INFORMATION SECURITY RISK AND BOUNDARY CHANGING BEHAVIOR

Hilal Pataci
Rensselaer Polytechnic Institute, patach@rpi.edu

T. Ravichandran
Rensselaer Polytechnic Institute, ravit@rpi.edu

Information Security Risk Perception and Boundary Changing Behavior of the Firm

Completed Research Paper

Hilal Pataci
Lally School of Management,
Rensselaer Polytechnic Institute,
patach@rpi.edu

T. Ravichandran
Lally School of Management,
Rensselaer Polytechnic Institute,
ravit@rpi.edu

Abstract

The escalating information security threats and their impacts have made firms pay careful attention to potential risks they face and the actions they can take to mitigate such risks. We explore if and how the information security risk perceptions of firms shape their boundary-changing behaviors. We argue that organizations have risk transfer, risk avoidance, risk reduction, risk acceptance options, and combine these options in their attempts to reduce the perceived effects of information security risks. Organizations through risk transfer could transfer some effects of information security risks to third parties, while boundary changing behaviors could alter the potential vulnerabilities of a firm and hence decisions to alter firm boundaries are likely to be shaped by risk perceptions. By fine-tuning 11 state-of-the-art NLP models with causal extraction, we find that organizations' information security risk perception is positively associated with their information security risk transfer behavior, and less-risky boundary changing actions.

Keywords

Information Security Risk, Risk Management, Boundary Changing Actions, Deep Learning

Introduction

Information security risks, the firm's probability of unintended loss of sensitive data to third parties (Von Solms and Van Niekerk, 2013), have gained increased recognition by management researchers given that each breach incident has been found to cost over $4.24 million (IBM, 2021). In addition to the high costs associated with information security breaches, the average time to fix and remedy are 148.6 days for critical impact risks and 260.7 days for low-impact risks in the USA (White Hat, 2018). Recovering from the impact of information security breaches consumes organizations' time and financial resources excessively and obliges organizations to take actions to reduce and prevent organization information security risk exposure.

Executive managers make critical decisions regarding the firm's future direction, such as decisions on resource allocations, entering and exiting industries, and boundary changing actions (Goll and Sambharya, 1998; Kwon et al., 2013; Banker and Feng, 2019), while they also consider the implications of their decisions on information security in advance. Even though executive-level strategic decision making is strongly influenced by their perceptions (March and Simon, 1958/1993), we still have limited knowledge on how their information security perceptions shape their strategic decision making, specifically for boundary changing actions that change the level of an organization's information security exposure (Theisen et al., 2018, Kapoor and Lim, 2007). Boundary changing actions such as Mergers &Acquisitions, Alliances, Third-party partnerships, and Divestitures change the level of an organization's information security risk exposure as they extend and link various parts of the organization to external entities (Majchrzak et al. 2015; Yin and Shanley, 2008). On one hand, organizations are required to govern their information security risk exposure, thus perceiving information security risk implications of their boundary changing actions in advance. On the other hand, they might still need to take boundary-changing actions to gain access to a range of valuable external resources and such actions could alter the organization's level of information security risk exposure. Top management, in the due diligence process, also considers the information security risks of a boundary-changing action, in addition to its benefits and the organization's needs. Considering the costs and the time spent to fix and remedy information security breaches, shedding a light on how organizations' information security risk perceptions shape their boundary-changing actions is necessary. In this study, by building on the behavioral theory of the firm (Cyer and March 1963/1992) that translates executive-level decision making into organizational decision making by considering organizations as a coalition of people, we aim to shed a light on the question of how organizations' information security risk perception shapes their boundary changing behavior.

It is challenging to identify and measure an organization's information security risk perception as the risk's perceived effects manifest over time. To measure an organization's information security risk perception with respect to its effects, we propose a novel approach. The Securities and Exchange Commission (SEC) announced on October 13, 2011, to address the disclosure obligations relating to cybersecurity risks and cyber incidents as a part of 1(A) Risk Factors section in their annual statements (10-K) (SEC, 2011). In this research, we fine-tune 10 generic and 1 domain-specific state-of-the-art NLP model, with causal extraction techniques to measure organizations' information security risk perceptions as the risk's perceived effects on the organization based on the information they share in their annual (10-K) reports' 1(A) Risk Factors section. We theorize that organizations perceive information security risks in terms of their effects on the organization, and this impact-driven information security risk perception shapes their strategic decision-making for boundary-changing actions and risk hedging.

The traditional information security risk management strategies articulated in the literature include risk transfer, risk acceptance, risk avoidance, and risk reduction (Majuca et al.,2006; Ogbanufe et al., 2021). Drawing on the behavioral theory of the firm and traditional risk management approaches, we propose that an organization's information security risk perception is expected to influence its choice of to accept, reduce, avoid, or transfer the perceived information security risks. We propose that the breadth of information security risk perception is positively associated with risk hedging due to the organization's need to transfer information security risks and negatively associated with boundary-changing actions that increase information security risk exposure due to the organization's need to avoid or reduce information security risks.

Literature Review and Hypotheses

The behavioral theory of the firm, by viewing the organization as a coalition, attributes to the division of labor in decision making, hence organizational *goals* are specific to those sub-units, organizational *expectations* are the result of drawing inferences from available information, while organizational *choice* is a response to a perceived problem among coalition members (Cyert and March 1963/1992; Gavetti et al., 2012). The course of an organization is shaped by strategic decision-making, and through the coalition conceptualization, the behavioral theory of the firm replaces the one man or peak coordinator with multiple authorities, hence by bargaining on the outcomes they collectively establish the organization's goals. Top management sustains the coalition and is responsible for strategic- decisions regarding the future direction of the firm such as resource allocations, entering and existing industries, boundary changing actions, and the way the firm interacts with stakeholders (Goll and Sambharya, 1998).

