The Informativeness of Cybersecurity Risk Disclosure

Introduction

Do they know?

Firm's acknowledgement and disclosure of its cybersecurity weaknesses and/or breaches is a crucial first step in the process of improving the firm's cybersecurity infrastructure

(He, Lee, Han, and Whinston 2016)

For what purpose?

Disclosing cybersecurity information, such acknowledgement could be considered as an externality for enhancing social welfare

(Gal-Or and Ghose 2005; Moore and Clayton 2011; Kunreuther and Heal 2003)

H1: Firms changes their contents of cybersecurity risk disclosure

when breach or ICW gets reported. (Breach: Self-reported / ICW: Auditor-reported)

Introduction

Vulnerability

Firms could provide less informative cybersecurity risk disclosure to obfuscate cybersecurity risk factors to deter future cyber threats, or simply they have not acknowledged their risk factors or the actual breach (i.e. breach detection gap) (Li et al. 2018)

Control

Firms could provide informative cybersecurity risk disclosure to signal the market to show their readiness to counter cybersecurity (Tang et al. 2013)

H2: Firms disclose relevant and effective controls to mediate their disclosed vulnerability which leads to future cybersecurity breach.

Exploratory Factor Analysis

		Component					
	1	2	3	4	5	6	7
T15	-0.680						
T23	-0.665						
T16	0.636						
T20	-0.621						
T10	0.611						
T0	0.584						
T2	-0.547	0.534					
T4	0.542						
T24	0.521						
T11	0.383						
T5		-0.750					
T26		-0.692					
T29		-0.679					
T1		0.667					
T6			-0.834				
T7			-0.665				
T22			0.597				
T28			-0.497				
T3			0.468				
T14			-0.461				
T12				-0.715			
T9				0.706			
T13				0.626			
T17					-0.783		
T21					0.756		
T18					0.478		
T25						-0.846	
T8						-0.679	
T19							0.726
T27							0.548

Extraction Method: Principal Component Analysis.
7 components extracted. Coefficients suppressed by 0.45.

Coefficients of each topic:

Positive – Related to Control

Negative – Related to Vulnerability

Each Components:

Business Continuation

Data Security

Data Regulation

Third Party Security

Network Security

e-commerce Security

Exploratory Factor Analysis

Level	Topic	Cluster	Label	Most Relevant Keywords	PP
Business Continuation	T15	Vulnerability	System Interruption	System, Security, Interruption	0/10
	T23	Vulnerability	Service Discontinued	System, Disruption, Customer	0/10
	T16	Control	Data Back-up	Repatriation, Duplication, Informatics	2/10
	T20	Vulnerability	System Intrusion	Breach, Attack, TPSPS	1/10
	T0	Control	Breach Reporting (Whistleblower)	Qui, Tam, Whistleblower	5/10
	T2	Vulnerability	System Breach	System, Breach, Technology	7/10
	T4	Control	Identification/Detection Model	ROM, DSH, CLO	6/10
	T24	Control	Remedial Action	Remediate, Imperfection, Azusa	4/10
Data Regulation	T5	Vulnerability	Violation of Data Regulation	Information, Security, Regulation	0/10
	T26	Vulnerability	Privacy Law	Privacy, Law, Regulation	0/10
	T29	Vulnerability	Violation of HIPAA	Privacy, Health, Breach	0/10
	T1	Control	Regulation Compliance	Regulation, Compliance, Guidance	0/10
Data Security	T6	Vulnerability	Litigation Cost (Data Breach)	Litigation, Cost, Loss	0/10
	T7	Vulnerability	Data Loss	Data, Information, Loss	0/10
	T22	Control	Access Control	Onesign, Authentication, Control	5/10
	T28	Vulnerability	Data Breach	Information, breach, security, loss	0/10
	T3	Control	Intrusion Prevention	NGIPS, SM, Fingerprint	7/10
	T14	Vulnerability	Reputation Loss	Reputation, Loss, Customer	0/10
Third-Party Security	T12	Vulnerability	SCM Data Leak	Data, Breach, TPSPS	2/10
	T9	Control	Supply Chain Security	CRD, RSD, ELA	7/10
	T13	Control	SCM Risk Mitigation	Fluctuation, Remediate, PGE	5/10
Network Security	T17	Vulnerability	Network Breach	Security, Breach, Network	1/10
	T21	Control	Network Security	IoT, Internet, IPSec	6/10
	T18	Control	Countermeasures for Network Security	Instrument, logon, hacktivists	5/10
e-commerce	T19	Control	e-commerce Assurance	Websense, Auditing, CLO	4/10
	T27	Control	Financial Transaction Regulation	RSD, CRD, Tract	4/10

Hypothesis Test

Hypothesis 1:

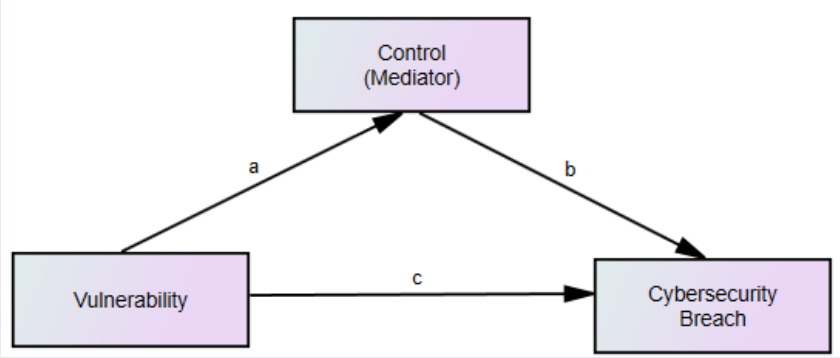
Regression Analysis

$$TML_{k,t} = \beta_0 + \beta_1 Breach_t + \beta_2 ICW_t + \beta_3 Breach * ICW_t + \beta_4 Industry_t + \beta_5 Net\ Income_t + \beta_6 Employee_t + \beta_7 R\&D\ Expenses_t + \beta_8 Intangible\ Assets_t + \epsilon_t$$

Firm Fixed Effect / Year Effect Included

Hypothesis 2:

Structural Equation Model



Mediation Effect of Control on Vulnerability