norms can become formalized into laws and because laws provide external validation of norms”.

Table 5. Institutional evolution in the CI industry.

Type of institutions	Effects on other institutional pillars	Explanation	Examples
Regulative	Cognitive	Measures to bring shift in the taken-for-granted interpretations of issues related to CI.	• New York's DFS urged financial companies to invest in CI. • The EU: ENISA is encouraging companies to buy CI
	Normative	Regulations as a driving force in the evolution of common norms and standards	• August 2013: adoption of the NIST's Cybersecurity Framework: The White House's emphasis on government agencies and the insurance industry to build better underwriting practices
Normative	Regulative	Engage in lobbying efforts to increase the growth of and reduce the risks to the CI industry	• The Insurance Council of New Zealand lobbied for better reporting and more access to data.
	Cognitive	Developing standards and facilitating customers' understanding of key aspects of CI	• Cyber Insurance Association's Cyber Insurance Forum in Zurich discussed about non-affirmative or silent cyber coverages
Cognitive	Regulative	Regulatory options to make insurers accountable	• Mondelez International's lawsuit against Zurich
	Normative	Demanding for industrial norms to govern the CI industry	• Ovum's survey: 23% would like to see an industry standard for benchmarking cyber-risks (Insurance Journal, 2017)

Prior research has also noted that the prohibition of a behavior can shape social norms regarding the behavior (Elster, 1989). For instance, a well-articulated prohibition against some behaviors (e.g., against operating businesses without CI) that has constitutional and moral legitimacy may lead to the development of certain organizational norms (e.g., purchasing CI policies).

From the above discussion it is apparent that the progress in each institutional component is likely to have a reinforcing effect on the other two, contributing to the growth of the CI industry. In addition, technological innovations are likely to shape the actions of various institutional actors. The key aspects of such relationships and mechanisms are presented in Table 5 and Fig. 1.

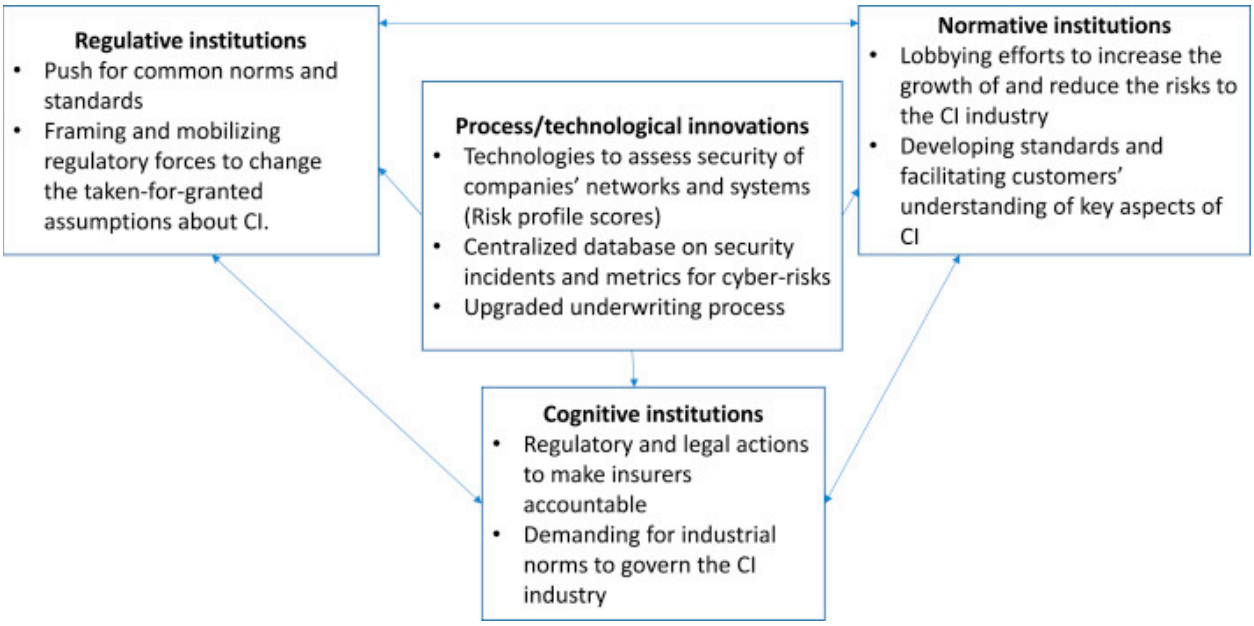

Fig. 1. Interrelationships among various institutions and the roles of process and technological innovations.

4.2.1. Effects of regulative institutions on other institutions

Framing and mobilizing regulatory forces to change the taken-for-granted assumptions about CI.

Governments can employ a wide variety of policy approaches and instruments to discourage or encourage certain behaviors of businesses and individuals (Ericson & Kessler, 2013). Especially a policy prohibiting certain behaviors (e.g., running a business without CI) needs to be considered and assessed in relation to moral issues and moral persuasiveness (Liberman et al., 2004). The way businesses and individuals perceive and respond to a policy and their willingness to comply are functions of how the policy is framed and articulated in relation to moral discourses (Ericson & Kessler, 2013). Businesses and individuals are likely to comply with a government policy (e.g., requirement to have CI) if they view that the policy is morally and constitutionally wrong.

Governments can use two approaches to discourage a behavior: a) prohibiting the behavior and enforcing it with a fine; b) taxing the behavior without prohibition (Ericson & Kessler, 2013).