Organizations, through risk management strategies imposed by top management, govern their information security risk exposure. An organization's attack surface, the set of ways in which an adversary can enter the system and cause damage (Manandhata and Wing, 2010), signifies how much an organization is exposed to information security risks. Even though the size of the attack surface is found to be positively associated with the information security risk of the organization (Borky and Bradley, 2018; Theisen, et al. 2018), existing research on how organizational decision-making shapes information security risk of the organization through governing the attack surface has not yet been elucidated. Drawing on the previous literature (Kwon and Johnson, 2014; Hurley and Hult, 1998; Ryu et al. 2005; Zakay et al. 2004), we know that perception is the ability to notice and be aware of a problem, and it affects actual learning and future performance of an organization. By building on the behavioral theory of the firm, we attempt to theorize that, organizations with broader information security risk perception have more organizational *expectations* because they have more awareness regarding the effects of information security breaches on the organization. Organizations pursue a common *goal* which is to govern the attack surface by *avoiding uncertainty*. We hypothesize that organizations with broader information security risk perceptions have more expectations to govern their information security attack surface, and therefore tend to avoid, transfer, and reduce the information security risks; while organizations with relatively narrow information security risk perceptions have fewer expectations, but mostly to accept the existing information security risks.

Mergers & Acquisitions, third-party partnerships, and divestitures change organizational boundaries as they extend and link various parts of the organization to external entities. Mergers and Acquisitions (M&A) are among the prominent actions for accessing external resources with complete control of assets (Yin & Shanley, 2008), while third-party partnerships provide access to those assets with a contract and certain conditions (Villalonga & McGahan, 2005; Tanriverdi et al., 2019). Divestitures, as a major tool for asset redeployment (Montgomery, Thomas, & Kamath, 1984), is an action to divest a company's existing businesses and is considered as transferring control of the company's assets to external parties (Dranikoff, Koller, and Shneirder A., 2002). Therefore, having cyber insurance corresponds to risk transfer behavior (H1) in our model. Preferences among M&As and third-party partnerships correspond to less risky boundary changing actions(H2), while avoidance of divestitures corresponds to boundary preservation (H3) and are shaped by risk avoidance, risk reduction, and risk acceptance behavior in our model. In this research, as shown in Figure 1, the breadth of information security risk perception induces organizations to transfer, avoid, and reduce information security risks.

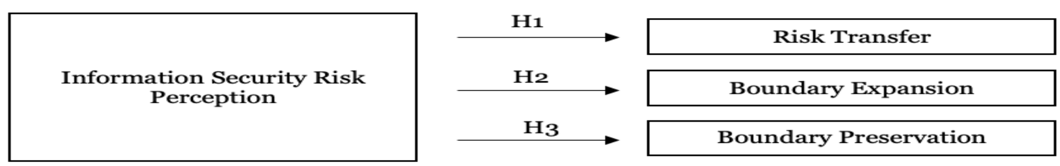

Figure 1: The Research Model

Risk Transfer

Transferring the information security risks for a fee (Majuca et al. 2006; Herath, H. Herath, T. 2011; Bolot & Lelarge, 2008) to a third party is one of the most common approaches in information security risk management and helps organizations to hedge(transfer) the effects of information security risks in their attempts to govern their information security attack surface. Cyber insurance, like any type of traditional insurance product, is a method of risk transfer, a risk-averse client is willing to pay a premium in exchange for a certain amount of coverage in the event of a loss that reduces the uncertainty in its outcome (Ogbanufe et al., 2021; Majuca et al., 2006). Therefore, we propose that the broader the information security risks an organization perceives, the more motivated it is to transfer these risks to third parties with cyber insurance.

> ***H_1:*** *The breadth of the information security risk perception is positively associated with a firm's risk transfer behavior.*

Boundary Expansion

M&As represent greater integration through the ownership of the assets of another organization while third-party partnerships provide access to those assets with a contract and certain conditions (Villalonga & McGahan, 2005; Tanriverdi et al., 2019). Third-party business partnerships, that provide mutually beneficial opportunities for all parties such as alliances, joint ventures, collaborations (Majchrzak et al. 2015), these types of partnerships, different than M&As, allow for partial control of corporate assets (Yang and Lin, 2011; Wang, 2007; Uzzi, 1996). Top management, in addition to its benefits and the organization's needs, evaluates the information security risk exposure of the organization following a boundary-changing transaction by considering its implications on the attack surface in the due diligence process. Therefore, by empirically controlling several factors that impact this decision-making process we hypothesize that organizations' choices for boundary expanding transactions are expected to be shaped by their information security risk perception. One of the major drivers of risks is the compatibility between the organizations, also conceptualized as relatedness vs unrelatedness (Yin & Shanley, 2008) of the organizations' business domains. Relatedness among organizations corresponds to lesser modifications at the attack surface given that both organizations have related IT systems, business rules, and procedures. Given the fact that additional modifications at the information security risk attack surface increase information security risks, organizations might pursue boundary-changing actions that require the least number of modifications. Boundary expanding actions among related organizations occur with a relatively smaller number of configurations at the attack surface, and this process results in fewer entry points for unauthorized access (Theisen et al., 2018; Henningsson, Yetton, Wynne, 2018; Kapoor & Lim, 2007; Henningsson and Kettinger, 2016; Tanriverdi, Roumani, and Nwankpa, 2019; Dranikoff, Koller, and Shneirder A, 2002.). Therefore, as summarized in Table 1, we hypothesize that organizations with broader information security risk perception prefer related M&A to unrelated M&A, related third-party partnerships to unrelated third-party partnerships for their boundary expanding actions.

