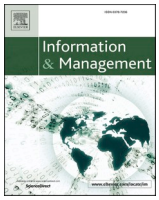
Information & Management 58 (2021) 103507

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im



Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures

Obi Ogbanufe [a], Dan J. Kim [b,*], Mary C. Jones [c]

[a] Department of Information Technology and Decision Sciences, G. Brint Ryan College of Business, University of North Texas, USA
[b] Department of Information Technology and Decision Sciences, G. Brint Ryan College of Business, University of North Texas, 1307 West Highland Street, Denton, TX 76201, USA
[c] Department of Information Technology and Decision Sciences, G. Brint Ryan College of Business, University of North Texas, USA

ARTICLE INFO

Keywords:
Risk management
Cybersecurity strategy
Cyberinsurance
Top management
Upper echelons theory
Institutional theory

ABSTRACT

Given the financial consequences of security breaches, security risk management has gained more attention in board rooms and garnered more involvement from top management. We undertake a study to understand the top managers' role in cybersecurity strategy, specifically with cyberinsurance. This study draws from institutional and upper echelons theories to explain how top managers' values and perceptions mediate the impact of external institutional pressures on the commitment to use cyberinsurance as a risk management strategy. We empirically test proposed hypotheses using data collected from executive-level managers of various firms and perform semi-structured interviews of six case sites as post hoc analysis. The results suggest that institutional pressures positively affect top managers' perceptions of job security, breach risk, financial risk, transaction cost, and regulatory oversight. In turn, these perceptions influence their commitment to cyberinsurance. We find that values and perceptions of personal relevance have a significant impact on their strategic decisions. The findings emphasize the critical role that top management plays in mediating the influence of institutional pressures on cybersecurity strategy. Implications for research and practice, along with limitations and future directions, are discussed.

1. Introduction

Cybersecurity breaches often result in the compromise of customer data that are ultimately very costly for organizations. Costs include notifying the individuals who are impacted by the security breach as well as legal fees, fines, and recovering from the breach [1]. For example, the security breach at Target in 2013 costs the company an estimated US$293 million, with over US$18 million in legal settlements [2]. Because of these high-profile breaches and the resulting costs, organizational board members and senior management have begun to pay more attention to them [3,4]. Thus, organizations are not only using traditional security risk management strategies (risk mitigation, risk acceptance, and risk avoidance), but also focusing on risk transfer strategies that can offer an even stronger overall cybersecurity solution [1]. The traditional approaches focus largely on deterrence, prevention, detection, and response [2,3] and have informed our understanding of managing security risk. However, these approaches do not help organizations address breach-related losses and residual security risks after a breach has occurred [4].

Risk transfer is a risk management approach that does address these types of losses. Research has shown that risk transfer through cyberinsurance provides a more comprehensive solution for cybersecurity [1, 5]. Cyberinsurance protects organizations from risks incurred through internet and information systems (IS) usage [6,7] by mitigating the financial impact of a cybersecurity breach. Cyberinsurance allows the companies to transfer security risks to the cyberinsurance provider [5]. In fact, many government standards and regulatory agencies now require the use of cyberinsurance. For example, the Securities and Exchange Commission (SEC) requires publicly traded firms to disclose the type of insurance used in their cybersecurity plans [14]. As such, the purchase of such insurance is a decision made by an organization; thus choosing to use cyberinsurance is a strategic decision [15].

Although there is ample literature on IS-related strategic decisions [e.g., 8–12], IS strategy within the cybersecurity context is a relatively underdeveloped topic. A close examination of the strategic choice and decision-making literature in IS indicates that there are few studies that have specifically examined the cybersecurity strategic decision (see Appendix A). Studies have examined information technology (IT)/IS

* Corresponding author.

https://doi.org/10.1016/j.im.2021.103507
Received 25 July 2020; Received in revised form 10 July 2021; Accepted 22 July 2021
Available online 28 July 2021

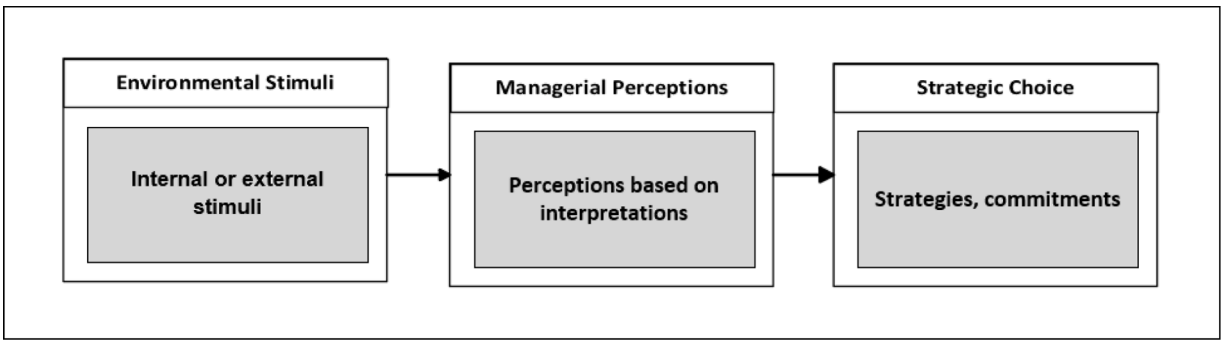


Fig. 1. Conceptual framework depicted from Hambrick and Mason's [18] UET.

management and IT strategic management [12,13]. However, we found only one study that specifically examines IS strategy within the context of cybersecurity, Angst et al. [14].

Researchers have explored theories that explain organizations' strategic choices or decisions. Among them is an institutional theory [15], which posits that external institutional pressures influence organizational decisions. In the IS field, several researchers have examined the role of institutional pressures on an organization's decision to adopt or assimilate technological innovations [16,17]. In addition, top echelons theory [18], which suggests that organizational outcomes are reflections of the values and perceptions of the organization's top executives, has been used in IS to examine strategic innovations and security investments in healthcare [10,14].

There has been little research, however, that uses the lens of both institutional theory and upper echelons theory (UET) to focus specifically on cybersecurity strategy. Fewer still are studies that unpack the top manager's values and perceptions of personal relevance with respect to the strategic decisions surrounding cybersecurity. This research gap should be addressed because a more detailed understanding of how institutional pressures and top manager's values and perceptions affect cybersecurity as an organizational strategy could be very useful for practice and could provide theoretical implications as well. Drawing from UET, institutional theory, and the cybersecurity literature, we propose a conceptual model to better understand how organizations commit to cybersecurity strategies in response to institutional pressures, values, and perceptions. Extending the findings from Liang et al. [16] who suggest that institutional pressures are mediated by top manager perceptions[1] in their effect on strategic enterprise resource planning (ERP) assimilation, we argue that institutional pressures influence cybersecurity strategic decisions. Due to the forces surrounding the cybersecurity landscape, not only are organizational decisions subject to the normative, mimetic, and coercive pressures exerted by other organizations, institutions, partners, and vendors, but the decisions are also subject to the top managers' values and perceptions. These assertions are supported by the top echelons theory that argues that external and internal stimuli are mediated by the top manager's perceptions [18].

While one can assume that institutional pressures and managerial perceptions may influence commitment to using cyberinsurance as a risk management strategy, there are currently few studies that have theoretically and empirically integrated these perspectives within the cybersecurity context. As such, more theory-based IS strategic studies in cybersecurity are important and timely in the currently fast-evolving cybersecurity landscape, especially since cybersecurity has moved to the top of the management agenda as a strategic issue [19,20] and occupies top managers' attention [21,22].

This research makes several contributions. First, by incorporating UET and institutional theory to study cybersecurity risk management strategy, this study complements prior integrative framework approaches to understanding top manager perspectives [e.g., 16]. Also, because this study bridges several perspectives in institutional theory [15], top echelons theory [18], and cybersecurity literature [22], we believe that it provides comprehensive insight and evidence of the top management decision-making towards a cybersecurity strategy. Second, and more importantly, by examining the values and perceptions that have personal relevance (e.g., job security and breach risk severity) to top managers, this study highlights how these factors could be leveraged to change and influence their commitment to a cybersecurity strategy. To our knowledge, no other study has employed UET and institutional theory to examine cybersecurity strategy and especially focused on individual risk factors that may affect organizational decisions. Thus, this study presents a novel inquiry into the use of UET in IS strategy.

2. Theoretical background

The foundation of our theoretical framework is made up of two elements: UET and institutional theory. UET argues that an organization's strategies, performance, and outcomes are reflections of the values and perceptions of the organization's top executives [18]. The values and perceptions of top executives (e.g., CEO) differ from one another, which results in differences in their estimation of organizational needs and leads to different organizational strategies [23]. Furthermore, top executives' *strategic choices* are based on their *perceptions*, which are influenced by *internal and external stimuli* [18]. UET provides theoretical explanations connecting top executive perceptions to strategic choice and suggests those perceptions are influenced by internal and external stimuli. Given that commitment is a strategic factor that provides evidence of how strategies evolve over time [24], we adopt commitment as a strategic decision. External stimuli also referred to as external pressures are expected to influence commitment through top manager's perceptions and values. The institutional theory became primary reasoning for the effect of such external stimuli on organizational decision-making [15]. External pressure (e.g., partner coercive practices, normative pressures from industry) affect organizational decision-making and strategic choice through the perceptions of top executives in the organizations [16]. The theoretical foundation of this study is shown in Fig. 1.

2.1. External institutional stimuli and cybersecurity strategy

Institutional theory [15] supports the influence of social, political, and technical factors on organizational behavior [16]. Institutional theory suggests that the need for legitimacy is the main driver for organizational behavior, more so than efficiency. The notion is that institutional pressures lead top managers to make strategic decisions that are similar to those of other reference organizations such as partners and others in their industry [14]. That is, to maintain legitimacy in their industry, organizations are inclined to conform to prevailing institutional norms to look like other firms [15]. This process is referred to as

[1] This study uses top managers, top executives, and executive-level managers interchangeably as the same meaning of position.

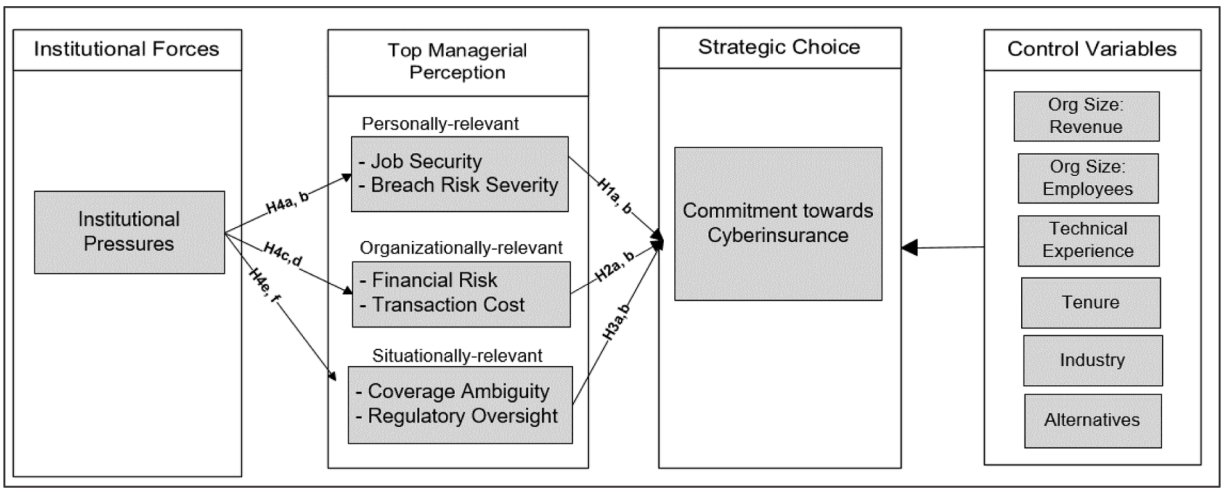


Fig. 2. Research model.

institutional isomorphism. There are three categories of institutional isomorphism: mimetic, coercive, and normative [15].

Coercive isomorphism is a combination of external pressures from other organizations on which the firm depends [25] and the expectations of other organizations in the industry [15]. It can be argued that the use of cyberinsurance arose from external pressures and expectations of others in the industry. Its use was first proposed in the financial sector [26,27]. Soon, it was argued that cybersecurity should be run by the insurance industry [28]. That argument was that in the same manner that organizations install sprinklers and alarms following insurance requirements, organizations will also invest in security management tools and procedures following insurance industry requirements. The insurance industry is one of the industries on which organizations depend for the protection of assets. The industry expectation to adopt business insurance is not new; however, the expectation has extended to cyberinsurance as cyber risks increase.

Mimetic isomorphism is the pressure to mimic other organizations as a result of uncertainties in the industry. Because cybersecurity is often a moving target, organizations may model their cybersecurity strategies similar to organizations they believe are legitimate [15], whether as a symbolic or substantive activity [14]. Several studies in IS use mimetic isomorphism to understand organizational and top management decision-making processes [16]. Normative isomorphism reflects a collective expectation within the industry of what is an appropriate, legitimate behavior [15]. Normative pressures have been described as a process of professionalism whereby industry participants are exposed to third parties, professional and trade organizations, and vendors that set the tone for expectations and best practices in a particular area. Thus, top managers and organizations may form perceptions and act based on these suggested norms.

2.2. Executives' perceptions

The processes through which executives make decisions have been described as complex and ill-defined, reflecting their beliefs, assumptions, and preferences [18]. Because the top manager's attention is limited and cannot include all aspects of the organization, their perceptions are also limited and selective [18]. In order to include managerial perceptions that are of value to them, we use the expectancy–valence framework to conceptualize factors that are of value. The expectancy–valence (value) framework posits that the action or choice of an individual is related to the individual's perceived benefits and risks of an expected outcome [29]. Researchers in a variety of disciplines have used this framework to better understand how the simultaneous assessment of risk and benefit affects behavior [30,31]. Expectancy–valence (value) is a function of three main factors: individual, organizational, and situational factors [32].

Strategic management research has found that top management discretion arises from individual, organizational, and environmental concerns [33]. These studies suggest that research about top manager's decision-making should address the role of three concentric factors: the environment, the organization, and the individual executive [34]. IS research has used a similar concentric approach and suggests that individuals' decisions are formed from three different factors: the individual, the social context within which the individual is situated, and external institutional pressures [e.g., 35]. Cybersecurity researchers have specifically called for an approach that examines three different aspects of the managers' decision-making. Ransbotham and Mitra [22] argue that more research in cybersecurity should seek to understand factors that enable more proactive organizational responses, including managerial, environmental, and organizational factors.