These approaches may lead to different outcomes. Moreover, political actors and popular discourse affect individuals' understanding of a policy's "meaning, motivation, authority, and legitimacy" (Ericson & Kessler, 2016, p. 43). Ericson & Kessler's (2013) study of a government mandate to purchase health insurance in the U.S.-- the 2010 Patient Protection and Affordable Care Act (PPACA)-- indicated that political discourse plays a key part in influencing the public's perception of and willingness to comply with a policy. In an experiment, insurance purchase intentions increased by 10.6% when the PPACA was articulated as a mandate compared to a tax with the same monetary penalty for non-compliance (Ericson & Kessler, 2013). Thus, in order to be effective and successful, government policies related to CI need to be morally persuasive to individuals.

Through framing and subsequently mobilizing regulatory forces, regulators can change the taken-for-granted assumptions, beliefs and attitudes, organizational systems, processes, rules, and routines related to CI. New York's Department of Financial Services (DFS) urged financial companies to invest in CI. The idea is that just like the fire insurance has played roles in improving building codes, CI can help strengthen cyber-defense (Scannell, 2014). Framing the CI issue this way may lead to change in the taken-for-granted assumptions about CI among organizations.

Similarly, the EU cybersecurity agency, European Network and Information Security Agency (ENISA) is encouraging companies to buy CI (Stupp, 2017). Referring to two big cyberattacks affecting EU economies in 2017, the ENISA argued: "Increased adoption of cyber insurance would prepare the market to respond more effectively to large-scale incidents such as WannaCry and NotPetya and support the economic sustainability of organizations affected by similar major incidents" (Stupp, 2017). A more widespread CI adoption can promote recovery of organizations from large scale cyber-disasters by transferring the risks to insurers.

4.2.1.1. Push for common norms and standards

There is the lack of standardization related to coverage, terminologies and glossaries (Blosfield, 2019). As an example, there is a confusion and a lack of consensus among policyholders and insurers regarding data breach costs covered by a policy. An assumption among policyholders is that if they experience a breach affecting credit card data, their CI will cover all liabilities. Such data are regulated by Payment Card Industry (PCI) rules.

Many insurers offer coverage for PCI costs. Nonetheless they vary widely regarding the definition of these costs. Some policies cover only PCI fines or penalties. Others pay for the costs for additional losses such as those associated with fraud assessments, card reissuance, case management fees and investigation expenses for PCI-Certified Forensic Investigator (Hare-Brown, 2019).

Due to external influences such as court rulings and consumer demand, insurers are covering social engineering frauds. The startup insurtech Cowbell Cyber added such frauds to its CI product. The new product covers policyholders' financial losses from phishing or fraudulent emails (insurancejournal.com, 2020).

The real challenge, however, is the lack of clear consensus about what constitutes social engineering. It is also not clear whether phishing emails are treated as such frauds (Hare-Brown, 2019).

Regulations may also act as a driving force in the evolution of common norms and standards. Some efforts in this direction have been made. In 2013, in order to support the adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the U.S. White House suggested that government agencies and the insurance industry need to work together to build underwriting practices that reduce cyber-risks and promote risk-based pricing. The White House argued that these measures foster a competitive CI market (Arnold & Porter Kaye Scholer, 2013). The ENISA has also urged the EU and national legislators to develop guidelines that would be useful in deciding the types of damages covered under CI.

CI policyholders are expected to take all necessary and reasonable precautions in order to keep them secure and minimize harms if they face cyberattacks. This is referred to as “due care”. If the insurance company believes that a CI policyholder failed to achieve “due care”, the claim may be denied in case of a cyber-incident. For larger CI policyholders, an insurer often conducts a comprehensive analysis of the company's policies and procedures before issuing the policy. This is necessary and economically justifiable for potentially large claim sizes. Conducting a “due care” analysis makes no economic sense for SMEs. A minimum requirement of “due care” is a written cybersecurity policy and strategy, which may indicate that the company has evaluated its security precautions and preparations against legal requirements, and industry best practices (Galvin, 2018). Most SMEs may not have the resources to do so. For instance, A survey conducted by executive coaching organization Vistage found that 62% of SMEs lacked an up-to-date cybersecurity strategy, or any cybersecurity strategy at all (Galvin, 2018).

What is more, having a policy and strategy document may not be sufficient proof of “due care” to satisfy an insurer and a court in case of a dispute. Companies may require logs, documentation, and other evidence to demonstrate their incident response policy, and how they have handled cyber incidents. Some policies may also require controls such as log reviews and audits of their credentials (Covington, 2016). However, these are prohibitively expensive for SMEs.

Smaller companies thus tend to purchase CI policies without a review of their level of protection. It is likely for many SMEs to discover that their “due care” was insufficient after the claim is denied (Covington, 2016). The fact that insurers do not share a common definition of “due care” presents further complexity and challenges (Covington, 2016).

Regulators have started to look at this challenge. The U.S. White House publication “Cyber-Insurance and Impact on Cyber-Security” put the issue this way: “The exact tools and metrics used by a cyber-insurance carrier is proprietary to that carrier, and might differ from carrier to carrier” (Covington, 2016). This situation is quite different from more traditional insurance policies, in which underwriters are often clear and concise about the coverage available to policyholders and use standard terms. Cyber-insurers, however, are arguably against using standard wordings due to concerns that it might be an illegal and anti-competitive practice to share an agreed standard policy (Hare-Brown, 2019). In this regard, the above observation makes

clear that regulators are recognizing the need for standardization. It is expected that in the future legislative and regulatory frameworks for standardization is likely to be developed in collaboration with the CI industry so that concerns such as noted above do not arise.

4.2.2. Effects of normative institutions on other institutions

Lobbying efforts to increase the growth of and reduce the risks to the CI industry.