	BOUNDARY CHANGING TRANSACTIONS (Adapted from Tanriverdi et al., 2019)					
	Mergers & Acquisitions		**Third-Party Partnerships**		**Divestitures**	
Definitio	Adds new businesses to a firm through the purchase of other firms.		Two or more independent firms collaborate to share data and other resources. Strategic alliances, joint ventures, manufacturing and supply agreements, R&D and marketing collaborations.		Divests existing businesses of a firm to another firm. To exist poorly performing businesses or remove unrelated business units that are not core to their primary business.	
	Related	**Unrelated**	**Related**	**Unrelated**	**Related**	**Unrelated**
Mechanisms	Target and acquirer from the same industry: acquirer scale expands.	Target and acquirer not from the same industry: acquirer gets access to complementary resources.	Transactions between firms from the same industry.	Transactions between firms from different industries.	The divested unit is in the same industry as the primary industry of the seller.	The divested unit is in a different industry than the primary industry of the seller.
	Less configuration at the attack surface: Extension of attack surface with relatively similar knowledge base, IT systems.	**More configuration at the attack surface:** Extension of attack surface with unrelated knowledge base, IT systems.	**Less configuration at the attack surface:** Extension of attack surface with relatively similar knowledge base, IT systems.	**More configuration at the attack surface:** Extension of attack surface with unrelated knowledge base, IT systems.	**More configuration at the attack surface:** Transferring a part of the attack surface to another organization by divesting from the main organization's attack surface. Gives access to IT systems and knowledge base. Full Exposure.	
Hypotheses	H2: Information security risk perception is positively associated with a firm's information security risk exposure reduction. Such that, organizations with broader information security risk perception are less likely to go for risk enhancing actions. H2a: Organizations with broader information security risk perception are more likely to engage in related M&A than unrelated M&A. H2b: Organizations with broader information security risk perception are more likely to engage in related than unrelated third-party partnerships.				H3: Organizations with broader information security risk perception are more likely to preserve their boundaries and avoid divestitures.	

Table 1: Boundary Changing Actions and Information Security Risk

> ***H₂:*** *Information security risk perception is positively associated with a firm's information security risk exposure reduction. Such that, organizations with broader information security risk perception are less likely to go for risk enhancing boundary expanding actions.*
> ***H2a****: Organizations with broader information security risk perception are more likely to engage in related M&A than unrelated M&A.*
> ***H2b****: Organizations with broader information security risk perception are more likely to engage in related than unrelated third-party partnerships.*

Boundary Preservation

Divestitures are a way of allocating control of resources between organizations (Penrose, 1959; Teece, 1980; Villalonga and McGahan, 2005) and transfer a fraction of the attack surface and dispose of entry points at the divested unit, and result in the highest number of configurations at the remaining attack surface of the organization. Therefore, we propose that organizations attempt to preserve their boundaries by avoiding disintegrative boundary-changing actions. Divestiture is the disintegrative form of boundary changing actions gives control of IT systems to other organizations and increases the vulnerabilities at the attack surface (Tanriverdi et al., 2019; Dranikoff, L., T. Koller, and Shneirder A. 2002) Therefore, organizations with broader information security risk perception have more organizational expectations to govern their information security attack surface by avoiding divestitures.

> ***H3****: Organizations with broader information security risk perception are more likely to preserve their boundaries and avoid divestitures.*

Empirical Approach

Sample and Data

Our sampling frame is S&P 500 firms for the 2015- 2018 period, and this yields us 1935 data points. However, due to missing values for our variables, we end up with 1565 data points. We track S&P 500 companies for 4 years to assess how their information security risk perception changes and how this change is shaping their risk hedging behavior and boundary changing behavior. We obtained information security risk perception and risk hedging data from 1/1-A sections of the 10-K disclosures, while boundary-changing transactions are obtained from Thompson SDC Platinum. For our control variables, we obtained firms' breach incidences from Privacy Rights Clearinghouse (PRC), while the rest of the control variables are obtained from the Compustat database.

Measures

Information Security Risk Perception (Independent variable): We use the information security risk spectrum as a proxy and conceptualize the information security risk spectrum as an array of effects caused by information security risks and ordered in accordance with the magnitudes of the organization's domains. Hence the breadth of the information security risk spectrum corresponds to the organization's level of information security risk perception. Broader the risk spectrum, the higher the perceived information security risks by the organization. To measure the information security risk spectrum, we use causal-extraction techniques (Hassanzadeh et al, 2020; Li et al., 2020). A causal relation is defined as an association between two events in which the first must occur and contribute to the creation of another: the former event known as the cause, and the subsequent event known as the effect (Akkasi and Moens, 2021). Therefore, in this research, cybersecurity-related risks are our causes that contribute to other events. Such that, '*data breaches cause financial loses and damage our reputation'*; in this sentence, 'data breaches' is the cause, and the effects are 1) financial loss and 2) reputational damage.