IS researchers have examined the role of institutional stimuli on an organization's decision to adopt technology innovations [e.g., 24, 25, 42]. A close examination of the literature in Appendix A reveals no integrative framework of both institutional theory and UET that incorporates values of personal relevance in depicting the top management's decision towards cybersecurity strategies.

2.3. Upper echelons theory and strategic commitment

Top executives have a critical role in firm performance overall [37–39]. These managers also provide an overarching assessment of the impact of cyber-related risk on their organization. A firm's approach to cybersecurity management requires careful managerial attention through a commitment to the inclusion of cybersecurity issues in the strategic decision-making that is related to the firm's overall performance [46]. Top management commitment is a key piece of the foundation on which organizational strategy is built, and it contributes to differences in organizational performance [24]. As a result, successful strategies tend to require top-level commitment to sustain them over time. Executive commitment indicates purposeful determination to pursue a business strategy that is challenging to attain yet essential for the growth or continued survival of the organization (e.g., for ethics, safety, service quality, sustainability, IS development, project implementation). Research suggests that top management commitment is critical in IS planning and strategy [40], service excellence [41], project management and IS implementations [42], and technology use [35].

Although cybersecurity is a strategic issue [20], few studies explore the drivers of top management commitment to cybersecurity strategies. This kind of commitment has been described as a state of mind that

holds individuals to a line of behavior [43]. It has also been described as the state of being dedicated to a goal, activity [44], or relationship [45]. Furthermore, it represents an obligation to continuously engage and perform in a future action [46]. Commitment in this study represents doing what is necessary throughout the adoption and use of cyberinsurance to manage cybersecurity risks.

2.4. Hypotheses development

From the discussions above, institutional pressures are posited to affect strategic choice through the top manager's concentric values and perceptions that are personally, organizationally, and situationally relevant to the cybersecurity context. Personal factors include *job security* and *breach risk*. Organizational factors include *financial risk* and *transaction cost*, and situational factors include *regulations* and *ambiguity*. Fig. 2 presents the research model for this study.

2.4.1. Personal relevance factors

The personal relevance factor represents the extent to which the strategic decision towards cyberinsurance is relevant to the personal well-being of the top manager [47]. The literature on strategic management suggests that failure to include individual factors and perspectives in organizational performance has weakened our ability to correctly interpret the role or function of the individual in influencing firm performance [37]. Personal relevance addresses the extent to which an individual has a personal stake in the decision or outcome of the decision process [54]. Research indicates that when a person relates the relevance of their decision-making to their own personal interests (e.g., job security, reputation), that person will be more likely to make a decision that supports their own interests [57]. Top managers vary in how they relate strategic decisions to personal interests, thus the nature of their decisions also varies, particularly with regard to risk management. For example, top managers that have more at stake may focus on a risk management strategy that will improve their job outlook, livelihood, performance, or other factors they perceive as being at stake [18,48,49]. In today's environment, top managers are often held accountable for cybersecurity breaches. Deciding not to purchase cyberinsurance could greatly negatively impact a top manager's professional and personal life if a breach occurs. Thus, top managers may opt for cyberinsurance to protect the factors that are personally relevant to them. Therefore, we hypothesize:

Hypothesis 1: Top managers' perceptions of personal risks and benefits are strongly related to their commitment to using cyberinsurance as a risk management strategy.

In this study, the personal relevance factors examined are related to how committing to cyberinsurance personally affects the top manager. We examine personal relevance factors that are not only important to the top management, but also relevant to the cybersecurity domain. One such factor is job security. Job security is an individual moor and has since been associated with long-term financial security and employment. IS research on job security has demonstrated its influence on behavioral intention to leave [50,51]. Also, studies have found that there is a relationship between an individual's perception of job security/insecurity and his or her commitment to a course of action [52].

Furthermore, decision-makers in IT believe their jobs would be lost as a result of a security breach [53]. Top managers in organizations have been demoted or fired due to security breaches [64,65,66]. For example, Sony fired its CEO as a result of a 2014 security breach in that company [65], and the chief security officer, chief information officer (CIO), and CEO of Equifax all retired following that firm's 2017 security breach [54]. Because top manager jobs and pay are often tied to how well they manage firm assets, especially in publicly traded firms, these managers focus on protecting assets, and thus their own jobs and pay [67]. This includes utilizing risk management if they see it as strengthening their job security [58,59]. Top management risk tolerance or engagement in risk mitigation is influenced by their perceptions of job security [55]. UET suggests that because the top managers' livelihoods come from the organization, they are motivated to preserve its continued performance and well-being [18]. Thus, if a top manager believes that risk management activities will provide job security, the likelihood increases that they will engage in those activities. Therefore, we hypothesize:

Hypothesis 1a: Top managers' perceived job security is positively related to their commitment to using cyberinsurance as a risk management strategy.

Although the impact of security breaches on the organization has been established in the literature [56–58], this section's focus is primarily on the personal relevance of the breach to the top manager. There are a few ways that the top manager's perception of the risk severity of a security breach could have personal relevance to the top manager. Perceptual assessment of risks is an important part of the top manager's role [59]. Specifically, assessing the risk of a cybersecurity breach has become one of the most important tasks for top managers [60]. CEOs and boards of directors now have direct oversight of cybersecurity in many organizations [61]. Hence, a cybersecurity breach to an organization might indicate that the top executive does not have a sufficient understanding of security risks. This could be perceived as failed fiduciary responsibility and could impact future employment opportunities for the executive. In addition, cybersecurity breaches often negatively impact a firm's market value and stock prices [56–58], and in turn, the top manager's stock options. Top executives who perceive the severity of the risk of cybersecurity breaches to their personal stock options have been known to take extreme actions, such as dumping their stocks ahead of a breach announcement by their firm [62]. Indeed, top manager's aspirations are largely tied to the amount of their income that is derived from the organization's performance [18]. If a top manager believes that the consequences of a security breach are severe, that manager will seek and use strategies to alleviate the likelihood of a breach. Given that cyberinsurance is known to help organizations recover from security breaches, we expect that top manager's perception of breach risk severity influences commitment to cyberinsurance. Therefore, we hypothesize:

Hypothesis 1b: Top managers' perceived breach risk severity is positively related to their commitment to using cyberinsurance as a risk management strategy.

2.4.2. Organizationally relevant factors

Organizationally relevant factors are organizational risks that top managers interpret to be likely incurred by the organization. Financial losses incurred from cybersecurity breaches come from both direct and indirect costs [76–78]. Damage to the firm's reputation is an example of an indirect cost [63–65]. An example of direct cost is the cost to notify individuals affected by the breach, which can be quite expensive. Notification cost is a key driver of the decision to invest in cyberinsurance [79]. One study argues that cyberinsurance could reduce the cost of data breaches by up to US$4.40 for each record breached [83]. This is a substantial potential cost-saving, and could even mean the difference in a small or medium firm's ability to survive a breach [84].

In addition to notification and reputation costs, organizations incur costs for such things as detection and escalation costs (e.g., forensics, assessment, and audits) and post-breach activities such as remediation, legal fees, and identity protection services. Firms also often incur lost business during and after a breach. It is estimated that by the end of 2021, financial losses due to cyber-attacks will reach $6 trillion per year [66]. As organizations face financial risks, top managers may look for strategies to help their organizations cover these costs. Given that cyberinsurance is known to cover such costs [67], top managers' beliefs about organizational risks and costs pertaining to cybersecurity may influence their commitment to cyberinsurance as a risk management strategy.

Hypothesis 2: Top managers' organizational risks perceptions are strongly related to their commitment to using cyberinsurance as a risk management strategy.

Perceived financial risk refers to top managers' assessment of the

potential for financial loss associated with security breaches. Cybersecurity is a key element of financial risk for most organizations [68]. Thus, top managers must make decisions and take actions to prevent long-term financial losses that may result from cybersecurity breaches [69]. The top manager's role in a firm includes responsibility for assessing and managing risks that could affect the firm's financial performance [70]. Thus, people in this position are increasingly being tasked to assess and understand their organization's financial risks related to cyber-attacks and security breaches. CEOs and top management should be acutely aware of the financial risk involved with cyber-attacks. As the cost of security breaches continues to increase and the costs of managing them also continue to rise, an increasingly prevalent risk management solution is cyberinsurance [69]. Insurance decisions are typically directly related to financial risk, and cyberinsurance is a solid approach to managing and recovering from cybersecurity-related financial losses [71,72]. We argue that when top managers assess the financial risks associated with cybersecurity incidents, it is likely that they will commit to using cyberinsurance as a risk management strategy.

Hypothesis 2a: Top managers' financial risk perception is positively related to their commitment to using cyberinsurance as a risk management strategy.

Transaction costs represent the energy, time, and costs associated with finding, transferring expertise, negotiating, supervising, and establishing a contract between clients and vendors [73,74]. Researchers have explicitly assessed transaction cost (e.g., search cost) from a top manager's viewpoint [17]. Top managers are expected to understand the impact of transaction costs and they often have the ultimate responsibility to determine whether the effort and cost incurred in sourcing, coordination, and monitoring are too costly for their organizations. Transaction costs associated with cyberinsurance may be viewed as expensive, and it is the top manager who decides whether their organization is better off committing or not committing to cyberinsurance.

It is important to consider relevant cyberinsurance transaction cost information because not doing so could lead to decisions that could harm the organization and incur additional costs [92]. Because insurance is a contract between the insurer and the insured, the transaction costs incurred include those generally encountered in the execution of a contract [91]. IS research has examined these costs in other contexts (e.g., outsourcing contracts) and has identified specific categories of relevant transaction costs [91,93]. Drawing on transaction cost theory, we combine *ex-ante* transaction costs (e.g., negotiating) and *ex-post* transaction costs (e.g., haggling, claims) to examine whether transaction cost affects top managers' cyberinsurance decisions.

Ex-ante transaction cost includes search, knowledge transfer, and negotiating costs during the time that the parties to the contract develop a general understanding of contract requirements [91]. This involves the time and effort to identify a vendor, to transfer and integrate knowledge between the insured organization and the insurance provider, and to actually negotiate the contract. Even if others in the organization actually conduct the transaction, it is generally the top manager who makes the final decision. Significant time and effort are required to integrate knowledge during knowledge transfer [91,94], and to draft and negotiate the final contract [95]. If top managers believe that the costs related to searching for an appropriate cyberinsurance product, are too great, they are less likely to commit to cyberinsurance.

Hypothesis 2b: Top managers' cyberinsurance transaction cost perception is negatively related to their commitment to using cyberinsurance as a risk management strategy.

2.4.3. Situationally relevant factors

Situational factors are those outside the control of an individual or organization, and as such, can pose serious constraints on a firm's ability to thrive [72]. Top managers may spend a great deal of time addressing these, especially those related to government regulations [96] and to market uncertainty or ambiguity [97,98]. A top manager's ability to assess these factors helps them to make informed strategic decisions about their firms [72, 98]. Cybersecurity-related situational factors include government regulations that require organizations to disclose cybersecurity breaches [75]. Perceptions of uncertainty and ambiguity are situational factors that have been demonstrated to significantly affect top managers' strategic decisions [59,76]. The cyberinsurance market typically has limited standard pricing models or policies and is often volatile and ambiguous [77,78]. Thus, top managers will likely consider such uncertainty when deciding whether to commit to a cyberinsurance strategy. Overall, a top manager who assesses security breach regulatory requirements and the uncertainties surrounding the cyberinsurance market related to security breaches will be influenced in their commitment to using cyberinsurance as a risk management strategy.

Hypothesis 3: Top managers' situational perceptions are related to their commitment to using cyberinsurance as a risk management strategy.

Ambiguity is the perceived extent of uncertainty in the environment [76]. Ambiguity arises from a lack of understanding about the implications of specific events or business situations [79]. Environments that are novel or highly complex generally present the greatest levels of ambiguity [80]. Following previous literature [76], we define cyberinsurance coverage ambiguity as the extent of uncertainty embedded in the top manager's perceptions of the environmental conditions in the cyberinsurance market. This includes such issues as unclear information, uncertainty about how important particular environmental conditions are, and uncertainty about the future and its impact on the business [81]. Ambiguity is often associated with equivocality, which is a state of misunderstanding, ambivalence, and discrepancies that leave managers uncertain about the inquiries to make [82]. In the cyberinsurance context, for example, top managers may be uncertain about the policies and the types of coverages. Because the cyberinsurance market is relatively new compared with other insurance products, it may lack sufficient actuarial data that insurers routinely use to adequately insure against losses [83]. Furthermore, the content and terminology of cyberinsurance policies are often neither uniform nor consistent [84].

Besides, the emergence of new technologies and markets increases the ambiguity of environments in which organizations operate [79,85]. In the face of emerging technologies and their associated risks, the ambiguity in cyberinsurance policies is also likely to increase. In fact, models have been created to provide guidance on effectively choosing a cyberinsurance product [86]. Therefore, we propose that ambiguity is a barrier to top managers' commitment to cyberinsurance.

Hypothesis 3a: Top managers' perceived cyberinsurance coverage ambiguity is negatively related to their commitment to using cyberinsurance as a risk management strategy.

Regulatory oversight is another situational factor that may be relevant to top managers' commitment to cyberinsurance. For example, the regulatory influence of Sarbanes–Oxley has been known to motivate top managers to require information security-related changes across the organization [8]. Regulatory oversight serves to ensure that people with delegated authority (e.g., top managers) are held responsible [87]. It enables the correction of failures in the market arising out of such things as health, safety, and environmental risks [88]. Regulatory oversight is usually conducted through a government agency that has the ability to supervise organizational actions [88]. Therefore, we define regulatory oversight as the extent to which the actions of an organization are supervised by a government body. Previous research links it to regulatory expectations or the extent to which regulators can mandate rules to guide the relationship between sellers and their customers [89]. Under regulatory expectations, enforcement deters violations, increases the likelihood of fines for violations, and decreases incidents of negative publicity from violations [88]. For example, the prevalence of cyber-attacks and security breaches has led to legislation mandating organizations to disclose security breaches involving data of individuals [75]. Organizations that are subject to regulatory oversight tend to pay

more attention to their internal controls [90]. Requirements for disclosure of security breaches have led to increased investment in cybersecurity [75] and the transfer of breach-related costs to third parties through cyberinsurance policies [91]. Thus, we expect that the top manager's perceptions of regulatory oversight influence their commitment to cyberinsurance. If there were no regulations, there might be little incentive to disclose, thereby limiting the expense associated with disclosure. For organizations that must disclose the breach, top managers are more likely to turn to cyberinsurance to cover the expense.