Insurers are directing lobbying and other efforts to shape policy developments in their favor. As mentioned earlier, the ICNZ lobbied for better reporting and more access to data (Walters, 2018). Likewise, the national trade association for U.S. insurers, American Property Casualty Insurance Association (APCIA) has argued that cyber underwriting regulations need to be "flexible, risk-focused, and scalable" so that policyholders can decide the CI plans that would work best for them. The Association has also presented an argument for its position against privacy laws that require the localization of insurers' data. The APCIA has noted that insurance companies may avoid jurisdictions that force data localization, which will weaken their cybersecurity (Gilligan, 2019). Similarly, in 2013, the U.S. insurance industry spent more than US$154 million on lobbying efforts, which included data security (Bronson, 2016).

A wider adoption of CI requires institutional changes. Institutional actors are likely to bring such changes more easily if their "subject positions" are dominant, which can allow them to gain wide legitimacy and bridge diverse stakeholders (Hoffman, 1999; Maguire et al., 2004). Moreover, their initiatives need to be perceived favorably by other institutional actors (Groenewegen & van der Steen, 2007). For this reason, associations of insurers find it attractive to collaborate with the government. For instance, in order to raise SMEs' awareness of cybercrime and importance of CI, in 2015, the Dutch Association of Insurers (VVN) teamed up with the Dutch Ministry of Security and Justice and MKB-Nederland (Dutch SME association) (insuranceeurope.eu, 2020).

4.2.2.1. Developing standards and facilitating customers' understanding of key aspects of CI

There have also been attempts directed towards developing standards and facilitating customers' understanding of CI. To take an example, Cyber Insurance Association, the forum of CI professionals in London, and the global reinsurance company, Société Commerciale de Réassurance (SCOR), teamed up to organize Cyber Insurance Forum to discuss non-affirmative or silent cyber coverages. These exposures are "neither explicitly included nor excluded in insurance policies or reinsurance treaties". The potential financial implications of such exposures are huge (Public, 2018). For instance, the 2017 NotPetya malware attack was estimated to result in insurance claims of over US$3 billion, of which about 90% was silent (Dyson, 2019). Consequently policies offered by major insurers such as Lloyd's (Gallin, 2020) and AIG s.

Likewise, the VVN, the Dutch Ministry of Security and Justice and MKB-Nederland held roadshows and organized campaigns that provided insights into SMEs' cyber-vulnerabilities and possible measures to be taken to increase cybersecurity (insuranceeurope.eu, 2020). In the same vein, the French insurance association (FFA) has published a brochure that outlines several ways for SMEs to minimize the impact of cyber-risks (insuranceeurope.eu, 2020).

4.2.3. Effects of cognitive institutions on other institutions

4.2.3.1. Regulatory and legal actions to make insurers accountable

When policyholders find that what they take-for-granted about CI coverage is challenged, they may choose regulatory options. As noted above, Mondelez International's lawsuit against Zurich American Insurance Company illustrates this tendency.

Policyholders have engaged in tactics such as lawsuits against insurers that refuse to cover cyber-attack-related losses. Several court rulings have found that it is the insurer's responsibility to cover losses associated with social engineering frauds. Such outcomes increase policyholders' confidence with CI. At least three court rulings suggest that phishing losses and social engineering frauds are covered by cybercrime policies (Loi, 2020). The courts ruled that losses resulting from Business Email Compromise (BEC), which is a kind of social engineering frauds, are covered by computer fraud provisions (Robertson, 2019). Not that in a BEC, also known as a CEO fraud, criminals impersonate high level executives (also known as C-level executives) to request employees to make financial transactions. Such requests are urgent and confidential and need to be made outside the company's standard procedures. Cybercriminals operate in a clever way to make the topic credible and build trust in their victims. They rely on information that is publicly available (Blanco, 2019). Such rulings increase policyholders' confidence that CI can protect them from cyber-risks.

4.2.3.2. Demanding for industrial norms to govern the CI industry

Policyholders are expressing frustration and demanding for industrial norms. Increased consumer pressures for industry norms are evidenced by recent surveys. As noted in Table 2, in a survey conducted by Ovum, 23% of the respondents expressed that they would like to see an industry standard for benchmarking cyber-risks (Insurance Journal, 2017). Such pressures may lead to the development of common norms in the CI industry.

Many businesses complain that existing CI products do not meet their needs. For instance, in a survey of CI policyholders, 55% were reported to be interested in new CI packages that cover cyber-risks such as data loss, denial of service and cyber extortion. However, only 26% had updated CI coverages (Ikeda, 2019).

Businesses and trade associations of insurers have mutual interest in developing standards and new CI programs to cover emerging risks. The APCIA has emphasized the roles of insurers in closing the current cyber protection gaps. It has recognized that, in order to do so, it will be necessary to develop new cyber underwriting processes and educate consumers on ways to minimize cyber-attacks (Gilligan, 2019).

4.3. Process and technological innovations

The CI industry is undergoing a fundamental change and a major upheaval. In most cases, such changes create confusion and uncertainty. The environment lacks norms, templates, and models about appropriate strategies and sources of legitimacy for various actors (Newman, 2000). To put

things in context, existing institutions are inadequate and obsolete to deal with the challenges facing the CI industry and market.

Various process and technological innovations may address these concerns (Fig. 1). For instance, new technological innovations can inspire CI-related regulatory activities. They may also affect norms, codes or conducts at the industry level. Moreover, they might also change the lens of organizational decision makers through which they view CI.

4.3.1. Technologies to assess security of companies' networks and systems

Some companies think that CI is cheaper than cybersecurity. Due to this, cyber-insurers may encounter moral risks. For instance, companies may buy CI rather than spending money to strengthen cybersecurity. In this way, they may find it more attractive to transfer risk to insurers rather than investing in costly risk mitigation efforts that are unproven. This phenomenon could lead to a moral hazard situation: companies take higher cybersecurity risks rather than improving cybersecurity cultures (Dionisi, 2017).