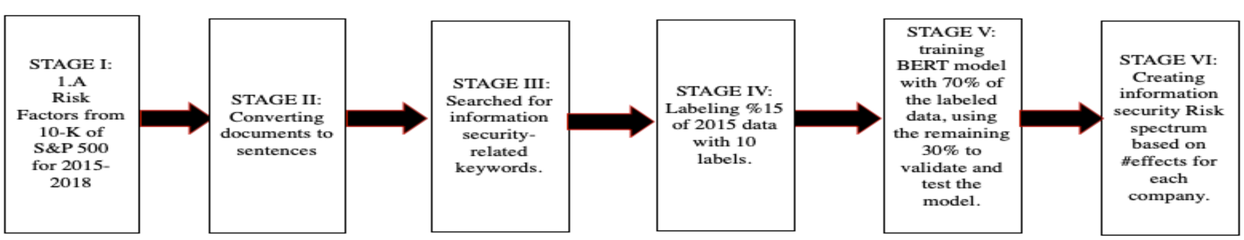

Figure 2: Model Summary

We start by extracting the 1.A Risk Factors section from 10-K documents of S&P 500 companies for the 2015-2018 period. We follow a systematic process outlined in Figure 2 and extracted the perceived effects of information security risks at the organization level in 10 domains: business, legal, reputation, sales, operational, production, third party, financial, system, and infrastructure, data. In Stage VI, we calculate how many times each effect was disclosed as a total count in 10 domains for each company. We experiment with 11 state-of-the-art NLP models; Roberta (base, large) (Liu et al., 2019), ALBERT (base-cased, base-uncased, large-cased, large-uncased) (Lan et al., 2019), BERT (base-cased, base-uncased, large-cased, large-uncased) (Devlin et al., 2018) for our task. Moreover, we also experiment with a domain-specific transformer-based model, Fin-BERT (Araci, 2019), a language model based on BERT trained and fine-tuned with 10-Ks and earning call transcripts. Among these models, fine-tuned BERT (base-cased) provides the best results, and we build a classifier and used that for multi-label text classification of the unlabeled data.

Model Name	Model Accuracy		LABELS									
			Business	Third Party	Legal	Reputation	System and Infrastructure	Data	Financial	Operational	Del. of Service	Production
BERT base cased	0.9267	F1	**0.78**	**0.83**	**0.74**	**0.93**	**0.65**	**0.89**	**0.81**	**0.84**	0.60	**0.78**
BERT base uncased	0.9103	F1	0.76	0.71	0.66	0.83	**0.71**	0.84	0.69	0.78	0.59	0.64
BERT large cased	0.8764	F1	0.72	0.08	0.67	0.78	0.57	0.76	0.62	0.59	0.00	0.00
BERT large uncased	0.9255	F1	**0.78**	0.80	**0.76**	0.89	**0.65**	0.86	**0.88**	**0.85**	**0.63**	0.71
ROBERTa (Base)	0.9206	F1	**0.79**	0.78	0.66	**0.94**	0.66	0.85	0.75	0.79	**0.86**	0.75
ROBERTa (Large)	0.9248	F1	**0.81**	0.76	0.74	**0.93**	**0.67**	0.88	0.83	**0.85**	0.40	0.57
ALBERT (Base-v1)	0.909	F1	0.71	0.62	0.68	0.91	0.56	0.82	0.75	0.80	0.50	0.62
ALBERT (XLarge-v1)	0.84	F1	0.47	0.20	0.16	0.34	0.55	0.59	0.67	0.00	0.00	0.00
ALBERT (Base-v2)	0.9152	F1	**0.78**	**0.82**	0.72	**0.93**	**0.67**	0.75	0.73	0.82	0.60	0.63
ALBERT (XLarge-v2)	0.8642	F1	0.63	0.00	0.45	0.34	0.24	0.55	0.71	0.39	0.00	0.00
FinBERT	0.9194	F1	0.76	**0.83**	0.67	0.88	**0.67**	0.85	**0.81**	**0.85**	0.40	0.50

Table 2: Deep Learning Model Results for Information Security Risk Perception *(Stage V)*

Risk Transfer (Dependent Variable H1): Proxied like Florakis et al. (2020). At stage 3 in Figure 2, we searched for 'insurance' as a word, for sentences with 'insurance', set risk hedging to 1; otherwise, 0.

Boundary Changing Transactions (Dependent Variable H2 & H3): We measure the boundary changing activity of an organization in a year (t+1) by counting the total number of transactions. We are interested in organizations' boundary-changing preferences, we convert the count variable to a ratio measure. H_2 is the ratio of less risky boundary expanding actions by dividing the total number of less risky boundary expanding actions by the total number of boundary changing actions. H_{2a} is the ratio of the total number of related M&A divided by the total number of M&A. H_{2b} is the ratio of the total number of related third-party partnerships divided by the total number of third-party partnerships. H_3 is the ratio of the total number of divestitures divided by the total number of boundary-changing actions. We expect this association to be negative, such that organizations with broader information security risk perception are expected to divest less to govern their information security attack surface.

Control Variables (All models): Tobin's Q (Chappell and Cheng, 1984), Firm size (Log of Total Assets), R&D intensity (Wang et al., 2013), Stock market reaction (Tanriverdi & Uysal, 2011), Slack (Iyer & Miller, 2008), Market value (Chappell and Cheng, 1984), Cash holdings (Chappell and Cheng, 1984), historical boundary changing actions 2010-2014 (Haleblian et al., 2006), historical data breaches (2010-2014).

Model Specification

Based on the Hausmann test and Breush-Pagan Lagrange Multiplier tests, we chose to use random effects models by controlling for industry and year effects for all our hypotheses and reporting all models.