Hypothesis 3b: Top managers' perceived regulatory oversight is positively related to their commitment to using cyberinsurance as a risk management strategy.

2.4.4. Institutional pressures

According to institutional theory, organizational decisions are subject to many institutional pressures that constrain their behaviors [15]. We define institutional pressures as the extent to which top managers experience the need to commit to cyberinsurance as a cybersecurity strategy by responding to mimetic, coercive, and normative pressures exerted by the institutional environment [92]. We argue that top management perceptions mediate the effect of institutional pressures (mimetic, coercive, and normative) on using cyberinsurance as a risk management strategy when it copies, is coerced by, and embraces as norms the choices other firms, vendors, suppliers have made in their efforts to address cybersecurity risks.

Using cyberinsurance as a risk management strategy often incurs costs and requires that the organizations devote time and effort in understanding their cyberinsurance needs, and continually monitor the cyberinsurance contract [73,74]. There is also uncertainty, ambiguity, and complexity in the extent of the contract's coverage in the event of a security breach [93]. In addition, it may require changes in the organization's cybersecurity structure. For example, organizations have been required to hire chief information security officer (CISO) [94] and maintain certain cybersecurity controls and procedures [1,95]. Given these uncertainties, costs, and structural changes, organizations may not consider committing to cyberinsurance as a risk management strategy unless it senses strong institutional pressures to do so. Using cyberinsurance to protect firms' financial assets and recover from security breach incidents is becoming an institutional requirement [96] for firms that collect, store, or transfer personally identifiable information through a website or application. Indeed, it is common for service contracts to require vendors to carry their own cyberinsurance, especially in IT vendor agreements. Such institutional environments are recognized as informing the organization's strategic decisions through the top manager's perceptions [18].

Although the extant literature has described how top manager's perceptions mediate the impact of institutional pressures on strategic decisions such as ERP assimilation [16] and integrated information delivery [92], it is unclear how such pressures impact cybersecurity strategies through top managers' perceptions. With respect to the top manager's perceptions (e.g., job security, breach risk, financial risk surrounding security breaches), we argue that they are influenced by pressures from the institutional environments. For example, firms from industries, such as financial services and retail (e.g., Equifax, Target) that have experienced security breach incidents have fired their top executives or accepted their subsequent resignations [97]. This implies that organizations mimic, are coerced by, or embrace the norms of other organizations' practices in how they respond to breach incidents. Top managers are the focal point of these institutional pressures, which inform their perceptions and may lead them to re-evaluate their overall perceptions on job security, breach risk, financial risk surrounding security breaches, transaction cost, the ambiguity of coverage, and cybersecurity-related regulations.

Hypothesis 4a–f: Institutional pressures positively influence top managers' perception of (a) job security, (b) breach risk, (c) financial risk, (d) transaction cost, (e) coverage ambiguity, and (f) regulatory oversight.

3. Methodology

This study used a cross-sectional survey method. We tested the proposed model through survey data collected from CEOs from diverse organizations. We also conducted semi-structured interviews of top managers from different organizations to validate the study results. Most constructs are measured using multiple items and with a 7-point Likert scale ranging from 1—strongly agree to 7—strongly disagree. Some open-ended questions were also used to better access respondents' understanding of the research constructs.

3.1. Measurement

All measurement items are summarized in Table B1 in Appendix B. Table B2 in Appendix B shows the operationalization of the constructs. We use previously validated measures, however, one of the constructs required new items that capture the content, context, and domain of the study. Following the Moore and Benbasat [98] procedure, we constructed measures for *regulatory oversight* by drawing on the regulatory provisions by both the Office of National Coordinator for Health Information Technology and National Transportation Safety Board. The former provides regulatory oversight for health information, and the latter provides oversight for transportation regulation. We used Cohen's kappa to assess inter-rater reliability [119]. Cohen's kappa was 0.93, which indicates adequate agreement.

The survey items were pretested by asking university students who were also asked to provide feedback about the questions, voice concerns, and describe perceived ambiguities in wording. In addition, at the request of one of the authors during a work-study program, a panel of experts in the cybersecurity risk and cyberinsurance domain reviewed the measurement items and suggested updates. Survey questions were revised based on comments received.

We also measured several control variables: organizational tenure, industry, organization size (number of employees, revenue), and experience in technology management. Organization tenure is included because research indicates that it may impact outcomes and commitment [99]. Prior research has included similar control variables in studies about management commitment and support [121, 122]. We include industry because top management commitment to security risk mitigation may differ if their industry is regulated such as in the finance or healthcare industries [see 100]. Given that organizations usually use alternative vehicles to mitigate cybersecurity risk, we also include these as controls in the model: other types of insurance products (e.g., general insurance), technology controls, and processes (e.g., backup, encryption, security policy, governance). Two dummy variables are used for measuring these two categories: technology alternatives (TALT) and other insurance alternatives (IALT). Each of the model's control variables is a single-item measure.

3.2. Data collection

A field survey was administered to executive-level managers to understand the factors that facilitate their commitment to cyberinsurance. They are the most likely people in their organizations to be knowledgeable about the positioning strategy of cyberinsurance in the organization. This is consistent with the key informant approach, in that, the most knowledgeable individual in the organization with regard to the topic studied is surveyed [101]. Furthermore, because security risks have risen in importance to organizations [20], the expectation is that top managers should understand how to manage cybersecurity risks [102].

Response rates for surveys involving top managers have declined over the years for many reasons including lack of time or lack of interest in the topic [103]. Despite this, there have been studies that have successfully surveyed executives with adequate response rates [e.g., 104]. Evidence also suggests that several factors increase the likelihood of

Table 1
Profile of respondents.

Category	Frequency (%)	Category	Frequency (%)
Industry		*Employees*	
Manufacturing	13 (8.6)	10,000 or more	4 (2.6)
Banking	4 (2.6)	5000–9999	14 (9.3)
Finance	8 (5.3)	1500–4499	7 (4.6)
Insurance	3 (2.0)	500–1,499	16 (10.6)
Retail	19 (12.6)	100–449	32 (21.2)
Transportation	2 (1.3)	50–99	19 (12.6)
Education	4 (2.6)	10–49	59 (39.1)
Technology	26 (17.2)		
Health	7 (4.6)	*Previous Knowledge*	
Government	2 (1.3)	Yes	127 (84.1)
Services	47 (31.1)	No	24 (15.9)
Other	16 (10.6)		
Revenue (U.S. million dollars)		*Other controls*	
$5 Billion or More	3 (2.0)	Self-insurance	66 (43.7)
$1 Billion–Under $5 Billion	13 (8.6)	Technology	122 (80.8)
$250 Million–Under $1 Billion	7 (4.6)	Other insurance	67 (44.4)
$100 Million–Under $250 Million	6 (4.0)	Security policies and governance	57 (37.7)
$50 Million–Under $100 Million	9 (6.0)	None	2 (1.3)
$15 Million–Under $50 Million	6 (4.0)		
$10 Million–Under $15 Million	11 (7.3)		
$5 Million–Under $10 Million	20 (13.2)		
$1 Million–Under $5 Million	48 (31.8)		
Under $1 Million	28 (18.5)		

Table 2
Reliability and convergent validity.

Construct	Cronbach's α	Composite Reliability	AVE
AMB	0.948	0.960	0.828
COMM	0.956	0.968	0.885
FIN	0.908	0.931	0.729
INSP	0.941	0.949	0.650
JSEC	0.943	0.959	0.854
REG	0.946	0.957	0.787
SEV	0.908	0.936	0.784
TXNC	0.944	0.958	0.851

Note: AVE = average variance extracted;;COMM= commitment to using cyberinsurance as a risk management strategy; AMB = ambiguity of cyberinsurance; FIN= financial risk; REG = regulation oversight risk; TXNC = transaction cost; SEV = breach risk severity; JSEC = job security; INSP= institutional pressures

responses from top executives including interest in the topic [103], monetary incentives, legitimate authority, and the low number of survey items [105]. In light of these, survey participants were recruited through a paid Qualtrics Panel. This is a service that matches researchers' sampling requirements to willing survey participants. Monetary incentives were offered through Qualtrics, and the number of survey items was reduced. Because cybersecurity is a top strategic issue facing executives [20], the salience of the topic of our study—cybersecurity and cyberinsurance—may have influenced and increased the visibility of our study, and in turn, the number of responses received [103]. A total number of 151 CEOs in the US participated.

To address possible concerns about social desirability and reporting their behavior, the survey stated that there were no right or wrong answers and asked participants to answer as honestly as they could. They were also informed that their responses were anonymous and that they would be aggregated for analysis and reporting. Table 1 summarizes the sample demographics. The survey respondents represent a broad sample of industries, the number of employees in the organization, and annual organizational revenue.

4. Data analysis and results

Using SmartPLS 3.0 as one of partial least squares (PLS) techniques [106], we analyzed the model. PLS is suited for testing reflective and formative factors in the same model [107]. Prior to examining the structural model, we evaluated the measurement model. We performed analyses to check the reliability and convergent validity of the measurement model. The results are summarized in Table 2. Cronbach's α for each construct is above the recommended value of 0.70 [108] and ranges from 0.908 (FIN) to 0.956 (COMM). Composite reliability ranges from 0.931 (FIN) to 0.968 (COMM). Average variance extracted (AVE) is greater than 0.50 for each of the constructs [109,110], ranging from 0.650 (INSP) to 0.885 (COMM), which provides support for adequate convergent validity. We used multiple approaches to evaluate discriminant validity. First, we used the approach recommended by Fornell and Larcker [110] and determined that the square root of each construct's AVE to be higher than the correlations between each pair of constructs in rows and columns in Table 3. Second, we used the heterotrait–monotrait (HTMT) ratio approach suggested by Henseler et al. [111]. Finally, we compared the loadings of an item on its hypothesized construct to its cross-loading on other constructs. All items loaded on their hypothesized constructs more strongly than they cross-loaded on other constructs (see Appendix C). The results of these methods suggest that there are no major measurement issues in the research constructs.

The variance inflation factor (VIF) was used to assess the extent to which multicollinearity was present. The VIF values are below the most conservative threshold of 3.00 [135] (AMB - 1.48., FIN - 1.95, JSEC - 2.07, REG - 1.57, SEV - 2.25, and TXNC - 1.45). In addition, we performed a test of autocorrelation using the Durbin–Watson statistic. The resulting value of 1.94 is well within the 1.5 and 2.5 rule-of-thumb, and thus, the data are likely not autocorrelated.

4.1. Common method bias

To assess common method bias (CMB), we used Harman's one-factor

Table 3
Convergent validity and correlations.

Construct	AMB	COMM	FIN	INSP	JSEC	REG	SEV	TXNC
AMB	0.91							
COMM	0.11	0.94						
FIN	0.21	0.60	0.85					
INSP	0.34	0.76	0.60	0.81				
JSEC	0.11	0.77	0.51	0.72	0.92			
REG	0.14	0.49	0.45	0.58	0.51	0.89		
SEV	0.24	0.67	0.65	0.66	0.63	0.34	0.89	
TXNC	0.55	–0.03	0.16	0.29	0.04	0.27	0.16	0.92

Note: COMM = commitment to using cyberinsurance as a risk management strategy; AMB = ambiguity of cyberinsurance; FIN= financial risk; REG = regulation oversight risk; TXNC = transaction cost; SEV = breach risk severity; JSEC = job security; INSP= institutional pressures

Table 4
Path analysis results.

	Path Coeff.	f^2	S.D.	t-stat	p-value	CI 2.5 %	CI 97.5 %	Result
H1: Individually relevant factors								
H1a: JSEC → COMM	0.438	0.333	0.076	5.778	0.000	0.283	0.581	Accept
H1b: SEV → COMM	0.217	0.074	0.079	2.749	0.006	0.056	0.365	Accept
H2: Organizationally relevant factors								
H2a: FIN → COMM	0.179	0.059	0.075	2.399	0.016	0.049	0.338	Accept
H2b: TXNC → COMM	–0.199	0.086	0.061	3.256	0.001	–0.316	–0.074	Accept
H3: Situationally relevant factors								
H3a: AMB → COMM	0.051	0.006	0.058	0.877	0.381	–0.063	0.165	Reject
H3b: REG → COMM	0.129	0.038	0.058	2.218	0.027	0.021	0.247	Accept
H4: Institutional pressures								
H4a: INST → JSEC	0.722	1.086	0.047	15.501	0.000	0.625	0.805	Accept
H4b: INST → SEV	0.660	0.770	0.056	11.876	0.000	0.542	0.759	Accept
H4c: INST → FIN	0.604	0.575	0.064	9.386	0.000	0.475	0.729	Accept
H4d: INST → TXNC	0.270	0.079	0.105	2.565	0.010	0.010	0.433	Accept
H4e: INST → AMB	0.323	0.117	0.073	4.425	0.000	0.191	0.475	Accept
H4f: INST → REG	0.578	0.503	0.060	9.589	0.000	0.457	0.694	Accept
Controls								
TECHEXP → COMM	0.097	0.028	0.050	1.940	0.052	–0.006	0.19	-
TENURE → COMM	–0.190	0.103	0.073	2.592	0.010	–0.313	–0.028	-

Note: COMM= commitment to using cyberinsurance as a risk management strategy; AMB = ambiguity of cyberinsurance; FIN= financial risk; REG = regulation oversight risk; TXNC = transaction cost; SEV = breach risk severity; JSEC = job security; INSP= institutional pressures

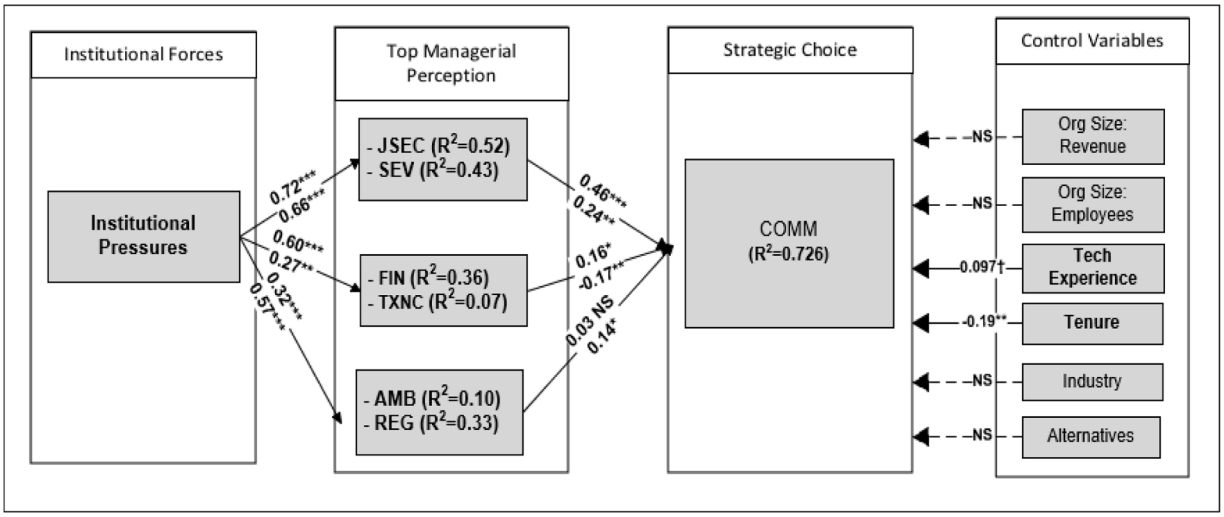


Fig. 3. Structural model paths.
Note: ***$p < 0.001$, ** $p < 0.01$, * $p < 0.05$, $^{\dagger}p < 0.10$, NS: not significant

test [136] and a factor-based partial least squares structural equation modeling (PLS-SEM) full collinearity test [137]. Using Harman's one-factor test, we included all reflective items in a principal components factor analysis. The largest factor variance of 38.4% indicates that no one factor accounted for a majority of the variance. The factor-based PLS-SEM algorithm accounts for measurement errors to assess variance maximization issues that are often found in classic PLS-SEM assessments. This test resulted in VIF values below the threshold of 5 [112, 113]. A fuller explanation of the tests is provided in Appendix C. Overall, these tests support that the measurement model meets the standards expected in IS research [114].