This moral hazard situation can be eliminated or at least reduced by developing mechanisms to track cybersecurity behaviors of policyholders. As of 2017, twelve CI startups were working in areas such as risk scoring and threat remediation (Cbinsights, 2017). These startups assess security of companies' networks and systems and offer security benchmarking. These benchmarking tools can help CI companies to make better underwriting decisions related to cyber liability. Some startups have also come up with FICO-like scores of risk profiles. Note that the FICO score measures consumer credit risk, which is widely used in the U. S. to assess creditworthiness of consumers in lending decisions.

On the other hand, adverse selection occurs if the policyholder has more information on risk than the insurer. This means that those with greatest risk have a higher tendency to buy insurance. Cyber-insurers can conduct security audits to avoid adverse selection by obtaining additional information on risk. However, this makes CI impractical for small businesses (The Hill, 2018).

4.3.2. Upgraded underwriting process

It is important for CI underwriters to determine a potential policyholder's cyber-risk profile and compare it with the level of risk that the insurer would like to take. An accurate assessment of cyber-risk can also help determine the level of premium that reflects the risk profile. The above developments can play a major role in upgrading the underwriting process. For instance, Israel's Sayata Labs uses artificial intelligence (AI) and data science to underwrite CI for SMEs (PYMNTS, 2019). Sayata's solutions help insurers to assess cyber-risks and offer recommendations to policyholders. As of 2018, Sayata was working with the insurer AXA. With more accurate assessment and diagnosis of policyholders' security postures, insurers and brokers can minimize their risks. Likewise, the startup insurtech Cowbell Cyber offers AI-powered CI for SMEs (insurancejournal.com, 2020).

4.3.3. Centralized database on cybersecurity incidents and metrics for cyber-risks

The lack of data makes it difficult for insurers to understand the nature of cyber-threats, the motivation behind them and the severity of loss (Stupp, 2017). Some initiatives have been taken to develop database on cybersecurity incidents and metrics for cyber-risks. The ENISA recommended that EU authorities set up a centralized database on cybersecurity incidents in order for CI companies to compare information related to cyberattacks. The agency believes that an EU-wide database and guidelines could improve the quality of information about cyber-risks.

4.4. Formation of dense networks and relationships in the CI industry

A faster diffusion of CI requires a paradigm shift in terms of how CI is perceived. Prior research indicates that such a shift involves a social learning process that comprises diverse participants with broad social and economic interests. These institutional actors want to accomplish multiple purposes that are not always congruent (Baumgartner & Jones, 1993). Unsurprisingly, due to the dynamic and transformative nature of CI and potentially important economic implications, it is drawing diverse actors. These include regulators such as the ENISA, the U.S. White House and the DFS, professional and trade associations and insurance companies.

As noted above, these actors seem to be in the mobilization stage (Purdy & Gray, 2009) and there is a significant trend towards collaboration, coordination and communication among them.

The above activities are indicative of the formation of a dense network of relationships among various actors in the institutional field formed around CI, which is likely to reduce incentives for opportunism (Axelrod & Cohen, 2001). This is because dense relationships and interactions result in the availability of information about the actions of various parties, which would help enhance trust. For instance, if formal mechanisms related to CI are created, insurers and policyholders do not have to depend on personal or organizational characteristics or past exchange history. Zucker (1986) refers to this phenomenon as institutionally based trust.

One implication is that policyholders can increase their capacity to negotiate with insurers to get lower premiums. For instance, insurers place a substantial burden of proof on policyholders to prove that they did not fail to achieve “due care”. That is, policyholders are required to prove that they were not negligent in allowing a cyber-incident. Consequently, only a small proportion of claims are being paid. This situation might change with an increased competition. For instance, some insurers might use technology as a competitive weapon and start utilizing third party cyber-risks assessment tools in order to increase their market shares. Overall, insurers are likely to face more pressures to be more reasonable and realistic and offer policies that reflect the cyber-risks facing their clients.

5. Discussion and implications

This paper sheds light on institutional mechanisms that are unique to the CI industry and market. For instance, prior research has suggested that building a regulative/law pillar system is the first stage of field formation. It is followed by a formation of normative institutions and then cognitive institutions (Hoffman, 1999). The above discussion suggests that the formation of CI-related institutional pillars is not necessarily in the same order as has been reported by prior researchers in industries such as cloud computing (Kshetri, 2013) and the natural environment

(Hoffman, 1999). Indeed, CI-related regulations have been slow to develop. For instance, CI has been available since the 1990s (iif.com, 2017; Kshetri, 2018). Organizations that adopted CI early did so not because of regulatory pressure (regulative institutions) but because they felt it necessary to have CI to protect against cyberattacks (cognitive institutions).

The explanation offered in this paper provided insights into how different institutional pillars reinforce one another. Such a mechanism is likely to influence a range of demand and supply side factors and create a system that can accelerate CI's growth.

Insurers, policyholders and governments can take measures to accelerate the diffusion of CI. The lack of clear regulatory guidance requires courts to make decisions as to whether insurers are required to provide coverage for certain damages. One way to avoid potential disputes for brokers and carriers is to work closely with clients to identify unique cyber-risks facing them, tailor CI coverage to address them and ensure the policyholder has a clear understanding of their CI (Gerhards, 2018).