H1. The Risk Transfer Behavior: An organization may or may not prefer to transfer its information security risks, which leads us to a yes (Y=1) or no (Y=0) decision of an organization to be investigated with Probit Regression models. Such that: y is the insurance ownership of company i, in year t; $\beta Information\ Security\ Risk\ Perception\ _{(it)}$ is information security risk perception of the company i:

$$\begin{aligned}&\mathrm{H_1: Probit\ (Insurance\ Ownership_{it})} = \beta_{0it} + \beta\mathrm{Information\ Security\ Risk\ Perception_{it}} + \beta\ \mathrm{Market\ Value_{it}} + \beta\ \mathrm{R\&D\ Intensity_{it}} + \beta\ \mathrm{Log\ (Assets)_{it}} + \\ &\beta\ \mathrm{Tobin'sQ_{it}} + \beta\ \mathrm{Profitability_{it}} + \beta\ \mathrm{Stock\ Return_{it}} + \beta\ \mathrm{Cash\ Holdings_{it}} + \beta\ \mathrm{Slack_{it}} + \beta\ \ \mathrm{Total\ Boundary\ Changing\ Actions_{2010-2014}} + \\ &\beta\ \ \mathrm{Total\ Number\ of\ Data\ Breaches_{2010-2014}} + \mathrm{Industry\ Control} + \mathrm{Year\ Control} + \mathrm{u}\end{aligned}$$

H2 &H3. Boundary Changing Behavior: Given that our dependent variable is a ratio (Papke and Wooldridge, 1996) and defined as $0 \leq y \leq 1$, with ratio and binary (0/ 1 values), we used a Fractional Probit regression based on the results of Akaike's Information Criterion (AIC) and Bayesian Information Criterion (BIC) tests.

$$\begin{aligned}&\mathrm{H_2:\ \ Fractional\ Probit\ (Less\ Risky\ Boundary\ Expanding\ Actions)_{it}} = \mathrm{G(}\ \beta_{0it} + \beta\mathrm{Information\ Security\ Risk\ Perception_{it}} + \beta\ \mathrm{Market\ Value_{it}} + \\ &\beta\ \mathrm{R\&D\ Intensity_{it}} + \beta\ \mathrm{Log\ (Assets)_{it}} + \beta\ \mathrm{Tobin'sQ_{it}} + \beta\ \mathrm{Profitability_{it}} + \beta\ \mathrm{Stock\ Return_{it}} + \beta\ \mathrm{Cash\ Holdings_{it}} + \beta\ \mathrm{Slack_{it}} + \\ &\beta\ \ \mathrm{Total\ Boundary\ Changing\ Actions_{2010-2014}} + \beta\ \ \mathrm{Total\ Number\ of\ Data\ Breaches_{2010-2014}} + \mathrm{Industry\ Control} + \mathrm{Year\ Control} + \mathrm{u)}\end{aligned}$$

$$\begin{aligned}&\mathrm{H_{2a}:\ \ Fractional\ Probit\ (Less\ Risky\ M\&A_{it})} = \mathrm{G(}\ \beta_{0it} + \beta\mathrm{Information\ Security\ Risk\ Perception_{it}} + \beta\ \mathrm{Market\ Value_{it}} + \beta\ \mathrm{R\&D\ Intensity_{it}} + \\ &\beta\ \mathrm{Log\ (Assets)_{it}} + \beta\ \mathrm{Tobin'sQ_{it}} + \beta\ \mathrm{Profitability_{it}} + \beta\ \mathrm{Stock\ Return_{it}} + \beta\ \mathrm{Cash\ Holdings_{it}} + \beta\ \mathrm{Slack_{it}} + \\ &\beta\ \ \mathrm{Total\ Boundary\ Changing\ Actions_{2010-2014}} + \beta\ \ \mathrm{Total\ Number\ of\ Data\ Breaches_{2010-2014}} + \mathrm{Industry\ Control} + \mathrm{Year\ Control} + \mathrm{u)}\end{aligned}$$

$$H_{2b}\text{: Fractional Probit (Less Risky Third Party Partnerships}_{it}) = G(\beta_{0it} + \beta\text{Information Security Risk Perception}_{it} + \beta\text{ Market Value}_{it} + \beta\text{ R\&D Intensity}_{it} + \beta\text{ Log (Assets)}_{it} + \beta\text{ Tobin'sQ}_{it} + \beta\text{ Profitability}_{it} + \beta\text{ Stock Return}_{it} + \beta\text{ Cash Holdings}_{it} + \beta\text{ Slack}_{it} + \beta\text{ Total Boundary Changing Actions}_{2010-2014} + \beta\text{ Total Number of Data Breaches}_{2010-2014} + \text{Industry Control} + \text{Year Control} + u)$$

$$H_{3}\text{: Fractional Probit (Boundary Preservation}_{it}) = G(\beta_{0it} + \beta\text{Information Security Risk Perception}_{it} + \beta\text{ Market Value}_{it} + \beta\text{ R\&D Intensity}_{it} + \beta\text{ Log (Assets)}_{it} + \beta\text{ Tobin'sQ}_{it} + \beta\text{ Profitability}_{it} + \beta\text{ Stock Return}_{it} + \beta\text{ Cash Holdings}_{it} + \beta\text{ Slack}_{it} + \beta\text{ Total Boundary Changing Actions}_{2010-2014} + \beta\text{ Total Number of Data Breaches}_{2010-2014} + \text{Industry Control} + \text{Year Control} + u)$$

where G is a non-linear function (cdf) that transforms values between [0,1] for all real numbers, satisfies $0 < G(z) < 1$ for all z. Different from the Probit model, the coefficients in this non-linear function are estimated from the following quasi maximum likelihood function.

$$\sum_{i}[w_{it}y_{it}\ln(\Phi(X_{it}\beta)) + w_{it}(1-y_{it})\ln(1-\Phi(X_{it}\beta))]$$

Findings

We theorize that organizations might have different motivations for boundary-changing actions, however, the information security risk perception of those organizations shapes their boundary-changing actions to expand or preserve their boundaries and risk transfer behavior. Results are presented in Table 3.