4.2. Structural Model Results

We applied bootstrap resampling to estimate structural model path coefficients using 5000 resampling cases and the bias-corrected bootstrap confidence interval. Results, including the standardized regression weights and significance levels, are provided in Table 4.

Findings indicate that the relationship between job security (JSEC) and commitment to cybersecurity (COMM) is statistically significant ($p<0.001$), supporting H1. The relationship between the individual factor of security breach (SEV) and COMM is also significant ($p < 0.01$), which lends support for H2. The significant relationship between the organization risk factor (FIN) and COMM ($p < 0.05$) lends support for H3. The organizational factor, transaction cost (TXNC), is significantly related to COMM ($p < 0.05$), which lends support to H4. The situational factor, the ambiguity of cyberinsurance (AMB), however, is not significantly related to COMM. Thus, results do not support H5. Regulatory oversight (REG) and COMM are significantly related ($p < 0.05$), lending support for H6. Finally, there is a significant relationship between institutional pressures (INSP) and job security ($p <0.001$), breach risk severity ($p <0.001$), financial risk ($p <0.001$), transaction cost ($p <0.01$), ambiguity ($p <0.001$), and regulatory oversight ($p <0.001$), which lends support to H4a–H4f. The final paths are provided in Fig. 3. COMM has an R^2 of 0.726 and an adjusted R^2 of 0.710.

We assessed effect sizes for each significant relationship. With regard to the effect of top managers perceptions on commitment, JSEC had a medium-high effect size ($f^2 = 0.333$) followed by small effect sizes for TXNC ($f^2 = 0.086$) and SEV ($f^2 = 0.074$). Thus, these seem to be of greater importance than the other effects. With regard to the effect of

Table 5
Mediation analysis.

	Coeff.	S.D.	T Stat	P-Value	CI 2.5 %	CI 97.5 %	Zero
INST → JSEC → COMM	0.334	0.066	5.037	0.000	0.207	0.467	No
INST → SEV → COMM	0.158	0.056	2.842	0.005	0.050	0.273	No
INST → FIN → COMM	0.100	0.055	1.821	0.069	0.012	0.233	No
INST → TXNC → COMM	–0.047	0.024	1.937	0.053	–0.102	–0.006	No
INST → AMB → COMM	0.013	0.021	0.603	0.546	–0.020	0.063	Yes
INST → REG → COMM	0.084	0.039	2.126	0.034	0.013	0.164	No

Table 6
Interviewee demographics.

Company name	Industry	Users	Tenure (year)	Job Title
Pharma	Pharmaceuticals	5500	17	Vice president
Health Consulting	Healthcare	500	20	CEO
Healthcare	Healthcare	5,000	5	Senior vice president
Financial	Financial	100,000	4	Executive director
Health Software	Healthcare	500	3	Chief privacy officer
Health Software	Healthcare	500	4	VP information security
Managed IT	Managed Serv.	7000	1	CIO

institutional pressures on top managers' perceptions, the effect sizes for JSEC, SEV, FIN, and REG were large (> 0.4), and the effect sizes for TXNC and AMB were small (0.1).

In our assessment of the role of control variables, findings indicate that technology experience is marginally significant in its relationship to COMM, which provides support that top managers' technology management experience may influence their commitment to cyberinsurance. Tenure also is significantly related to COMM, but the relationship is negative. This suggests that the more years a top manager has worked, the less likely they are to commit to cyberinsurance as a risk management strategy. Using confidence intervals in the bootstrap method, we tested for mediation of top managers' perceptions [115]. Doing this allows testing of mediation as opposed to testing indirect relationships [116]. The coefficients for the values between the independent variables and dependent variables are calculated simultaneously. We looked to see whether there was a value of zero in the confidence interval; if not present, there is 95% confidence that mediation exists [116]. The results indicate that institutional pressures are indeed mediated by perceptions of job security, breach risk, financial risk, transaction cost, and regulations, but are not mediated by the ambiguity of coverage (Table 5).

4.2.1. Post hoc interviews with senior executives

We performed post hoc interviews with top managers of different organizations to further explore their views related to the nomological network in our study. The qualitative interviews include top executives outside of the survey sample, which reduces the possibility of influencing the original survey instruments on the interviewers as well as supports the external validity of our study [92] The interviewees are from medium to large organizations from different sectors. We conducted seven semi-structured interviews with six case sites. The executives include CEO, vice president, chief privacy officer, etc (see Table 6 for their demographics).

Overall, the interviews support our hypothesized relationships. Specifically, the interviews confirmed that forces surrounding organizational decisions regarding cybersecurity strategies are subject to the normative, mimetic, and coercive pressures exerted by other organizations, institutions, partners, and vendors. In addition, organizations effectively use cyberinsurance as a cybersecurity strategy.

"*Essentially, how we implement security strategies is driven by three things, regulatory environment, commercial environment (i.e., customer contracts), and industry standards, that is we look at the minimum required to be considered reasonable. Doing a true assessment to mitigate threat involves technologies, training, and cyberinsurance.* " *(VP of Information Security of Healthcare Software Company)*

"*With PCI, there are fines and penalties associated with it. Insurance is a requirement to do business. HIPPA 162–164 are also requirements. Sometimes, we are driven by best practices from other organizations and the industry. For example, NIST drives a lot of the things we do here. In addition, it needs to align with the corporate strategy.* " *(Executive Director, Financial Services)*

"Cyberinsurance is a business requirement. You have to have it. It became a service level agreement." *(CEO, Healthcare Consulting)*

When asked about the role of personal risks such as job security in their cybersecurity strategies, especially cyberinsurance, these senior executives note the following:

"*It is at the back of everyone's mind. Anything that catastrophic will weigh on people and should affect one's job.*" *(CIO MSSP)*

"*The role of the CIO and CFO is to present the risk exposure to the CEO and the board. They present the options to close the gap. If they don't, their job should be on the line. Anyone with a C in their title is paid to manage the risks and the issues in the organization. Their jobs are on the line to manage the risk.* " *(CEO, Healthcare Consulting)*

"*Anthem breach got our leadership to invest money into security. OPM breach also helped in pushing our CEO and the board. If the consequences are severe, they should lose their jobs. Some of them deserve to lose their jobs because of a breach. Some of the breaches are based on incompetence of the leadership and so they need to lose their jobs.*" *(Executive Director, Financial Services)*

"*My experience with breaches in organizations where top people were impacted was because the organization wanted to show that the organization was doing something or making a change, and not necessarily because the organization actually made a change.*" *(Vice President, PharmA)*

Consistent with our argument earlier about the perception of organizational risks, these executives indicated that the high implications and the financial cost of breaches are the reasons for using cyberinsurance risk management. They also note that these implications can be especially devastating for smaller firms.

"*We leverage cyberinsurance because the cost of breaches can be high. In the healthcare space there are legacy systems that don't necessarily have testing and validations completed on them. My organization is also performing acquisitions and mergers with organizations that do not have expertise in security or how to address the issues that arise out of it.*" *(Vice President, PharmA)*

"*Financial risk has to feature into the decision for cybersecurity strategy. Because of the integration of cloud, IoT, and legacy systems that are expensive to evolve and maintain, the financial risks would feature in the cybersecurity strategy. These fit into the strategy of the organization and it is up to the board.*" *(Executive Director, Financial Services)*

"*The risk of a breach exceeds the dollar value and equity value of organizations we do business with today. The challenge of data breach is with big and small organizations. However, the smaller the organization, the harder it is, in fact, the breach can put them out of business. In 2006, we had a multimillion-dollar contract with another healthcare organization. Today, our organization would not have been able to sign that deal because of the requirements to comply with security requirements. Don't know how we would have been able to do it if this was now.*" *(CEO, Healthcare Consulting)*

"*We do security to protect ourselves, we might be sued if our customers loose data through a breach. So it weighs on us. Assuming it costs $0.50c to mail letters to their 40 thousand customers, that is a lot of money. Also, assuming that it cost $50 per person to pay for monitoring services after a*

breach, that is a lot of money. We don't want to be sued. We definitely discuss these things with our clients. The thing is that it can cost about $50,000 to implement and protect their organization but may cost $5,000,000 to recover from a breach. We have cyberinsurance. We have to cover for us and our customers as well. We took out a coverage of $2 million per incident for our customers. We also have cyberinsurance of $4M for our own organization. We offer cyberinsurance to our customers, but many of them say they don't want it." *(CIO MSSP)*

More importantly, their perceptions of regulations also played a critical role in their cyberinsurance and overall cybersecurity strategies.

"*HIPAA establishes the baseline. We then go above HIPAA. We also adopt the recommendations from NIST. We generally default to HIPAA and NIST. I would say that SOX (802/1102) is where we started seeing key leadership individuals liable for records retention. In a previous experience, part of my job was to keep the CEO out of jail. When the CEO is held liable for proper security strategies, this is when it becomes important.*" *(VP of Information Security of Healthcare Software Company)*

"*Regulations drive strategies. It drives a lot of strategies. The penalties can be high especially for health care related organizations.*" *(CIO MSSP)*

"*The board should make the decision and not the government on whether to purchase cyberinsurance*" *(CEO, Healthcare Consulting)*

When asked about uncertainties around the events covered by cyberinsurance, some senior executives confirmed the influence of coverage ambiguity and uncertainty on their commitment to using cyberinsurance as a risk management strategy, while others expressed general unconcern.

"*A lot of people don't understand what's covered in their policy and what's not. Organizations need to be careful when they look at plans, because they may have exposure because of not carefully looking at their plans. They should read the policies to understand the exposures and whether not applying MFA, for example can constitute a denial. Organizations have been denied payment because they did not implement certain practices in their organizations. Insurance companies decline payment because the insured do not read the policies. Nobody knows what's included and excluded in these policies. I review the cyberinsurance policies to ensure that they provide adequate coverage*" *(CIO MSSP)*

The senior executives that expressed general unconcern about cyberinsurance coverage noted the following:

"*With a company of our size, we have no power to negotiate our coverage. I am not worried about coverage. Our cyberinsurance policy exists to check the box that we carry insurance.*" *(VP of Information Security of Healthcare Software Company)*

Our real risk is reputational risk and no amount of insurance coverage can cover reputational risk. Anthem had cyberinsurance when they were breached. This impacted their assets. If our organization has that kind of breach, it would kill us. Size matters. With a large company like Anthem, a breach may not affect them as much, but with a company of our size, we would die. (Chief Privacy Officer, Healthcare Software Company)

5. Discussion

We sought to understand top managers' commitment to cyberinsurance as a risk management strategy. The empirical results confirm most of the predictions in our model and highlight the importance of individual, organizational, and situational factors in top managers' commitment. Specifically, findings suggest that top managers' perceptions mediate the influence of institutional pressures on their commitment and use of cyberinsurance as a risk management strategy.

Individual factors (i.e., job security and perceived breach risk severity) were more strongly related to this commitment than either organizational or situational factors. In other words, top managers' desire to protect their personal well-being [47] seems to have the greatest impact on their commitment to a cyberinsurance risk management strategy. Our findings confirm agency and expectancy theories that suggest that managers are interested in investments that protect the firm's assets and, therefore, that also protects their personal interests such as job security and salary [68]. This highlights the importance of personal relevance in the top manager's commitment to risk management approaches, which is different from personal relevance in employee security behaviors [47,117]. Top managers have different inherent responsibilities than other employees, and the severity of the consequences of failure to ensure a good security risk management strategy may be more severe. Most employees do not have security risk management responsibilities in their job descriptions, and sanctions for them are often social sanctions as opposed to sanctions involving future careers and income that top managers face. Top managers have fiduciary responsibilities and are often held directly accountable to organizational stakeholders; thus, the consequences are more severe. This work provides new insights into top managers' roles in the context of cybersecurity research. It also provides a foundation to conduct future research that explores and theorizes the *characteristics of top managers' roles and responsibilities* in order to more fully understand the severity of the threat to their employees and why it may or may not affect their decisions.

Concerning organizational factors, financial risk and transaction cost significantly influence commitment to cyberinsurance. Security issues pose a substantial financial impact on organizations [e.g., 64]. Indeed, financial losses incurred from security breaches have remained a primary motive for cybersecurity research [118]. This study, however, takes a different perspective and specifically examines potential financial loss from the perspective of the top manager who is responsible for managing all cybersecurity risks, including financial risks that may affect the performance of the organization. Our findings provide a foundation on which to further build the cybersecurity risk management research stream, one that focuses on the top manager's perspective. Future research is also needed to examine the influence of financial risk perception on other security risk management strategies. Transaction cost was particularly salient, reflecting that transactional cost saving is a strong rationale for a risk management strategy. The evidence of the strong influence of transaction cost on strategic commitment is consistent with prior research that has examined the influence of transaction cost on strategic contracting and outsourcing decisions [119,e.g., 120]. For example, Ang and Straub [120] argue that top managers should be aware of the need to factor in the effort, time, and costs involved in assessing the benefits the organization may receive from cyberinsurance. Top manager commitment to cyberinsurance is expected to be tempered by the extent of transaction costs incurred in searching for, negotiating, and monitoring a cyberinsurance contract.