The government's role is especially important for the simple fact that cyber-attacks on national infrastructures can lead to significant harms. Policymakers are aware of the challenges faced by the CI industry and market. The U.K. regulator, Prudential Regulatory Authority (PRA), which supervises over 1500 financial institutions, noted that challenges such as lack of historical data and models, and expertise are among the main hinderances in CI's growth (gccapitalideas.com, 2019). In particular, the governments can play a major role in developing common metrics for cyber-risk management. They can do so by encouraging companies to share cyber-risk information and security practices. In addition, they should standardize corporate reporting on cyber-risks and data breaches (Levite & Hoffman, 2019). For instance, if governments require companies to report cost, sophistication, number, nature and frequency of cyberattacks faced and how these indicators vary across firms with different types of cybersecurity measures, insurers will have access to valuable information that allows them to evaluate cyber-risks and underwrite a CI policy.

The way a policy is articulated affects individuals' perceptions of the policy. However, how it is viewed by individuals is not completely under the government's control (Ericson & Kessler, 2016). For instance, in the case of the PPACA, before the U.S. Supreme Court's ruling, the government's desired articulation was negatively affected by the opponents of the policy and discussions in the popular press (Ericson & Kessler, 2013). The press had questioned the constitutionality and moral authority of the policy (Ericson & Kessler, 2013). This underscores the importance of government initiatives in educating the media and the public about the importance of CI.

6. Concluding remarks

CI is emerging as an important tool to protect organizations against future cyberattack-related losses. The current size of the CI market does not reflect the cyber-risks. This paper argues that institutions are changing in a way that favors the growth of the CI market. Many of the current challenges are also likely to be addressed with new technological solutions and process innovations.

Since most organizations are underinsured or uninsured, governments should introduce policies for encouraging widespread adoption of CI. The policies need to be clearly articulated in a way that motivates firms to buy CI. For instance, the value and legitimacy of a policy that require to have CI can be increased by framing it as a practice to strengthen cybersecurity and linking organizational cybersecurity with national cybersecurity.

Acknowledgement

Detailed, generous and insightful comments on earlier versions from Erik Bohlin, Editor in Chief and two anonymous JTPO reviewer helped to improve the paper drastically.

References

businessinsurance.com. (2014). *Target data breach prompts insurers to scale back cyber coverage for retailers*. http://www.businessinsurance.com/article/20140330/NEWS07/303309967/target-data-breach-prompts-insurers-to-scale-back-cyber-coverage-for.

natlawreviewcom. (2014). What is cyber liability insurance?. http://www.natlawreview.com/article/what-cyber-liability-insurance.

aon.com. (2017). *Global cyber risk transfer comparison report sponsored by aon risk solutions independently conducted by Ponemon Institute LLC publication date: April 2017*. https://www.aon.com/germany/risk-services/cyber_risiken/2017-global-cyber-risk-transfer-comparison-report.pdf.

iif.com. (2017). *Cyber risk insurance: A growth market adapting to a changing risk*. The Institute of International Finance.

gccapitalideas.com. (2019). *Silent cyber: Solutions emerge amid the uncertainties*. GC Capital Ideas. https://www.gccapitalideas.com/2019/10/20/silent-cyber-solutions-emerge-amid-the-uncertainties/.

professionalsecuritycouk. (2019). *Insurers ask for cyber breach data, 14 May*. https://www.professionalsecurity.co.uk/news/interviews/insurer-asks-for-cyber-breach-data/.

insuranceeuropeeu. (2020). *Insurers' role in increasing cyber resilience*. https://www.insuranceeurope.eu/sites/default/files/attachments/Insurers%E2%80%99%20role%20in%20increasing%20cyber%20resilience.pdf.

insurancejournal.com. (2020). Cowbell cyber adds social engineering coverage, opens platform to non-insureds. *Insurance journal*. https://www.insurancejournal.com/news/national/2020/04/20/565391.htm.

insureon.com. (2020). *Third-party cyber liability insurance. Insureon*. https://www.insureon.com/insurance-glossary/cyber-liability-third-party.

spglobalcom. (2020). *Technology research*. S&P Global. https://www.spglobal.com/en/research-insights/featured/cyber-insurance.

techinsurancecom. (2020). *First-party vs. third-party cyber liability insurance. TechInsurance*. https://www.techinsurance.com/resources/first-party-vs-third-party-cyber-liability-insurance.

Allied Market Research. (2020). *Cyber insurance market is expected to grow $28.60 billion by 2026: Says AMR. GlobaNewswire*. https://www.globenewswire.com/news-release/2020/03/31/2009314/0/en/Cyber-Insurance-Market-Is-Expected-to-Grow-28-60-Billion-by-2026-Says-AMR.html.

Aon Benfield. (2017). *Global cyber market overview uncovering the hidden opportunities*.

Arnold & Porter Kaye Scholer. (2013). *New government cybersecurity standards could impact many companies, August 12*. https://www.lexology.com/library/detail.aspx?g=d5650eac-65dd-42de-8784-5c62f5798b94.

Ashford, W. (2019). *Cyber insurance uptake growing, but not all firms convinced*. https://www.computerweekly.com/news/252456724/Cyber-insurance-uptake-growing-but-not-all-firms-convinced.

Axelrod, R. (1997). *The complexity of cooperation*. Princeton, NJ: Princeton University Press.

Axelrod, R., & Cohen, M. D. (2001). *Harnessing complexity: Organizational implications of a scientific frontier*. New York: Basic Books.

Barnett, W. P., & Carroll, G. R. (1993). How institutional constraints affected the organization of early US telephonies. *Journal of Law, Economics, and Organization, 9*, 98–126.

Baukes, M. (2016). *Cyber insurance in the wake of PF chang's vs Chubb*. https://www.insurancejournal.com/magazines/mag-features/2016/09/06/424905.htm.