	I: H1: Information Security Risk Hedging	II: H2: Less Risky Boundary Expansion	III: H2a: Less Risky M&A	IV: H2b: Less Risky Alliances	V: H3: Boundary Preservation
Independent Variable $_{(t)}$					
Information Sec Risk Spectrum	0.00165*** (0.000220)	0.000322+ (0.000191)	0.000366+ (0.000207)	0.000760** (0.000274)	-0.000129 (0.000239)
Control Variables $_{(t-1)}$					
Market Value	-0.000000883	-0.000000229	-8.46e-08	0.000000114	-0.0000034***
	(0.000000739)	(0.000000477)	(0.000000580)	(0.000000596)	(0.000000931)
R&D Intensity	-2.116*	0.422	1.111	0.312	-2.459*
	(0.995)	(0.764)	(0.877)	(1.076)	(1.216)
Log (Assets)	0.0260	-0.0517	0.00857	0.153*	0.313***
	(0.0517)	(0.0443)	(0.0491)	(0.0676)	(0.0592)
Tobin's Q	0.0411	0.00440	-0.00727	0.0410	0.0296
	(0.0291)	(0.0253)	(0.0271)	(0.0362)	(0.0428)
Profitability (ROA)	0.0573	0.557	0.876	-0.601	-1.042
	(0.570)	(0.502)	(0.577)	(0.654)	(0.738)
Cash Holdings	0.291	-0.580+	-0.741*	0.710	-1.094*
	(0.356)	(0.334)	(0.360)	(0.490)	(0.556)
Slack	-0.0982*	0.0378	0.0554	-0.0508	-0.00757
	(0.0388)	(0.0319)	(0.0341)	(0.0441)	(0.0555)
Stork Return	-0.0000603 (0.00101)	0.000596 (0.000801)	0.000229 (0.000866)	-0.000997 (0.00113)	-0.00125 (0.00122)
Historical BCA	-0.000801 (0.00463)	0.0235*** (0.00377)	0.0246*** (0.00418)	0.0155*** (0.00463)	0.0206*** (0.00486)
Historical Breach (2010-2014)	0.0783+ (0.0425)	0.0353 (0.0363)	-0.0203 (0.0476)	0.0937+ (0.0546)	0.0288 (0.0487)
Year Control	Y	Y	Y	Y	Y
Industry Control	Y	Y	Y	Y	Y
Chi2	206.3	120.9	103.8	129.8	155.8
AIC	1760.1	1362.1	1453.7	522.4	1228.3
BIC	1872.6	1474.6	1566.1	634.9	1340.8
N	1566	1566	1566	1566	1566

Table 3. Results

Model I in Table 3 indicates that an organization's information security risk perception is associated with its risk hedging (risk transfer) behavior, H1 [ß=0.00165] is supported. Model II in Table 3 shows that an organization's information security risk perception is positively associated with its less risky boundary expansion behavior, H2 [ß=0.003] is supported. Model III in Table3 shows that organizations' information security risk perception is positively associated with their less risky M&A preferences, H2a [ß=0.0036] is supported. Model IV in Table 3 shows that organizations' information security risk perception is positively associated with their less risky third-party partnership preferences, H2b [ß=0.0076] is supported. Model V in Table 3 shows that organizations' information security perception is not significantly associated with its boundary-changing actions, and H3 is not supported. Even though we could not find support for our H3, we found an interesting point in our supplementary analysis. In our supplementary analysis for Model V, we find that organizations that perceive the financial effects[ß=0.069] of information security risks are less likely to preserve their organizational boundaries, meaning that they tend to do more diversification, and this might be because of more compelling business considerations.

Conclusion

We aim to shed a light on how organizations' boundary-changing actions are shaped by their information security risk perceptions. Understanding how organizations perceive their information security risks provided us an opportunity to explore the mechanisms behind their decision-making to transfer, accept, reduce, or avoid information security risks. We find that organizations might have different motivations for boundary changing actions, however information security risk perception of those organizations shapes their boundary changing actions to expand their boundaries, and their decisions to hedge the information security risks. We also investigated each hypothesis with 10 domain effects and information security risk perception. Such as, we find that organizations that perceive the financial effects of information security risks are more likely to purchase cyber insurance and hedge the risk, while organizations that perceive the third-party effects are more likely to prefer less risky boundary expanding actions.

We fine-tune 10 generic, 1 domain-specific state-of-the-art transformer-based NLP model with domain knowledge and measure an organization's information security risk perceptions with a causal extraction approach from annual statements. To our knowledge, our research is one of the initial attempts to borrow the causal extraction approach and combine it with transformer-based NLP models to measure how information security risk and its effects are perceived by organizations systematically in this domain.