Concerning situational factors, cyberinsurance ambiguity was not significantly related to commitment. This suggests that decision-makers do not consider cyberinsurance ambiguity as a factor in their commitment to cyberinsurance. Though surprising, this result was confirmed through post hoc interviews of some senior executives who expressed unconcern over the uncertainty of cyberinsurance coverage. The interviews also suggest that irrespective of the cyberinsurance ambiguities, using cyberinsurance as a risk management strategy is fueled more by other factors such as appeasing investors and regulators (regulatory oversight). Contrary to previous notions that cyberinsurance market conditions (characterized by difficulty in estimating cyber losses and risks) are related to reduced cyberinsurance use by managers [4], our results indicate that individual factors (such as job security and regulatory oversight) are key determinants of commitment. Thus, our findings lend support to the notion that cyberinsurance market conditions alone (situational factors) do not drive strategic commitment to cyberinsurance. More research is needed that explores the effects of other aspects of cyberinsurance market conditions.

The strong relationship between regulatory oversight and commitment to cyberinsurance confirms previous findings about the effect of regulatory compliance and requirements on strategic decision-making [e.g., 59,121]. In comparison, Kwon and Johnson [75] find that regulations can result in counterintuitive reactions in firms. For example, regulations can be effective in providing problem-solving strategies, yet

they can also reduce an organization's ability to be pre-emptive in making decisions. An environment with no regulatory requirement for breach disclosures means that few organizations will disclose breaches. Hidden breaches mean less actuarial data available for insurance companies to draw upon in setting rates, and thus lead to higher insurance premiums. On the other hand, regulatory requirements ensure that organizations disclose security breaches. When organizations disclose breaches, they might as well acquire cyberinsurance to cover the losses incurred from the breach. As such, regulatory requirement and oversight prompts top managers to expose breaches and motivates their commitment to cyberinsurance. Furthermore, when an organization submits a cyberinsurance claim, this decreases its ability to hide the breach [4], which may correct the perception of an overpriced cyberinsurance market and decrease information asymmetry between the insured organization and the insurance companies. It is important to note that just because an organization adopts cyberinsurance does not mean that they will file claims when they suffer a security breach. Indeed, organizations do not often file cyberinsurance claims [77] because doing so might expose their security operations and damage the organization's reputation. Even though an organization has acquired cyberinsurance to assuage investors and regulators, they might choose to not file claims. As such, in order to more fully understand the top manager's commitment to cyberinsurance, future research could expand on commitment by including items that account for extent of claim filings.

Our results also confirm that institutional pressures from other organizations, vendors, and partners affect top management perceptions. Thus, it is consistent with findings reported by Kettinger et al. [92] and Hsu et al. [25]. In addition, our findings support Angst et al. [122], that note that institutional pressures are predictive of technology-related practices in an organization. This study also contributes to the integration of both UET and institutional theory in a single research [e.g., 16], confirming that top management perceptions and values mediate institutional pressures in strategic decision-making. Our qualitative interviews further reinforce the quantitative results. Regarding control variables, technology management experience significantly (marginal) influenced commitment. This finding supports prior literature that suggests that the top manager's technology experience affects the performance of their organization and especially regarding monitoring and reporting security breaches [123]. As more top executives are expected to commit to cybersecurity strategies [124], prior IT experience may become an asset or requirement for top managers. We also find that longer tenure is negatively related to commitment, indicating that top managers who have spent a long time at their jobs tend to not commit to cyberinsurance.

5.1. Theoretical implications

This study has some implications for future research. First, by incorporating multiple dimensions of the values and perceptions (individually related, organizationally related, and situationally related), this study extends beyond traditional conceptualizations of upper echelons in IS research. This is one of few studies that empirically investigates how values and cognitive elements of top managers lead to cybersecurity strategies—which are strategic choices made by top executives. Most scholarly research on UET in IS has focused on the effects of top executive background (demographic and experiential) characteristics on strategic choice [e.g., 12]. In addition, this research follows previous recommendations to evaluate these three components in cybersecurity research. For example, the literature on top manager decision-making [33] argues that because executives are constrained by environmental, normative, and inertial limitations, an investigation into the executives' decision-making should be determined by three sets of factors: the environment, the organization, and the individual executive [34].

Because this study bridges UET, institutional theory, perspectives from the expectancy-valence framework [32], and the cybersecurity literature [22], we believe that it provides more comprehensive insight and evidence of the top manager's decision-making towards a cybersecurity strategy. As such, in order for decision-makers to commit to cyberinsurance as a risk management strategy, their commitment should be based on these components (individual, organizational, and situational). Consequently, we believe that this study will have an impact on future studies in the area of cybersecurity strategic decisions by top managers.

Individual, organization, and situational factors may all be required to increase the top manager's commitment to cyberinsurance. Considering only the organization-related risks alone or situational risks alone without the individual aspect may decrease the strength of commitment, and may not fully capture the concentric factors surrounding the top manager's decision-making. The expectation is that when upper echelons or top management decisions are used to explain a phenomenon, researchers should consider incorporating these three value and cognitive components as they may provide a more comprehensive view of what and how the decision-maker arrives at a certain decision. Also, as more studies are conducted that examine the top manager's perspective in cybersecurity, it should include this concentric view.

Second, cybersecurity research has often examined security behaviors from the perspective of employee behavior, such as compliance with security policies. By examining the top manager's perspective, we demonstrate that cybersecurity decisions should also highlight the top managers who are responsible for the strategic decisions utilized by employees. Top managers' commitment influences the risk management strategies that their organizations pursue. Consequently, we add insight about top manager decision-making to the cybersecurity literature [e.g., 125], and we extend this literature by positing a risk transfer strategy. With employee perspectives predominant in the literature, top managers' views on cybersecurity create a balanced research agenda. Furthermore, it may be important to examine both views in a single study because the two views do not always correspond or complement each other. Such research could help top managers find and close gaps where their cybersecurity impact communications fall short. Accordingly, using our model and findings as a backdrop, future research could empirically examine both the top manager and employee views.

Third, much of the cybersecurity research has focused on deterrence, prevention, and responses to security issues through the examination of related procedures, processes, or technologies [e.g., 2,3,126]. These, however, are primarily mitigation-based risk management approaches, and as such, they are limited in providing an overall solution [127,128]. This study extends the literature about security risk transfer strategies such as pooling, hedging, and relying on insurance [12].

5.2. Practical implications

An organization's shareholders may generate insights from the finding that individual factors such as job security are more strongly linked to top manager's commitment to a risk management strategy, than situational and organizational influences. Shareholders may leverage this insight to incentivize top managers' decisions about managing security risks by focusing more on the job security of the top manager than situational or organizational factors.

With respect to the influence of financial risk and breach risk severity on commitment, the outcome of this study should be interesting to CIOs and CISOs who have technology and security responsibilities. Considering that top managers (e.g., CEOs) are concerned about the financial impact and severity of cybersecurity breaches, being able to capture the severity of breaches in monetary and business-relevant terms (e.g., the effect on customer purchase, subscription, safeguarding contracts, mergers and acquisitions (M&A), intellectual property) that relate to the CEO's fiduciary responsibilities [124] may garner more attention and commitment from the CEO. Thus, CIOs and CISOs looking to engage the CEO to commit or make cybersecurity investments should do so using language (e.g., financial risk) that elicits attention and commitment. Our findings also show that transaction cost served as a formidable barrier to

Table B1
Survey instruments.

	Measurement items
Ambiguity	AMB1: It is difficult to understand what risks are being insured through cyberinsurance
	AMB2: There is often a lack of common language in the meaning of cyber incidents covered in cyberinsurance
	AMB3: There is difficulty in fully understanding the risk and appropriate cyberinsurance coverage
	AMB4: There is a lack of clarity about the limits of coverage on cyberinsurance policies
Commitment	COMM1: I am committed to supporting efforts in adopting cyberinsurance for managing security risks
	COMM2: I encourage the use of cyberinsurance for managing security risks
	COMM3: I am committed to a vision of adopting cyberinsurance for managing security risks
	COMM4: The use of cyberinsurance for managing security risks is important to our organization
Financial Risk	FIN1: Lead to a financial loss due to notifying affected individuals, public relations, fines, etc.
	FIN2: Subject our organization to financial loss
	FIN3: Lead to a financial loss due to reimbursing customers for fraudulent charges
	FIN4: Expose our organization to suffer financial loss due to reporting requirements or legal fines
	FIN5: Lead to a financial loss due to lost revenue (dropped)
Job Security	JSEC1: Cyberinsurance protection will protect my job
	JSEC2: Cyberinsurance protection will help control the undesirable events that might affect my job
	JSEC3: Cyberinsurance protection will offer me continued long-term job security
Regulatory Oversight	REG1: Defines specific operational activities that must be followed by our organization
	REG2: Oversees and supervises our organization's operations and actions
	REG3: Specifies objectives and outcome criteria that govern our operations (e.g., data breach notification)
	REG4: Takes action to hold our firm accountable for the performance and safety of our products and
	REG5: Works closely with our firm to remedy and conform to regulated actions (e.g., data breach notification)
Security Breach severity	SEV1 If our organization's business operations were to be disrupted from a security breach, it would be severe
	SEV2: If our organization were to lose customers from a security breach, it would be serious
	SEV3: If our organization were to cover the costs of a security breach incident, it would be significant
	SEV4: If our organization's security is breached, it would be expensive to recover (dropped)
Transaction Cost	TXNC1: The cost of negotiating a cyberinsurance contract would be too much
	TXNC2: The cost of monitoring and verifying the cyberinsurance contract details would be too much
	TXNC3: The cost of transferring knowledge about our organization's security to the cyberinsurance company would be too much
	TXNC4: In general, it would be a hassle contracting with a cyberinsurance company
Institutional Pressures	COE1: Our relationships with business partners may be threatened, if we are not willing to adopt cyberinsurance
	COE2: We may be willing to adopt cyberinsurance, because we are subject to contractual obligations or negative sanctions
	COE3: If we are willing to adopt cyberinsurance, concessions may be granted, or desirable consequences may arise
	COE4: If we are willing to adopt cyberinsurance, we may receive support and assistance in technological aspects
	MIM1: Our organization may follow our competitors' actions, and adopt cyberinsurance
	MIM2: Our organization follows or imitates the behavior of other firms within our network
	MIM3: Our organization tends to follow our main competitors in engaging in collective sense-making
	MIM4: Our organization follows the trend of our main competitors
	NORM1: Participating in some cyberinsurance promotion events generates some pressures on our organization to adopt cyberinsurance
	NORM2: Other organizations may exert some pressures on our organization to adopt cyberinsurance
Control Variables	InfoSec Management: How many years of experience do you have in information security management?
	Technology management: How many years of experience do you have in technology management?
	Tenure: How many years have you been in your current position?

Table B2
Construct measurement and indicator type.

Construct	Operationalized Definition	Type	Items adapted from
Commitment to cyberinsurance	The extent to which the top manager is committed to the use of cyberinsurance to manage security risks in their organization.	R	[35]
Regulatory oversight	The extent to which the individual believes that a government agency has regulatory oversight over the organization's activities	R	Developed in relation to previous literature
Job security	The perception of whether cyberinsurance will protect their job, offer continued long-term job security, and control the undesirable events affecting the job.	R	[133,51]
Breach risk	The degree to which the top manager believes that the consequences of the security breach would be severe	R	[134]
Financial risk	The degree to which there is potential for financial loss associated with security breaches	R	
Transaction cost	The effort, time, and costs associated with searching, knowledge transfer, creating, negotiating, monitoring, and enforcing a cyberinsurance contract between the organization and insurance vendor.	R	[135]
Cyberinsurance coverage ambiguity	The degree of uncertainty inherent in perceptions of the state of cyberinsurance coverage.	R	[76,92]
Institutional pressures	The degree that commitment to cyberinsurance is based on mimetic, coercive, and normative pressures exerted by the institutional environment.	F	[17]

Note: R = reflective, F = formative

Table C1
HTMT ratio of the correlations.

	AMB	COMM	FIN	JSEC	REG	SEV
COMM	0.119					
FIN	0.221	0.638				
JSEC	0.102	0.795	0.521			
REG	0.156	0.516	0.445	0.549		
SEV	0.274	0.675	0.72	0.639	0.361	
TXNC	0.586	0.091	0.15	0.075	0.274	0.17

commitment, thus, suggesting that lower transaction costs in searching and contracting with cyberinsurance carriers may present an opportunity for insurance companies to seek better ways to streamline the acquisition and contracting of their services. Furthermore, our findings

Table C2
Confidence intervals of HTMT.

	Original Sample	Sample Mean	2.50%	97.50%
COMM → AMB	0.119	0.145	0.05	0.296
FIN → AMB	0.221	0.238	0.086	0.423
FIN → COMM	0.638	0.639	0.463	0.793
JSEC → AMB	0.102	0.127	0.04	0.284
JSEC → COMM	0.795	0.794	0.69	0.885
JSEC → FIN	0.521	0.522	0.344	0.678
REG → AMB	0.156	0.169	0.057	0.331
REG → COMM	0.516	0.518	0.393	0.629
REG → FIN	0.445	0.444	0.259	0.62
REG → JSEC	0.549	0.55	0.416	0.674
SEV → AMB	0.274	0.281	0.105	0.478
SEV → COMM	0.675	0.675	0.561	0.779
SEV → FIN	0.72	0.726	0.588	0.858
SEV → JSEC	0.639	0.639	0.498	0.765
SEV → REG	0.361	0.363	0.179	0.529
TXNC → AMB	0.586	0.585	0.447	0.698
TXNC → COMM	0.091	0.119	0.061	0.217
TXNC → FIN	0.15	0.178	0.073	0.331
TXNC → JSEC	0.075	0.114	0.055	0.225
TXNC → REG	0.274	0.277	0.121	0.447
TXNC → SEV	0.17	0.182	0.068	0.351

Note: COMM= commitment to using cyberinsurance as a risk management strategy; AMB = ambiguity of cyberinsurance; FIN= financial risk; REG = regulation oversight risk; TXNCN = transaction cost; SEV = breach risk severity; JSEC = job security, COE = coercive pressure, MIM = mimetic pressure, NORM = normative pressure

highlight that regulations requirements are at the core of the top manager's decision. Regulatory agencies such as the SEC require firms to disclose cybersecurity risks. If regulatory agencies are interested in the viability of an organization by looking at their cybersecurity risk management strategies, chances are that investors and potential business partners may seek similar risk management information from firms that are not listed on the stock market (e.g., small and medium enterprises). We hope that this study encourages organizations with or without regulatory oversight from a government agency to commit to cyberinsurance.