Baumgartner, F. R., & Jones, B. D. (1993). *Agendas and instability in American politics*. Chicago: University of Chicago Press.

Bay, K. (2020). *The missing piece*. Insurance Business America. https://www.insurancebusinessmag.com/us/opinion/the-missing-piece-219693.aspx.

Blanco, A. (2019). *'CEO fraud': What is it and how does it work*. BBVA. https://www.bbva.com/en/ceo-fraud-how-does-it-work-and-how-to-prevent-it/.

Blosfield, E. (2019). *How to turn today's confusion into a sustainable cyber insurance market*. https://www.insurancejournal.com/news/national/2019/03/26/521646.htm.

Boddy, S. (2017). *Cyber insurance read the fine print!*. https://www.darkreading.com/partner-perspectives/f5/cyber-insurance-read-the-fine-print!/a/d-id/1329113.

Bronson, C. (2016). *The insurance industry is spending millions in politics – but where is it going?, 10 May*. https://www.insurancebusinessmag.com/us/news/breaking-news/the-insurance-industry-is-spending-millions-in-politics–but-where-is-it-going-31724.aspx.

Burns, J., & Nielsen, K. (2006). How do embedded agents engage in institutional change? *Journal of Economic Issues, 40*(2), 449–456.

Cbinsights. (2017). *12 tech startups transforming cyber insurance, risk scoring, and threat remediation*. https://www.cbinsights.com/research/cyber-insurance-risk-scoring-startups/.

Ciab. (2018). *Market index surveys*. https://www.ciab.com/market-intel/market-index-surveys/.

Clarke, D. (2020). *Canada: Cyber warfare and the act of war exclusion*. Blaney McMurtry LLP. https://www.mondaq.com/canada/Insurance/909286/Cyber-Warfare-And-The-Act-Of-War-Exclusion.

Cohn, C. (2018). *Insurers cash in on new European data privacy rules*. https://uk.reuters.com/article/uk-insurance-cyber-gdpr/insurers-cash-in-on-new-european-data-privacy-rules-idUKKCN1IM1A1.

Colyvas, J. A., & Powell, W. W. (2006). Roads to institutionalization: The remaking of boundaries between public and private science. *Research in Organizational Behavior, 27*, 305–353.

Condon, S. (2018). *Survey: 7 out of 10 US healthcare firms have no cybersecurity insurance*. https://www.zdnet.com/article/survey-7-out-of-10-us-healthcare-firms-have-no-cybersecurity-insurance/.

Covington, R. (2016). *Why your cyber insurance investment may not pay off*. https://www.csoonline.com/article/3018877/why-your-cyber-insurance-investment-may-not-pay-off.html.

Deephouse, D. L. (1996). Does isomorphism legitimate? *Academy of Management Journal, 39*, 1024–1039.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*, 147–160.

Dionisi, S. (2017). *Cybersecurity: Impact on insurance business and operations, joint risk management section*. Canadian Institute of Actuaries Casualty Actuarial Society Society of Actuaries.

Dyson, B. (2019). *Pressure mounting on insurers to tackle silent cyberrisk 17 June*. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/52342876.

Elster, J. (1989). Social norms and economic theory. *The Journal of Economic Perspectives, 3*(4), 99–117.

Ericson, K. M., & Kessler, J. B. (2013). *The articulation effect of government policy: Health insurance mandates versus taxes, NBER working paper No. 18913*. https://www.nber.org/papers/w18913.

Ericson, K. M., & Kessler, J. B. (2016). The articulation of government policy: Health insurance mandates versus taxes. *Journal of Economic Behavior & Organization, 124*, 43–54.

Ferland, J. (2019). Cyber insurance – what coverage in case of an alleged act of war? Questions raised by the Mondelez v. Zurich case. *Computer Law & Security Report, 35*, 369–376.

Friedman, S. (2017). *Deloitte University Press, Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising market*. https://www2.deloitte.com/insights/us/en/industry/financial-services/demystifying-cybersecurity-insurance.html.

Gallin, L. (2020). *Lloyd's details phased implementation of silent cyber mandate, 30 January*. https://www.reinsurancene.ws/lloyds-details-phased-implementation-of-silent-cyber-mandate/.

Galvin, J. (2018). *60 percent of small businesses fold within 6 Months of a cyber attack*. Here's How to Protect Yourself. May 7 https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html.

Gangcuangco, T. (2020b). *Gallagher poll points to cyber underinsurance. Insurance Business UK*. https://www.insurancebusinessmag.com/uk/news/cyber/gallagher-poll-points-to-cyber-underinsurance-212781.aspx.

Gerhards, E. (2018). *Cybersecurity insurance: Popular but poorly understood*. https://www.propertycasualty360.com/2018/07/10/cybersecurity-insurance-popular-but-poorly-underst/?slreturn=20190228072908.

Gilligan, E. (2019). *APCIA addresses cyber risks and cyber underwriting in Latin America at FIDES conference, september 9*. http://www.pciaa.net/pciwebsite/Cms/Content/ViewPage?sitepageid=57630.

Greenwood, R., & Hinings, C. R. (1996). Understanding radical organizational change: Bringing together the old and the new institutionalism. *Academy of Management Review, 21*, 1022–1054.

Groenewegen, J., & van der Steen, M. (2007). The evolutionary policy maker. *Journal of Economic Issues, 41*(2), 351–358.

Grones, G. (2019). *Top 10 cyber insurance companies in the US*. Insurance Business America. https://www.insurancebusinessmag.com/us/news/cyber/top-10-cyber-insurance-companies-in-the-us-195463.aspx.