Practical Implications

The market for insuring against these losses has grown rapidly in the past decade and is expected to be $20 billion worth market by 2025 (Romanosky et al. 2019). We believe that our research findings might have practical implications for the cyber insurance market. An organization that perceives to be more vulnerable to system & infrastructure effects while another that perceives to be more vulnerable to data effects might need different contracts and be subject to different premiums. Considering their perceived vulnerabilities in the cyber insurance contracts might decrease the information asymmetry in the cyber insurance market. On the other hand, considering organizations' risky boundary expansion and preservation behavior concerning their information security risk perceptions, moral hazard problems, and free-rider issues in the cyber insurance market might be evaluated. Let's assume that company A perceives to be more vulnerable in system & infrastructure effects of information security risks is going to acquire company B which is also perceived to be more vulnerable in system & infrastructure effects of information security risks from another industry. In the case of companies, A and B being insured by the same insurance company, if any breach incident that occurs at company A cascades to company B and jeopardizes the insurer's business and capital. Therefore, we believe that information security risk perception of the organizations might be considered to understand how they perceive their vulnerabilities and how strong their risk appetite for boundary changing actions, by also considering how their vulnerability and boundary changing behavior impact market efficiency.

Implications for Research

Some important issues remain for future research. We only considered S&P 500 companies for the 2015 - 2018-year, future research might expand the sample space and time window. Such that, in our exploratory data analysis, we were able to observe that organizations perceive relatively more effects of information security risks after 2016. This might be because of General Data Protection Regulation (GDPR) that was released on 14th April 2016. Future research might investigate why some companies perceived more effects (and different effects) of information security risks with respect to their peers following GDPR.

Cyber insurance coverages are found to exclude cyber breaches caused by the act of terrorism, war, and military action (Romanosky et al. 2019). As we discussed above, insurers might jeopardize their business and capital when several parties they insured are impacted by a breach incident. Therefore, how organizations could hedge their information security risks when a cyber-attack is due to military action or war is an interesting question, especially in today's world where we are facing international conflicts and an increasing number of cyber-attacks due to these conflicts.

REFERENCES

Akkasi, A., and Moens, M. F. 2021. “Causal relationship extraction from biomedical text using deep neural models: A comprehensive survey,” *Journal of Biomedical Informatics*, (119: 103820).

Araci, D. 2019. “Finbert: Financial sentiment analysis with pre-trained language models,”. *arXiv preprint arXiv:1908.10063*.

Banker, R. D., and Feng, C. 2019. “The impact of information security breach incidents on CIO turnover,” *Journal of Information Systems* (33:3), pp. 309-329.

Baysinger, B., and Hoskisson, R. 1989. “Diversification strategy and R&D intensity in multiproduct firms,” *Academy of Management Journal* (32), pp. 310-332.

Bolot, J. C., and Lelarge, M. 2008. “A new perspective on internet security using insurance,”. In *INFOCOM 2008-The 27th Conference on Computer Communications*, pp. 1948-1956.

Borky, J. M., and Bradley, T. H. 2018. *Effective model-based systems engineering*. Springer.

Cyert, R. M., and March, J. G. 1992. *A behavioral theory of the firm*. Martino Publication. (originally published in 1963)

Devlin, J., Chang, M. W., Lee, K., and Toutanova, K. 2018. “Bert: Pre-training of deep bidirectional transformers for language understanding,” *arXiv preprint arXiv:1810.04805*.

Dranikoff, L., T. Koller, and Shneirder A. 2002. “Divestiture: Strategy's Missing Link.” *Harvard Business Review,* pp. 74-83.

Fiegenbaum, A., and Thomas, H. 1988. “Attitudes toward risk and the risk-return paradox: prospect theory explanation,” *Academy of Management journal* (*31*:1), 85-106.

Florakis, C., Louca, C., Michaely, R., and Weber, M. 2020. “Cybersecurity Risk (No. w28196),” *National Bureau of Economic Research*.

Gavetti, G., Greve, H. R., Levinthal, D. A., and Ocasio, W. 2012.” The behavioral theory of the firm: Assessment and prospects, “Academy *of Management Annals* (*6*: 1), pp. 1-40.

Goll, I., and Sambharya, R. B. 1998. “Rational model of decision making, strategy, and firm performance.” *Scandinavian Journal of Management* (14:4), 479-492.

Haleblian, J., Kim, J., & Rajagopalan, N. 2006. “The influence of acquisition experience and performance on acquisition behavior: Evidence from the U.S. commercial banking industry,” *Academy of Management Journal (49*-2), pp.357-370.

Hassanzadeh, O., Bhattacharjya, D., Feblowitz, M., Srinivas, K., Perrone, M., Sohrabi S., Katz, M. 2019. “Causal Knowledge Extraction through Large-Scale Text Mining.” AAAI 2020, pp. 13610-136112.

Henningsson, S. and Kettinger, W.J., 2016. “Understanding information systems integration deficiencies in mergers and acquisitions: A configurational perspective,” *Journal of Management Information Systems 33*(4), pp.942-977.

Henningsson, S., Yetton, P.W. and Wynne, P.J., 2018. “A review of information system integration in mergers and acquisitions,” Journal *of Information Technology*, *33*(4), pp.255-303.

Henry W, C., and Cheng, D. C. 1984. “Firms' acquisition decisions and Tobin's q ratio,” *Journal of Economics and Business (36*:1), pp. 29-42.

Herath, H., and Herath, T. 2011. “Copula-based actuarial model for pricing cyber-insurance policies,” *Insurance Markets and Companies: Analyses and Actuarial Computations(*2:1), pp.7-20.

Hurley, R. F., and Hult, G. T. M. 1998. “Innovation, Market Orientation, and Organizational Learning: An Integration and Empirical Examination,” *Journal of Marketing* (62:3), pp. 42-54.