5.3. Limitations and future research

This study, like most research, is subject to limitations. The survey participants (CEOs of their respective firms) were ideal as key informants, yet including other top managers may have provided different insights. Another limitation is that study focused on a limited number of organizational and situational factors. Future research could investigate the role of additional organizational factors such as litigation risks or sanctions. In addition, future research could include other individual factors such as reputation or executive litigation that might influence the top manager's commitment to cyberinsurance. Building on the findings, we argue that incorporating job security as a personal relevance factor in future research on security motivation is key to additional insight on the role of job security in employee security behavior.

Another avenue for further research is the role of cyberinsurance use as a cybersecurity best practice. Cyberinsurance companies require their

Table C3
Loadings and cross loadings result.

	AMB	COE	COMM	FIN	JSEC	MIM	NORM	REG	SEV	TXNC
AMB1	0.90	0.19	0.08	0.19	0.06	0.22	0.34	0.16	0.18	0.52
AMB2	0.94	0.32	0.18	0.25	0.16	0.36	0.43	0.17	0.28	0.50
AMB3	0.93	0.23	0.11	0.18	0.07	0.28	0.33	0.11	0.24	0.52
AMB4	0.94	0.27	0.11	0.19	0.07	0.27	0.37	0.17	0.25	0.52
COE1	0.29	0.88	0.74	0.54	0.61	0.53	0.65	0.46	0.60	0.11
COE2	0.23	0.90	0.63	0.48	0.57	0.58	0.67	0.58	0.48	0.03
COE3	0.25	0.90	0.66	0.52	0.54	0.62	0.65	0.52	0.54	0.13
COE4	0.08	0.82	0.68	0.55	0.57	0.63	0.55	0.55	0.51	–0.02
COMM2	0.16	0.73	0.97	0.58	0.72	0.61	0.56	0.42	0.61	–0.04
COMM3	0.06	0.67	0.91	0.54	0.72	0.55	0.54	0.46	0.58	–0.09
COMM4	0.14	0.76	0.97	0.56	0.70	0.61	0.60	0.48	0.56	–0.02
COMM5	0.08	0.71	0.90	0.56	0.68	0.59	0.53	0.46	0.56	–0.08
FIN1	0.17	0.58	0.57	0.87	0.47	0.45	0.46	0.41	0.62	0.13
FIN2	0.25	0.41	0.47	0.89	0.35	0.31	0.33	0.27	0.56	0.12
FIN3	0.13	0.53	0.52	0.85	0.42	0.41	0.45	0.40	0.51	0.12
FIN4	0.18	0.62	0.54	0.83	0.52	0.48	0.57	0.48	0.54	0.19
FIN5	0.15	0.40	0.44	0.83	0.29	0.28	0.27	0.21	0.52	0.01
JSEC1	0.11	0.61	0.68	0.44	0.95	0.63	0.52	0.50	0.52	0.07
JSEC2	0.09	0.61	0.73	0.48	0.91	0.60	0.52	0.41	0.59	–0.05
JSEC3	0.09	0.62	0.68	0.42	0.95	0.62	0.56	0.50	0.51	0.04
MIM1	0.23	0.65	0.64	0.48	0.65	0.84	0.51	0.34	0.61	0.15
MIM2	0.35	0.58	0.51	0.36	0.53	0.92	0.62	0.36	0.47	0.34
MIM3	0.25	0.57	0.57	0.37	0.61	0.92	0.61	0.42	0.47	0.28
MIM4	0.24	0.59	0.59	0.42	0.62	0.93	0.61	0.41	0.51	0.29
NORM1	0.35	0.71	0.54	0.45	0.48	0.59	0.93	0.47	0.45	0.32
NORM2	0.37	0.73	0.59	0.51	0.58	0.61	0.90	0.46	0.47	0.31
REG1	0.14	0.48	0.38	0.37	0.49	0.34	0.42	0.90	0.30	0.19
REG2	0.20	0.54	0.42	0.36	0.44	0.39	0.46	0.93	0.27	0.29
REG3	0.11	0.55	0.47	0.37	0.50	0.44	0.45	0.93	0.32	0.30
REG4	0.15	0.55	0.44	0.39	0.41	0.36	0.41	0.88	0.28	0.17
REG5	0.07	0.53	0.48	0.36	0.50	0.39	0.46	0.87	0.31	0.23
SEV2	0.19	0.58	0.59	0.58	0.53	0.52	0.50	0.28	0.86	0.17
SEV3	0.26	0.49	0.42	0.53	0.45	0.45	0.34	0.24	0.90	0.11
SEV4	0.24	0.60	0.66	0.64	0.59	0.56	0.49	0.35	0.93	0.14
TXNC3	0.52	0.07	–0.08	0.11	–0.03	0.26	0.30	0.26	0.14	0.91
TXNC4	0.52	0.13	0.00	0.14	0.07	0.32	0.40	0.24	0.14	0.95
TXNC5	0.50	0.19	0.05	0.20	0.10	0.37	0.44	0.31	0.22	0.93
TXNC6	0.50	–0.04	–0.15	0.06	–0.05	0.17	0.22	0.15	0.07	0.91

Note: COMM= commitment to using cyberinsurance as a risk management strategy; AMB = ambiguity of cyberinsurance; FIN= financial risk; REG = regulation oversight risk; TXNCN = transaction cost; SEV = breach risk severity; JSEC = job security, COE = coercive pressure, MIM = mimetic pressure, NORM = normative pressure

Table C4
Full collinearity VIF test using factor-based PLS.

	AMB	COE	COMM	FIN	JSEC	MIM	NORM	REG	SEV	TXNC
AMB		1.49	1.62	1.58	1.36	1.59	1.58	1.56	1.58	1.30
COMM	3.77	3.40		3.69	3.11	3.72	3.76	3.74	3.79	2.93
FIN	2.03	2.07	2.02		2.11	2.10	2.11	2.11	1.74	2.10
JSEC	2.88	2.96	2.58	3.01		2.68	2.90	2.75	2.92	2.01
MIMIC	2.61	2.60	2.63	2.77	2.41		2.65	2.67	2.73	2.31
NORM	2.92	2.49	2.71	2.95	2.85	2.86		2.89	2.88	2.63
REG	1.82	1.67	1.89	1.94	1.69	1.94	1.94		1.88	1.68
SEV	2.33	2.32	2.38	2.02	2.28	2.34	2.36	2.29		2.31
TXNC	1.66	1.91	1.78	2.16	1.61	2.00	1.95	1.91	2.14	

Note: COMM= commitment to using cyberinsurance as a risk management strategy; AMB = ambiguity of cyberinsurance; FIN= financial risk; REG = regulation oversight risk; TXNCN = transaction cost; SEV = breach risk severity; JSEC = job security, COE = coercive pressure, MIM = mimetic pressure, NORM = normative pressure

insured to undergo initial and periodic assessments so they can determine the presence of specific security controls in order to certify that the organization is eligible to be insured [1,95]. Thus, cyberinsurance could act as an incentive to increase cybersecurity best practices in organizations [71,129]. Insurance providers routinely offer reduced premiums if the insured has increased levels of self-protection (e.g., house insurance discounts for the installation of home security systems or smoke detectors). If cyberinsurance carriers offered such incentives to organizations, this could promote increased security best practices [58]. Thus, future research should investigate the effect of cyberinsurance on security practices in organizations.

6. Conclusion

This study examined top managers' perspectives of a cybersecurity strategy. We drew from institutional theory and UET to test a model that links top managers' values and perceptions as mediators between external institutional pressures and the commitment to use cyberinsurance as a risk management strategy. Both quantitative and post-hoc qualitative (through interviews of top executives) analyses provide a comprehensive insight of the top manager's decision-making towards a cybersecurity strategy, which is a departure from employee security perspectives. Findings provide a framework within which future research may examine organizational cybersecurity strategy by incorporating top manager perceptions into the theoretical lens through which the strategy is examined. Several directions for future research using this framework are suggested. Findings also provide guidance for practitioners in framing top IT manager conversations with other top managers, such as the CEO or chief financial officer (CFO), from the perspective of how cybersecurity strategy may impact those top managers personally and professionally. In sum, this study better informs our collective understanding by providing evidence about the influences on top managers when making organizational cybersecurity strategy decisions.

CRediT authorship contribution statement

Obi Ogbanufe: Conceptualization, Data curation, Methodology, Writing – original draft. **Dan J. Kim:** Data curation, Supervision, Writing – review & editing. **Mary C. Jones:** Writing – review & editing.

Appendix A: Selected studies related to IS strategic choice/decision

Table A1

Reference/ Strategic choice	Summary	Theory	Key drivers/factors	Sampling frame/#
[13] IT management	The study seeks to understand, which technology management responsibilities that particular senior executives are held accountable for when there are serious IT deficiencies.	Upper echelons perspective	IT material weakness, CEO and CFO turnover	Organizational level 278 firm-year observations
[17] Inter-organization system	To understand the institutional pressures organization leaders faced and their intentions to adopt inter-organizational systems for financial electronic data interchange	Institutional theory	Mimetic, coercive, and normative pressures	Organizational level CEOs, CFOs, and CIOs of 222 organizations
[130] Trucking supply chain	Examines environmental benefits and institutional pressures that influence the continued use of bypass systems by truck drivers.	Institutional theory	Competitive pressure, organizational pressure, industry pressure, participation among other drivers, financial benefits and environmental benefits	Individual level 212 truckers
[122] Healthcare EHR sourcing	Examines how antecedents such as strategic orientation (mission), formal structure (size), and internal dynamics (patient case mix complexity) influence whether hospitals utilize single-sourcing configuration.	Institutional theory	Closeness to single-sourcing, hospital-age, for-profit, teaching, hospital-size	Organizational level. 2,824–3,417 hospitals
[16] ERP system assimilation	Examines how top management mediates the impact of external institutional pressures on the assimilation of enterprise systems within organizations	Institutional theory, top management (upper echelons theory)	Coercive, mimetic, normative factors, top management beliefs, top management participation, assimilation	Individual level. 77 ERP project supervisors as key informants
[12] IS strategic	Posits that shared understanding between the CIO and TMT regarding the role of IS in the	Upper echelons theory	Shared language, Shared understanding, CIO business knowledge, TMT IS knowledge,	Individual level. Matched-pair surveys of

(continued on next page)

(*continued*)

management	organization is an important antecedent for IS strategic alignment		demographic similarity, experiential similarity, structural systems of knowing, Social systems of knowing, IS strategic alignment	621 CIOs and 243 TMT executive
[92] Integrative information delivery	Examines how external and environmental pressures influence the manager's decision for integrative information delivery.	Institutional theory	External pressure (coercive, mimetic, normative)	Individual level. 103 non-IS top executives CEOs, CFOs, and vice presidents, key informants. Semi-structured interviews with 8 executives.
[131] Organization agility	Examines how technology, organizational, and environmental elements combine to produce agility. Specifically, the role that business intelligence and communication technologies play in how firms achieve organizational sensing agility, decision-making agility, and acting agility in different organizational and environmental contexts.	Organizations as information processing framework	Sensing agility, Top management team energy, decision-making agility, acting agility, unpredictability, communication	Organizational level. 218 managers from 106 firms.
[11] IS strategy	Examines the relationship between IS strategy and firm performance, as well as the environmental conditions surrounding how an IS strategy might outperform others.	IS strategy and firm performance	Technological turbulence, Market uncertainty, firm performance, innovative IS strategy, conservative IS strategy, undefined IS strategy,	Organizational level. 263 executives using one highest ranking executive the organization.
[10] IT innovation in healthcare	Investigates IT innovation by examining the factors that influence a hospital's strategic choice to be an IT innovator and the influence of IT innovation on hospital performance.	Visionary leadership, upper echelons theory, organizational climate theory, and resource-based view	CIO strategic leadership, IT innovation, TMT attitude towards IT, IT impact, hospital climate, hospital performance	70 matched pairs of hospital CIOs and executives. Semi-structured interviews with 10 executives.
[14] IT security investment in healthcare	Investigates the role that symbolic versus substantive adoption of IT practices plays in the effectiveness of IT security through reducing the likelihood of data security breaches.	Institutional theory	IT security investments, symbolic/ substantive adoption, likelihood of data breach	Organizational level. 5,882 hospitals
[132] Inter-organization business process	Investigates differential effects of relational, institutional, and inertial mechanisms on the assimilation of inter-organizational business process in dominant and non-dominant firms.	Relational view of the firm, institutional theory, and organizational inertia theory	Relational view: relational specificity, relational depth, relational extendibility Institutional theory: coercive pressure, mimetic pressure, and normative pressure Inertial theory: resource rigidity, routine rigidity	Cross-case analysis on data from 11 firms in the high-tech industry
(Hsu, Lee, & Straub, 2012) Security management	Explores information security management as administrative innovation, with a focus on economic efficiency and internal organizational capability resulting from institutional pressures to conform.	Institutional theory	Perceived environmental uncertainty, perceived gain in competitive advantage, top management support, it capability, cultural acceptability, institutional influences (peer influence, supervisory authority influence), adoption of security management, assimilation of security management	Individual level. 140 top IS managers in Korea
[36] Web assimilation	Examines organizational factors that influence the achievement of web assimilation within the organization for its e-commerce activities.	Institutional theory	Top management championship, strategic investment rationale, and extent of coordination, web assimilation	Organizational level. 62 match pairs of top executives and IT professionals.

Note: TMT = top management team; ERP = enterprise resource planning; ERP = enterprise resource planning; CIO = chief information officer; CFO = chief financial officer.

Appendix B: Survey instruments and operationalization of constructs

.

Appendix C: Discriminant validity test using the Heterotrait–Monotrait (HTMT) Ratio approach

There are two ways of assessing discriminant validity using the HTMT method [111]. First, assess whether the value of HTMT below a recommended threshold. Second, use a confidence interval to test whether an HTMT null hypothesis of equal to or more than 1. From the first test, the result shows that the highest absolute value for our measures is 0.79 (see Table B1), thus, satisfying the 0.85 threshold [111]. From the second test, we find that all upper confidence intervals are below the value of 1. Thus, suggesting that HTMT values are significantly different from 1 (see Table C2). The combination of the test results leads us to conclude that discriminant validity is achieved in our measurement model.