Grzadkowska, A. (2019). *With evolution in cybercrime, brokers' roles are more complex and critical*. https://www.insurancebusinessmag.com/us/news/cyber/with-evolution-in-cybercrime-brokers-roles-are-more-complex-and-critical-163659.aspx.

Grzadkowska, A. (2020). *Increasing ransomware demands are challenging many carriers*. Insurance Business America. https://www.insurancebusinessmag.com/us/news/cyber/increasing-ransomware-demands-are-challenging-many-carriers-218976.aspx.

Hare-Brown, N. (2019). *Confusing terminology stunts the growth of cyber insurance* (Vol. 4, pp. 16–17). Issue: Computer Fraud & Security.

Harrington, J. S. (2017). *Cyber insurance: Many choices now that there is No choice, april 12*. https://www.insurancejournal.com/news/national/2017/04/12/447585.htm.

Hayek, F. A. (1979). *Law, legislation and liberty (3 vols)*. Chicago: University of Chicago Press.

Hobson, A., & Adams, I. (2020). *California dreams about cyber insurance, and federal lawmakers should pay attention*. The Hill. https://thehill.com/opinion/cybersecurity/486427-california-dreams-about-cyber-insurance-federal-lawmakers.

Hoffman, A. J. (1999). Institutional evolution and change: Environmentalism and the US chemical industry. *Academy of Management Journal, 42*(4), 351–371.

Holyoke, T. T. (2003). Choosing battlegrounds: Interest group lobbying across multiple venues. *Political Research Quarterly, 56*(3), 325–336.

IBM Security. (2019). *Cost of data breach report*. https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.181209767.1686129232.1586105132-321662522.1584074488.

Ikeda, S. (2019). *New report indicates cyber insurance providers are too slow to respond to emerging threats, customer needs, may 31*. https://www.cpomagazine.com/cyber-security/new-report-indicates-cyber-insurance-providers-are-too-slow-to-respond-to-emerging-threats-customer-needs/.

Insurance Journal. (2017). *Why 27% of U.S. Firms have No plans to buy cyber insurance*. https://www.insurancejournal.com/news/national/2017/05/31/452647.htm.

Insurance Journal. (2018). *How UK brokers view cyber insurance*. https://www.insurancejournal.com/news/international/2018/05/15/489196.htm.

ITIJ. (2018). *Standardising cyber terminology*. https://www.itij.com/feature/standardising-cyber-terminology.

Johns, M. (2017). *How will GDPR affect insurance companies in the UK?*. https://www.centurylink.co.uk/blog/will-gdpr-affect-insurance-companies-uk/.

Kshetri, N. (2013). *Privacy and security issues in cloud computing: The role of institutions and institutional evolution. 37* pp. 372–386). May–June. Telecommunications Policy.

Kshetri, N. (2018). The economics of cyber-insurance. *IEEE IT Professional, 20*(6), 9–14.

Kshetri, N., & Dholakia, N. (2009). Professional and trade associations in a nascent and formative sector of a developing economy: A case study of the NASSCOM effect on the Indian offshoring industry. *Journal of International Management, 15*(2), 225–239.

Levite, A., & Hoffman, W. (2019). *A moment of truth for cyber insurance*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/02/07/moment-of-truth-for-cyber-insurance-pub-78342.

Liberman, V., Samuels, S. M., & Ross, L. (2004). The name of the game: Predictive power of reputations versus situational labels in determining prisoner's dilemma game moves. *Personality and Social Psychology Bulletin, 30*(9), 1175–1185.

Lindsey, N. (2019). *Cyber insurance not valid in case of cyber war*. Says Major Insurance Company. https://www.cpomagazine.com/cyber-security/cyber-insurance-not-valid-in-case-of-cyber-war-says-major-insurance-company/.

Loi, P. (2020). Another federal circuit finds phishing loss covered under crime policy. *Insurance journal*. https://www.insurancejournal.com/news/national/2020/02/11/557918.htm.

MacRae, D. (2020). *75% of large businesses suffered security breaches in 2019. Digit*. https://digit.fyi/75-of-large-businesses-suffered-security-breaches-in-2019/.

Maguire, S., Hardy, C., & Lawrence, T. B. (2004). Institutional entrepreneurship in emerging fields: HIV/aids treatment advocacy in Canada. *Academy of Management Journal, 47*(5), 657–679.

Market Research Future. (2019). *Cyber insurance market is booming due to cyber risks by the adoption of cloud technologies by various businesses december 20*. https://www.globenewswire.com/news-release/2019/12/20/1963293/0/en/Cyber-Insurance-Market-is-Booming-Due-to-Cyber-Risks-by-the-adoption-of-Cloud-Technologies-by-Various-Businesses.html.

Marsh, & McLennan Companies. (2017). *Cyber risk in asia-pacific the case for greater transparency risk in focus series,*.

McCarthy, K. (2019). *Cyber-insurance shock: Zurich refuses to foot NotPetya ransomware clean-up bill – and claims it's 'an act of war*. https://www.theregister.co.uk/2019/01/11/notpetya_insurance_claim/.

McDaniels, C. (2017). *The pitfalls of cyber insurance*. http://www.darkreading.com/endpoint/the-pitfalls-of-cyber-insurance/a/d-id/1329656.

McIntosh, R. (2019). *Analysis lack of insurance in crypto is keeping institutional capital away*. https://www.financemagnates.com/cryptocurrency/news/lack-of-insurance-in-crypto-is-keeping-institutional-capital-away/.

Meckbach, G. (2019). *Why the cyber market has become so crowded*. https://www.canadianunderwriter.ca/commercial-lines/why-the-cyber-market-has-become-so-crowded-1004155640/.