IBM. 2021. *Cost of a data breach study*. Ponemon Institute.

Iyer, D. N., and Miller, K. D. 2008. “Performance feedback, slack, and the timing of acquisitions,” *Academy of Management Journal* (51:4), pp.808-822.

Johnson, S. 2010. SEC Pushes Companies for More Risk Information. URL: *http://www.cfo.com/article.cfm/14513695*. (visited June 6, 2020).

Kapoor, R., and Lim, K. 2007. “The impact of acquisitions on the productivity of inventors at semiconductor firms: A synthesis of knowledge-based and incentive-based perspectives,” *Academy of Management Journal*, (50:5), 1133-1155.

Khalili, M.M., Naghizadeh, P. and Liu, M., 2017.” Embracing risk dependency in designing cyber-insurance contracts,” In *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 926-933.

Kwon, J., Ulmer, J. R., and Wang, T. 2013. “The association between top management involvement and compensation and information security breaches,” *Journal of Information Systems* (27:1), pp.219-236.

Kwon, J. and Johnson, M.E., 2014. "Proactive versus reactive security investments in the healthcare sector," *MIS Quarterly*, 38(2), pp.451-A3.

Laughhunn, D. J., Payne, J. W., and Crum, R. 1980. "Managerial risk preferences for below-target returns," *Management Science*, (26:12), pp.1238-1249.

Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., ... and Stoyanov, V. 2019. "Roberta: A robustly optimized Bert pretraining approach." *arXiv preprint arXiv:1907.11692*

Majchrzak, A., Jarvenpaa, S. L., and Bagherzadeh, M. 2015." A review of interorganizational collaboration dynamics," *Journal of Management* (41:5), pp. 1338-1360.

Manadhata, P. K., and Wing, J. M. 2010. "An attack surface metric," *IEEE Transactions on Software Engineering (*37: 3), pp.371-386.

March, J. G., and Shapira, Z. 1987. "Managerial perspectives on risk and risk-taking," *Management Science* (33:11), pp. 1404-1418.

March, J. G., and Simon, H. A. 1993. Organizations John Wiley & Sons. *New York*. (original work published in 1958).

Majchrzak, A., Jarvenpaa, S. L., and Bagherzadeh, M. 2015. "A review of interorganizational collaboration dynamics," *Journal of Management* (41: 5), pp. 1338-1360.

Majuca, R. P., Yurcik, W., and Kesan, J. P. 2006. "The evolution of cyber insurance," *arXiv preprint cs/0601020*.

Mintzberg, H. 1983. *Power in and around organizations*. Prentice-Hall.

Montgomery, C., A. Thomas, and R. Kamath. 1984. "Divestiture, Market Valuation, and Strategy." *Academy of Management Journal*, pp. 830-840.

Ogbanufe, O., Kim, D. J., and Jones, M. C. 2021. "Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures," *Information & Management* (*58*:7), pp.1-18.

Penrose E. 1959. *The Theory of the Growth of the Firm*. Wiley: New York.

Romanosky, S., Ablon, L., Kuehn, A. and Jones, T., 2019. "Content analysis of cyber insurance policies: How do carriers price cyber risk?," *Journal of Cybersecurity*, 5(1).

Ryu, C., Kim, Y. J., Chaudhury, A., and Rao, H. R. 2005. "Knowledge Acquisition via Three Learning Processes in Enterprise Information Portals: Learning-by-Investment, Learning-by-Doing, and Learning-from-Others," *MIS Quarterly* (29:2), pp. 245-278.

SEC.2011. *CF Disclosure Guidance: Topic No.2 URL: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm* (visited on November 17, 2021).

Tanriverdi, H., Roumani, Y., and Nwankpa, J. 2019. "Structural Complexity and Data Breach Risk," *ICIS 2019 Proceedings*. *pp*. 1-18. Munich: ICIS.

Tanriverdi, H., and Uysal, V. B. 2011. "Cross-business information technology integration and acquirer value creation in corporate mergers and acquisitions," *Information Systems Research* (22:4), pp.703-720.

Teece D. 1980. "Economies of scope and the scope of the enterprise," *Journal of Economic Behavior and Organization,* pp. 223–247.

Theisen, C., Munaiah, N., Al-Zyoud, M., Carver, J. C., Meneely, A., and Williams, L. 2018." Attack surface definitions: A systematic literature review," *Information and Software Technology* (104), pp. 94-103.

Uzzi, B. 1996. "The sources and consequences of embeddedness for the economic performance of organizations: The network effect," *American sociological review*, pp. 674-698.

Villalonga, B., and McGahan, A. 2005. "The choice among acquisitions, alliances, and divestitures." *Strategic Management Journal* (26), pp. 1183-1208.

Von Solms, R., and Van Niekerk, J. 2013." From information security to cyber security," *Computers & Security* (38), pp. 97-102.

Wang, T., Kannan, K. N., and Ulmer, J. R. 2013. The association between the disclosure and the realization of information security risk factors. *Information systems research*, (*24*: 2), pp. 201-218.

White Hat. 2018. *WhiteHat Security 2018 Application Security Statistics Report*. White Hat.

Yin, X., and Shanley, M. 2008." Industry determinants of the 'merger versus alliance' decision," *Academy of Management Review*, (33: 2), pp. 473-491.

Zakay, D., Ellis, S., and Shevalsky, M. 2004. "Outcome Value and Early Warning Indications as Determinants of Willingness to Learn from Experience," *Experimental Psychology* (51:2), pp.150-157.