Testing common methods bias

Common methods bias (CMB) is addressed in multiple ways. First, in the survey design process, we followed recommendations and psychologically separated the measures by using dissimilar response format, such as Likert scales and open-ended questions. Using different format is beneficial in reducing context-related cues [136]. Also, following Podaskoff et al. [137], we informed participants about the anonymity of the survey and reminded them that their responses are neither right nor wrong. Secondly, we assessed the CMB in the data using two methods. We performed Harman's [138] one-factor test that assessed all reflective items using principal components factor analysis. Six factors were revealed and the largest factor variance was 38.5%, indicating that a single factor did not account for most of the variance. Also, we used a factor-based partial least squares structural equation modeling (PLS-SEM) full collinearity test to assess CMB [139]. The factor-based PLS-SEM process integrates measurement errors that address issues with variance maximization, which are inherent in standard PLS-SEM. The assessment revealed variance inflation factor (VIF) values that are below the threshold of five [112,113]. A summary of the results from the CMB analysis is depicted in Table C1. These results suggest that CMB is not a major problem in this study.

Tables C3 and C4

Reference

[1] R.P. Majuca, W. Yurcik, J.P. Kesan, The Evolution of Cyberinsurance, 2006. http://arxiv.org/ftp/cs/papers/0601/0601020.pdf.

[2] D.W. Straub, R.J. Welke, Coping with Systems Risk: Security Planning Models for Management Decision Making, MIS Q, 1998, pp. 441–469.

[3] R. Willison, M. Warkentin, Beyond Deterrence: An Expanded View of Employee Computer Abuse, 37, MIS Q, 2013, pp. 1–20.

[4] T. Bandyopadhyay, V. Mookerjee, R. Rao, Why IT managers don't go for cyber-insurance products, Commun. ACM. 52 (2009) 68–73.

[5] C.A. Siegel, T.R. Sagalow, P. Serritella, Cyber-risk management: technical and insurance controls for enterprise-level security, Inf. Syst. Secur. 11 (2002) 33–49.

[6] R. Böhme, G. Kataria, On the limits of cyber-insurance. Trust and Privacy in Digital Business, Springer, 2006, pp. 31–40.

[7] S. Romanosky, L. Ablon, A. Kuehn, T. Jones, Content analysis of cyber insurance policies: how do carriers price cyber risk? J. Cybersecur. 5 (2019) 1–19, https://doi.org/10.1093/cybsec/tyz002.

[8] Q. Hu, P. Hart, D. Cooke, The role of external and internal influences on information systems security - a neo-institutional perspective, J. Strateg. Inf. Syst. 16 (2007) 153–172.

[9] J. Leonard, H. Higson, A strategic activity model of Enterprise System implementation and use: Scaffolding fluidity, J. Strateg. Inf. Syst. 23 (2014) 62–86.

[10] D.E. Leidner, D. Preston, D. Chen, An examination of the antecedents and consequences of organizational IT innovation in hospitals, J. Strateg. Inf. Syst. 19 (2010) 154–170, https://doi.org/10.1016/j.jsis.2010.07.002.

[11] D.E. Leidner, J. Lo, D. Preston, An empirical investigation of the relationship of IS strategy with firm performance, J. Strateg. Inf. Syst. 20 (2011) 419–437.

[12] D.S. Preston, E. Karahanna, Antecedents of IS strategic alignment: a nomological network, Inf. Syst. Res. 20 (2009) 159–179, https://doi.org/10.1287/isre.1070.0159.

[13] A. Masli, V.J. Richardson, W.W. Marcia, R. Zmud, Senior Executives' IT Management Responsibilities: Serious IT-Related Deficiencies and CEO/CFO Turnover, MIS Quarterly 40 (3) (2016) 687–708.

[14] C. Angst, E.S. Block, J. D'Arcy, K. Kelley, When do it security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches, MIS Quarterly 41 (2017) 893–916.

[15] P.J. DiMaggio, W.W. Powell, The iron cage revisited : institutional isomorphism and collective rationality in organizational fields, Am. Sociol. Rev. 48 (1983) 147–160.

[16] H. Liang, N. Saraf, Q. Hu, Y. Xue, Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management, 31, MIS Q, 2007, pp. 59–87.

[17] H.H. Teo, K.K. Wei, I. Benbasat, Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective, 27, MIS Q, 2003, pp. 19–49. http://www.jstor.org/stable/30036518 (accessed March 7, 2017).

[18] D. Hambrick, P.A. Mason, Upper echelons: the organization as a reflection of its top managers, Acad. Manag. Rev. 9 (1984) 193–206.

[19] K. Hedström, E. Kolkowska, F. Karlsson, J.P. Allen, Value conflicts for information security management, J. Strateg. Inf. Syst. 20 (2011) 373–384, https://doi.org/10.1016/j.jsis.2011.06.001.

[20] L. Kappelman, R. Torres, E. Mclean, C. Maurer, V. Johnson, K. Kim, The 2018 SIM IT Key Issues and Trends Study, 18, MIS Q. Exec, 2018, pp. 237–263.

[21] Experian, Experian Data Breach Industry Forecast, Experian, 2015. http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf.

[22] S. Ransbotham, S. Mitra, Choice and chance: A conceptual model of paths to information security compromise, Inf. Syst. Res. 20 (2009) 121–139.

[23] D. Hambrick, Upper echelons theory : an update, Acad. Manag. Rev. 32 (2007) 334–343.

[24] P. Ghemawat, Commitment: The Dynamic of Strategy, Free Press, New York, 1991.

[25] C. Hsu, J.N. Lee, D. Straub, Institutional influences on information systems security innovations, Inf. Syst. Res. 23 (2012) 918–939, https://doi.org/10.1287/isre.1110.0393.

[26] G. Medvinsky, C. Lai, B.C. Neuman, Endorsements, licensing, and insurance for distributed system services, in: Proceedings of the 2nd ACM Conference ACM Computer and Communications Security Conference, ACM, 1994: pp. 170–175.

[27] D. Geer, Risk management is still where the money Is, Comput. (Long. Beach. Calif). 36 (2003) 129–131.

[28] B. Schneier, Insurance and the computer industry, Commun. ACM. 44 (2001) 114–115.

[29] N.T. Feather, Values, valences, and course enrollment: Testing the role of personal values within an expectancy - valence framework. J. Educ. Psychol. 80 (1988) 381–391.

[30] J.P. Peter, L.X. Tarpey, A comparative analysis of three consumer decision strategies, J. Consum. Res. (1975) 29–37.

[31] D.J. Kim, D.L. Ferrin, H.R. Rao, Trust and satisfaction, two stepping stones for successful e-commerce relationships: A longitudinal exploration, Inf. Syst. Res. 20 (2009) 237–257, https://doi.org/10.1287/isre.1080.0188.

[32] G.L. Desanctis, An Examination of an Expectancy Theory Model of Decision Support System Use, Texas Tech Univeristy, 1982.

[33] D. Hambrick, E. Abrahamson, Assessing managerial discretion across industries, Acad. Manag. J. 38 (1995) 1427–1441.

[34] C. Crossland, D. Hambrick, Differences in managerial discretion across countries: how nation-level institutions affect the degree to which CEOs matter, Strateg. Manag. J. 32 (2011) 797–819, https://doi.org/10.1002/smj.

[35] W. Lewis, R. Agarwal, V. Sambamurthy, Sources of Influence on Beliefs About Information Technology Use: An Empirical Study of Knowledge, 27, MIS Q, 2003, pp. 657–678.

[36] D. Chatterjee, R. Grewal, V. Sambamurthy, Shaping up for E-Commerce: Institutional Enablers of the Organizational Assimilation of Web Technologies, 26, MIS Q, 2002, pp. 65–89.

[37] E. Mollick, People and process, suits and innovators: The role of individuals in firm performance, Strateg. Manag. J. 33 (2012) 1001–1015.

[38] M. Bertrand, A. Schoar, Managing With Style: The Effect of Managers on Firm Policies, 2002. https://ssrn.com/abstract=376880.

[39] D. Hambrick, T.S. Cho, M. Chen, The influence of top management team heterogeneity on firms competitive moves, Adm. Sci. Q. 41 (1996) 659–684.

[40] M. Newman, R. Sabherwal, Determinants of Commitment to Information Systems Development: A Longitudinal Investigation, MIS Q, 1996, pp. 23–54.

[41] E. Babakus, U. Yavas, O.M. Karatepe, T. Avci, The effect of management commitment to service quality on employees' affective and performance outcome, J. Acad. Mark. Sci. 31 (2003) 272–286, https://doi.org/10.1177/0092070303253525.

[42] R.P. Marble, A system implementation study: Management commitment to project management, Inf. Manag. 41 (2003) 111–123, https://doi.org/10.1016/S0378-7206(03)00031-4.

[43] T.D. Clark, M.C. Jones, C.P. Armstrong, The Dynamic Structure of Management Support Systems: Theory Development, Research Focus, and Direction, 31, MIS Q, 2007, pp. 579–615.

[44] B.M. Staw, Counterforces to change, in: P.. Goodman (Ed.), Change in Organizations, Jossey-Bass, San Francisco, 1982, pp. 87–121.

[45] J. Goo, R. Kishore, R.H. Rao, K. Nam, The Role of Service Level Agreements in Relational Management of Information Technology Outsourcing: An Empirical Study, 33, MIS Q, 2009, pp. 119–145.

[46] J.S. Coleman, Foundations of Social Theory, The Belknap Press of Harvard University Press, Cambridge, MA, 1990.

[47] R.S. Lazarus, C.A. Smith, Knowledge and appraisal in the cognition—emotion relationship, Cogn. Emot. 2 (1988) 281–300.

[48] N. Doherty, Integrated Risk Management: Techniques and Strategies for Managing Corporate Risk, McGraw Hill, New York, NY, 2000.

[49] M. Adams, C. Lin, H. Zou, Chief executive officer incentives, monitoring, and corporate risk management: evidence from insurance use, J. Risk Insur. 78 (2011) 551–582.

[50] M. Hsu, J. Jiang, G. Klein, Z. Tang, Perceived career incentives and intent to leave, Inf. Manag. 40 (2003) 361–369.

[51] D.H. McKnight, B. Phillips, B.C. Hardgrave, Which reduces IT turnover intention the most: Workplace characteristics or job characteristics? Inf. Manag. 46 (2009) 167–174.

[52] F.V. Fox, B.M. Staw, The trapped administrator: effects of job insecurity and policy resistance upon commitment to a course of action, Adm. Sci. Q. 24 (1979) 449–471, https://doi.org/10.2307/2989922.

[53] Absolute, IT Confidential - The State of Security Confidence, 2016. https://blogs.absolute.com/it-professionals-share-bad-habits-in-new-absolute-survey/(. accessed January 31, 2017).

[54] J. Russell, Equifax CEO Richard Smith has 'retired' following huge data breach, TechCrunch, 2017. https://techcrunch.com/2017/09/26/equifax-ceo-richard-smith-has-retired-following-huge-data-breach/ (accessed April 30, 2018).

[55] Y.H. Kwak, K.S. LaPlace, Examining risk tolerance in project-driven organization, Technovation 25 (2005) 691–695.

[56] I. Bose, A.C.M. Leung, Do phishing alerts impact global corporations? A firm value analysis, Decis. Support Syst. 64 (2014) 67–78, https://doi.org/10.1016/j.dss.2014.04.006.

[57] S. Goel, H.A. Shawky, The Impact of federal and state notification laws on security breach announcements, Commun. Assoc. Inf. Syst. 34 (2014) 37–50.

[58] L.A. Gordon, M.P. Loeb, L. Zhou, The impact of information security breaches: has there been a downward shift in costs? J. Comput. Secur. 19 (2011) 33–56.

[59] B.K. Boyd, J. Fulk, Executive scanning and perceived uncertainty: a multidimensional model, J. Manage. 22 (1996) 1–21, https://doi.org/10.1177/014920639602200101.

[60] R. McCullen, The CEO's critical role in driving cybersecurity readiness, Forbes (2018). https://www.forbes.com/sites/forbestechcouncil/2018/01/05/the-ceos-critical-role-in-driving-cybersecurity-readiness/#1a09f7094170 (accessed October 2, 2019).

[61] K. Bissell, R. LaSalle, F. van den Dool, J. Kennedy-White, Gaining ground on the cyber attacker: 2018, State Cyber Resil. (2018) https://www.accenture.com/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf#zoom=50.

[62] SEC, Former Equifax Executive Charged With Insider Trading, SEC, 2018. https://www.sec.gov/news/press-release/2018-40 (accessed August 7, 2019).

[63] Ponemon, Cost of Cyber Crime Study: United States, 2016 (2015), 2015. http://www.ponemon.org/library/2015-cost-of-cyber-crime-united-states.

[64] K. Campbell, L.A. Gordon, M.P. Loeb, L. Zhou, The economic cost of publicly announced information security breaches: empirical evidence from the stock market, J. Comput. Secur. 11 (2003) 431–448.

[65] H. Cavusoglu, B. Mishra, S. Raghunathan, The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers, Int. J. Electron. Commer. 9 (2004) 70–104.

[66] CybersecurityVentures, Cybercrime Damages $6 Trillion by 2021, CybersecurityVentures. (2017). https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (accessed April 30, 2018).

[67] R. Böhme, G. Schwartz, Modeling Cyber-Insurance: Towards a Unifying Framework, WEIS, 2010.

[68] B. Srinidhi, J. Yan, G.K. Tayi, Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors, Decis. Support Syst. 75 (2015) 49–62.

[69] S. Ingram, The Financial Risk of Cyber Security Breaches, PwC. (2014). https://www.digitalpulse.pwc.com.au/financial-risk-cyber-security/ (accessed August 6, 2019).

[70] S. Jaatinen, A Guide to Financial Risk for CEOs, EUROMONEY. (2016). https://www.euromoney.com/article/b12knynhdntf4n/a-guide-to-financial-risk-for-ceos (accessed August 6, 2019).

[71] L.A. Gordon, M.P. Loeb, T. Sohail, A framework for using insurance for cyber-risk management, Commun. ACM. 46 (2003) 81–85.

[72] J. Bolot, M. Lelarge, A new perspective on internet security using insurance, in: Proceedings of the INFOCOM 27th Conference on Computer Communications IEEE, IEEE, 2008.