Musotto, R., & Naser, M. (2020). Ransomware attack on sheep farmers shows there's no room for woolly thinking in cyber security. *Mar, 8*, 2020. https://theconversation.com/ransomware-attack-on-sheep-farmers-shows-theres-no-room-for-woolly-thinking-in-cyber-security-132882.

National Conference of State Legislatures. (2020). *Budgeting for cybersecurity*. National Conference of State Legislatures. https://www.ncsl.org/documents/taskforces/Budgeting_For_Cybersecurity_32041.pdf.

Newman, K. L. (2000). Organizational transformation during institutional upheaval. *Academy of Management Review, 25*(3), 602–619.

North, D. C. (1990). *Institutions, institutional change and economic performance*. Cambridge, UK: Cambridge University Press.

North, D. C. (1994). Economic performance through time. *The American Economic Review, 84*(3), 359–368.

North, D. C. (1996). Epilogue: Economic performance through time. In L. J. Alston, T. Eggertsson, & D. C. North (Eds.), *Empirical studies in institutional change*. Cambridge, PA: Cambridge University Press.

O'Nell. (2018). *Cyber insurance claim denials*. http://millerfriel.com/blog/cyber-insurance-claim-denials/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

Price, S. (2020). *Largest health insurance companies of 2020*. Value Penguin. https://www.valuepenguin.com/largest-health-insurance-companies.

Public. (2018). *SCOR and the cyber insurance association host A joint cyber insurance forum in Zurich*. http://www.publicnow.com/view/904E58039E71FDD46E3F9A5C4F53E59756D3E82D.

Purdy, J. M., & Gray, B. (2009). Conflicting logics, Mechanisms of diffusion, and multilevel dynamics in emerging institutional fields. *Academy of Management Journal, 52*(2), 355–380.

PYMNTS. (2019). *Robocalls go unpunished, exposing regulatory gaps*. https://www.pymnts.com/legal/2019/robocalls-regulatory-gaps-fcc/.

Ralph, O. (2018). *Cyber attacks: The risks of pricing digital cover, March 18, 2018*. https://www.ft.com/content/31515a18-238f-11e8-ae48-60d3531b7d11.

Ralph, O. (2019). *Data hacks and big fines drive cyber insurance growth*. Financial Times. https://www.ft.com/content/751946b2-fb0a-11e9-a354-36acbbb0d9b6.

Reay, R., Golden-Biddle, K., & GermAnn, K. (2006). Legitimizing a new role: Small wins and microprocesses of change. *Academy of Management Journal, 49*, 977–998.

reinsurancenews. (2018). *Cyber re/insurance is already rapidly maturing: PCS*. https://www.reinsurancene.ws/cyber-reinsurance-already-rapidly-maturing-pcs/.

Robertson, C. (2019). *Covering phishing & other social engineering attacks: The state of play in computer fraud insurance*. Ice Miller. https://www.icemiller.com/ice-on-fire-insights/publications/covering-phishing-other-social-engineering-attac/.

Ross, A. (2019). *The state of cyber insurance coverage in the UK, 4 April*. https://www.information-age.com/state-of-cyber-insurance-coverage-123481467/.

Row, S. (2018). *Common gaps in coverage for data security incidents*. https://www.nwpolicyholder.com/2018/04/common-gaps-in-coverage-for-data-security-incidents/.

Scott, R. (1987). The adolescence of institutional theory. *Administrative Science Quarterly, 32*, 493–511.

Scott, R. (1995). *Institutions and organizations*. Thousand Oaks, CA: Sage.

Scott, R. (2001). *Institutions and organizations* (2nd ed.). Thousand Oaks, CA: Sage. Scott, W. R., Ruef, M., Mendel, P. J., & Caronna, C. A. (2000). *Institutional change and healthcare organizations: From professional dominance to managed care*. Chicago, IL: University of Chicago Press.

Seo, M. G., & Creed, W. E. D. (2002). Institutional contradictions, praxis, and institutional change: A dialectical perspective. *Academy of Management Review, 27*(2), 222–247.

Stoller, D. (2020). *Cyber insurance purchases will surge with California privacy law. Bloomberg law*. https://news.bloomberglaw.com/privacy-and-data-security/cyber-insurance-purchases-will-surge-with-california-privacy-law.

Stupp, C. (2017). *EU guidelines would help cyber insurance industry, agency says*. https://www.euractiv.com/section/cybersecurity/news/eu-guidelines-would-help-cyber-insurance-industry-agency-says/.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review, 20*, 571–610.

The Hill. (2018). *Using cyber-insurance to improve cyber-security: Legislative solutions for the insurance market*. https://thehill.com/sites/default/files/ISA_CyberSecurityCyberInsurancePaper_0.pdf.

Trice, C. (2019). *Competition, lack of major claims payouts driving aggressive cyber writing*. S&P Global. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/53006735.

Van der Veen, A., & Tagel, G. (2011). Effect of policy interventions on food security in Tigray, Northern Ethiopia. *Ecology and Society, 16*(1), 18. http://www.ecologyandsociety.org/vol16/iss1/art18/.

Verdict. (2020). *Cyber insurance: Timeline 3 april*. https://www.verdict.co.uk/cyber-insurance-timeline/.

Walters, L. (2018). *Businesses under attack but few have cyber insurance*. https://www.newsroom.co.nz/2018/10/04/264365/few-businesses-have-cyber-insurance-as-attacks-ramp-up.

Yadron, D. (2014). *Target hackers wrote partly in Russian, displayed high skill, report finds*. http://online.wsj.com/news/articles/SB10001424052702304419104579324902602426862 .

Zucker, L. (1986). Production of trust: Institutional sources of economic structure 1840-1920. *Research in Organizational Behaviour, 8*(3–11).