[73] S. Dhar, B. Balakrishnan, Risks, benefits, and challenges in global IT outsourcing, J. Glob. Inf. Manag. 14 (2006) 59–89.

[74] M. Benaroch, L. Fink, Contract Design Choices and the Balance of EX Ante and Ex Post Transaction Costs in Software Development Outsourcing, 40, MIS Q, 2016, pp. 57–82.

[75] J. Kwon, M.E. Johnson, Proactive Versus Reactive Security Investments in the Healthcare Sector, 38, MIS Q, 2014, pp. 451–472.

[76] S.J. Carson, A. Madhok, W. Tao, Uncertainty, opportunism, and governance: the effects of volatility and ambiguity on formal and relational contracting, Acad. Manag. J 49 (2006) 1058–1077, https://doi.org/10.5465/AMJ.2006.22798187.

[77] T. Bandyopadhyay, V. Mookerjee, A model to analyze the challenge of using cyber insurance, Inf. Syst. Front. 21 (2017) 301–325, https://doi.org/10.1007/s10796-017-9737-3.

[78] M. Eling, W. Schnell, What do we know about cyber risk and cyber risk insurance? J. Risk Financ. 17 (2016) 474–491, https://doi.org/10.1108/JRF-09-2016-0122.

[79] F. Santos, K. Eisenhardt, Constructing markets and shaping boundaries: Entrepreneurial power in nascent fields, Acad. Manag. J. 52 (2009) 643–671.

[80] N.Y. Stanley Budner, Intolerance of ambiguity as a personality variable, J. Pers. 30 (1962) 29–50, https://doi.org/10.1111/j.1467-6494.1962.tb02303.x.

[81] R. Daft, N. Macintosh, A tentative exploration into the amount and equivocality of information processing in organizational work units, Adm. Sci. Q. 26 (1981) 207–224.

[82] R. Daft, R. Lengel, L.K. Trevino, Message Equivocality, Media Selection, and Manager performance : Implications for Information Systems, 11, MIS Quartely, 1987, pp. 355–366.

[83] P. Naghizadeh, M. Liu, Opting out of incentive mechanisms : a study of security as a non-excludable public good, IEEE Trans. Inf. Forensics Secur. 11 (2016) 2790–2803.

[84] P.H. Meland, I.A. Tondel, B. Solhaug, Mitigating risk with cyberinsurance, IEEE Secur. Priv. 13 (2015) 38–43, https://doi.org/10.1109/MSP.2015.137.

[85] A.P. Petkova, A. Wadhwa, X. Yao, S. Jain, Reputation and decision making under ambiguity : a study of US. Venture capital firms ' investments in the emerging clean energy sector, Acad. Manag. J. 57 (2014) 422–448.

[86] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, S.K. Sadhukhan, Cyber-risk decision models: to insure IT or not? Decis. Support Syst. 56 (2013) 11–26.

[87] M. Ogul, B. Rockman, Overseeing oversight: new departures and old problems, Legis. Stud. Q. 15 (1990) 5–24.

[88] M. Collins, C. Urban, The dark side of sunshine: Regulatory oversight and status quo bias, J. Econ. Behav. Organ. 107 (2014) 470–486.

[89] T. Dinev, H. Xu, J. Smith, P. Hart, Information privacy and correlates : an empirical attempt to bridge and distinguish privacy-related concepts, Eur. J. Inf. Syst. 22 (2012) 295–316.

[90] E. Boo, D. Sharma, Effect of regulatory oversight on the association between internal governance characteristics and audit fees, Account. Financ. 48 (2008) 51–71.

[91] UK Marsh, The Role of Insurance in Managing and Mitigating the Risk, Cyber Security, 2015, https://www.marsh.com/uk/insights/research/uk-cyber-security-role-of-insurance-in-managing-mitigating-risk.html (accessed September 5, 2016).

[92] W. Kettinger, C. Zhang, K.C. Chang, A view from the top: integrated information delivery and effective information use from the senior executive's perspective, Inf. Syst. Res. 24 (2013) 842–860, https://doi.org/10.1287/isre.1120.0473.

[93] Deloitte, Cyber Insurance a key element of the corporate Risk Management Strategy, 2017. https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_CyberInsurance_Noexp.PDF (accessed February 13, 2020).

[94] Pireg, What regulations require the designation of a chief information security officer (CISO), (2020). https://piregcompliance.com/ciso-as-a-service/what-regulations-require-the-designation-of-a-chief-information-security-officer-ciso/ (accessed February 16, 2020).

[95] D. Young, J. Lopez, M. Rice, B. Ramsey, R. McTasney, A framework for incorporating insurance in critical infrastructure cyber risk strategies, Int. J. Crit. Infrastruct. Prot. 14 (2016) 43–57.

[96] W. Wagner, Cyber insurance: why you should require certain vendors to have it, Priv. Data Secur. Insight. (2015). https://www.privacyanddatasecurityinsight.com/2015/05/cyber-insurance-why-you-should-require-certain-vendors-to-have-it/ (accessed February 5, 2020).

[97] P. Ziobro, J. Lublin, ISS's View on Target Directors Is a Signal on Cybersecurity, Wall Str. J. (2014). https://www.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278 (accessed January 30, 2018).

[98] G.C. Moore, I. Benbasat, Development of an instrument to measure the perceptions of adopting an information technology innovation, Inf. Syst. Res. 2 (1991) 192–222.

[99] S. Finkelstein, D. Hambrick, Top-management-team tenure and organizational outcomes: the moderating Roie of managerial discretion, Adm. Sci. Q. 35 (1990) 484–503.

[100] R. Sen, S. Borle, Estimating the contextual risk of data breach: an empirical approach, J. Manag. Inf. Syst. 32 (2015) 314–341.

[101] R. Sabherwal, Y.E. Chan, Alignment between business and IS strategies: a study of prospectors, analyzers, and defenders, Inf. Syst. Res. 12 (2001) 11–33.

[102] Experian, Data Breach Response, 2015 (2014). https://www.experian.com/assets/data-breach/brochures/response-guide.pdf.

[103] C. Cycyota, D. Harrison, What (Not) to expect when surveying executives: a meta-analysis of top manager response rates and techniques over time, Organ. Res. Methods 9 (2001) 133–160, https://doi.org/10.1177/1094428105280770.

[104] M.L. Mcdonald, J.D. Westphal, Access denied : low mentoring of women and minority first-time directors and its negative effects on appointments to additional boards, Acad. Manag. J. 56 (2013) 1169–1198.

[105] M.K. Bednar, J.D. Westphal, Surveying the corporate elite: theoretical and practical guidance on improving response rates and response quality in top management survey questionnaires. Research Methodology in Strategy and Management, Emerald Group Publishing Limited, 2006, pp. 37–55, https://doi.org/10.1016/S1479-8387(06)03004-9.

[106] Ringle, Christian M., Wende, Sven, & Becker, Jan-Michael. (2015). SmartPLS 3. Boenningstedt: SmartPLS. Retrieved from https://www.smartpls.com.

[107] W. Chin, P.R. Newsted, Structural equation modeling analysis with small samples using partial least squares. Statistical Strategies for Small Sample Research, Sage Publications, Thousand Oaks, CA, 1999, pp. 307–341.

[108] J.F. Hair, W.C. Black, B.J. Babin, R.E. Anderson, R.L. Tatham, Multivariate Data Analysis, Pearson Prentice Hall Upper Saddle River, NJ, 2006.

[109] W. Chin, Issues and Opinion on Structural Equation Modeling, 22, MIS Q, 1998 vii–xvi.

[110] C. Fornell, D.F. Larcker, Structural equation models with unobservable variables and measurement error: algebra and statistics, J. Mark. Res. (1981) 382–388.

[111] J. Henseler, C.M. Ringle, M. Sarstedt, A new criterion for assessing discriminant validity in variance-based structural equation modeling, J. Acad. Mark. Sci. 43 (2014) 115–135.

[112] R. Kline, Principles and Practice of Structural Equation Modeling, Guilford Press, New York, 1998.

[113] N. Kock, Common method bias in PLS-SEM: a full collinearity assessment approach, Int. J. Collaborat. 11 (2015) 1–10.

[114] D.W. Straub, M.-C. Boudreau, D. Gefen, Validation guidelines for IS positivist research, Commun. Assoc. Inf. Syst. 13 (2004) 380–427.

[115] K.A. Bollen, R. Stinet, Direct and indirect effects: classical and bootstrap estimates of variability, Sociol. Methodol. 20 (1990) 115–140.

[116] A.F. Hayes, Beyond baron and Kenny: statistical mediation analysis in the new millennium, Commun. Monogr. 76 (2009) 408–420, https://doi.org/10.1080/03637750903310360.
[117] A.C. Johnston, M. Warkentin, M. Siponen, An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric, 39, MIS Q, 2015, pp. 113–1A7.
[118] K. Bagchi, G. Udo, An analysis of the growth of computer and Internet security breaches, Commun. Assoc. Inf. Syst. 12 (2003) 46.
[119] C. Koh, S. Ang, D.W. Straub, IT outsourcing success: a psychological contract perspective, Inf. Syst. Res. 15 (2004) 356–373.
[120] S. Ang, D.W. Straub, Production and Transaction Economies and IS Outsourcing: A Study of the U. S. Banking Industry, 22, MIS Q, 1998, p. 535.
[121] P. Hough, N. Duffy, Top management perspectives on decision support systems, Inf. Manag. 12 (1987) 21–30.
[122] C. Angst, K. Wowack, S. Handley, K. Kelly, Antecedents of information systems sourcing strategies In U.S. hospitals: a longitudinal study, MIS Ouart. 27 (2017) 1–14.
[123] J. Haislip, J.-H. Lim, R. Pinsker, Do the Roles of the CEO and CFO Differ When it Comes to Data Security Breaches? AMCIS, 2017, pp. 1–10.
[124] K. Bissell, R. Lasalle, K. Richards, The cyber-committed CEO and Board, 2017. https://www.accenture.com/_acnmedia/pdf-42/accenture-cyber-committed-ceo-and-board-pov.pdf#zoom=50 (accessed August 5, 2019).
[125] Y. Lee, K.R. Larsen, Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software, Eur. J. Inf. Syst. 18 (2009) 177–187.
[126] H. Cavusoglu, B. Mishra, S. Raghunathan, The value of intrusion detection systems in information technology security architecture, Inf. Syst. Res. 16 (2005) 28–46.
[127] P. Ifinedo, Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition, Inf. Manag. 51 (2014) 69–79.
[128] T. Herath, R. Rao, Protection motivation and deterrence: a framework for security policy compliance in organisations, Eur. J. Inf. Syst. 18 (2009) 106–125.
[129] J. Bolot, M. Lelarge, Cyber insurance as an incentivefor internet security, Manag. Inf. Risk Econ. Secur. (2009) 269–290.
[130] K. Marett, R. Otondo, S. Taylor, Assessing the Effects of benefits and institutional influences on the continued use of environmentally munificent bypass systems in long-haul trucking, MIS Ouart. 37 (2013) 1301–1312.
[131] Y. Park, O.A. El Sawy, P.C. Fiss, The role of business intelligence and communication technologies in organizational agility: a configurational approach, J. Assoc. Inf. Syst. 18 (2017) 648–686, https://doi.org/10.17705/1jais.00001.
[132] H. Bala, V. Venkatesh, Assimilation of interorganizational business process standards, Inf. Syst. Res. 18 (2007) 340–362, https://doi.org/10.1287/isre.1070.0134.
[133] S.J. Ashford, C. Lee, P. Bobko, Content, cause, and consequences of job insecurity: a theory-based measure and substantive test, Acad. Manag. J. 32 (1989) 803–829, https://doi.org/10.2307/256569.
[134] S. Milne, S. Orbell, Can protection motivation theory predict breast selfexamination? A longitudinal test exploring the role of previous behaviour, Underst. Chang. Heal. Behav. Heal. Beliefs Self-Regulat. (2000) 51–71.
[135] M. Jones, D. Mothersbaugh, S.E. Beatty, Switching barries and repurchase intentions in services, J. Retail. 76 (2000) 259–274.
[136] P.M. Podsakoff, S.B. MacKenzie, J.-Y. Lee, N.P. Podsakoff, Common method biases in behavioral research: a critical review of the literature and recommended remedies, J. Appl. Psychol. 88 (2003) 879.
[137] B. Jarvis, Cheryl, B. MacKenzie, Scott, P.M. Podsakoff, A critical review of construct indicators and measurement model misspecification in marketing and consumer research, J. Consum. Res. 30 (2003) 199–218.
[138] P.M. Podsakoff, S.B. MacKenzie, N.P. Podsakoff, Sources of method bias in social science research and recommendations on how to control it, Annu. Rev. Psychol. 63 (2011) 539–569.
[139] N. Kock, G. Lynn, Lateral collinearity and misleading results in variance-based SEM: an illustration and recommendations, J. Assoc. Inf. Syst. 13 (2012) 546–580.

Obi Ogbanufe is an Assistant Professor of Information Technology and Decision Sciences at the University of North Texas. She is a recipient of the NSF CyberCorps Scholarship for Service award. She has published in *Information Systems Journal, Decision Support Systems* and the *International Journal of Human–Computer Interaction*. Her research interests include information security, cybercrime, health information technology, risk management, and smart devices.

Dan J. Kim is a Fulbright Sr. Scholar and Professor of Information Technology and Decision Sciences at the University of North Texas. His research interests are in multidisciplinary areas, such as information security and privacy, business and intlligence analytics, trust in electronic commerce, and others. His research work has been published or forthcoming in more than 180 papers, in refereed journals, peer-reviewed book chapters, and conference proceedings including *ISR, JMIS, JAIS, EJIS, CACM, DSS, I&M*, etc. His publications have been cited more than 9,000 times over the last five years and he is ranked top 1.2% of most-cited worldwide researchers in the information systems area. He has been awarded several research grants for multi-years including NSF, NSA, and Core Fulbright Scholarship grant. He serves or served as a guest, senior, and associate editor for several top journals, including *MISQ, I&M, ISF, ISM, and ECRA*.

Mary C. Jones is a Professor of information systems in the Information Technology and Decision Sciences Department at the University of North Texas. Her work appears in numerous journals, including *MIS Quarterly, European Journal of Information Systems, Behavioral Science, Decision Support Systems, System Dynamics Review*, and *Information and Management*. Her research interests are primarily in the impact on organizations of large scale, organizational spanning information systems, and in organizational-level IT management issues. She teaches a variety of courses, including enterprise applications of business intelligence/analytics, IT project management, and doctoral seminars in general systems theory and in research methods.