IT Risk Factor Disclosure and Stock Price Crashes

Victor Song
Sauder School of Business
University of British Columbia
victor.song@sauder.ubc.ca

Hasan Cavusoglu
Sauder School of Business
University of British Columbia
cavusoglu@sauder.ubc.ca

Gene M. Lee
Sauder School of Business
University of British Columbia
gene.lee@sauder.ubc.ca

Mary L. Z. Ma
School of Administrative Studies
York University
mlizhiyk@yorku.ca

Abstract

As firms are increasingly more dependent on Information Technology (IT) for their business strategies and value creation activities, risks associated with IT become one of the top concerns for corporate boards and managers. This study examines the impact of IT-related risk factor disclosure in Item 1A of the 10-K annual report on stock price crashes. We use Latent Dirichlet Allocation topic modeling to identify risk categories in risk disclosures between 2006 and 2017. IT risk emerged as one of the key risk categories. We find that IT risk disclosure is positively correlated with a firm's future stock price crash risk. We further separate IT risk factor disclosures into two categories: IT value risk that relates to a firm's use of and reliance on information technology for its operations to reach its goals and objectives, and cybersecurity risk that could lead to a loss or leak of data. We find that while the correlation between cyber security risk disclosure and a firm's future crash risk is significant, IT value risk disclosures do not have a significant correlation.

1 Introduction

Long considered as a strategic asset for organizations, information technology (IT) has become essential for the success and even survival of the firm. IT plays a significant strategic and operational role in businesses. It is, therefore, the key responsibility of management to manage the risks associated with information systems (IS) to minimize their negative consequences to the firm [1]–[3]. As publicly traded firms are required to disclose their IT risks along with the other risks that they are exposed to in their annual financial filings with the SEC, the question then arises as to whether these risk disclosures are important, and what the long-term impacts of these disclosures are to the firm.

A considerable amount of research has examined the relation between IT failure events and its immediate market effects. Cavusoglu et al. [3] found that a cybersecurity breach costs a target firm on average $1.65 billion per announcement. Bharadwaj et al. [4] found that IT failures results in a 2% drop in stock prices over a two-day window. Viewing IT failure as a strategic weakness, Goldstein et al. [5] also found a negative stock price relation to the IT failures. On the contrary, Gordon et al. [6] found that information security announcements actually increase a firm's stock prices, arguing that such disclosures signal active involvement by the firm in securing their IT assets.

However, to the best of our knowledge, there is no existing study in the IS literature that looks at the *long-term* effect of IT risk disclosures on the firm. Risk factor disclosures can hint at future firm performance degradations, but IT risk disclosure literature is sparse. Wang et al. [7] looked at IT security risk factors and its linkage to the realization of data breaches, but their dataset is limited to hand-collected cybersecurity breach announcements in major media outlets and they do not look into the market impact of the risk disclosure itself. Furthermore, cybersecurity risks are not the only information technology related risks that a firm is exposed to. Yet, the existing literature predominantly focuses on cybersecurity.

This paper aims to contribute to the risk factor disclosure literature by filling in the knowledge gap concerning the long-term effects of IT-related risks. Our primary research question is whether IT-related risk factor disclosures affect a firm's stock price crash risk, a long-term stock return measure. And if so, do cybersecurity and other IT risks differ in their

URI: https://hdl.handle.net/10125/64480
978-0-9981331-3-3

impact? To answer our research question we use topic modeling techniques to identify IT risk disclosures in Item 1A in 10-K filings. We use the resource weaknesses perspective from strategic management literature as a theoretical guide to categorize the IT risk disclosures into IT value and IT cybersecurity risk disclosures.

We found that, consistent with our main hypothesis, IT risk factor disclosures are positively associated with the long-term stock price crash risk of the company. IT cybersecurity risk factors in particular were found to have a positive association with the crash risk, but IT value risk factors did not.

2 Stock Price Crash Risk

Our paper focuses on stock price crash risk, which captures the chances of extreme negative returns in a firm's stock. Theoretically, stock price crashes are caused by managers withholding negative information about the firm and preventing that information from being made public. When the amount of negative information being stockpiled reaches a level that managers cannot withhold any longer, the bad news is released all at once, leading to a stock price crash [8]. The accounting literature investigates several determinants of crash risk, however, there is as yet no study that investigates the effect of IT risk factor disclosures on stock price crash risk.

3 Hypothesis Development

Given the important role of IS/IT plays in day-to-day business operations and overall firm strategy in any contemporary organization, failures in a firm's IT adversely influence the firm's ability to achieve its business objectives and gain a competitive advantage. In any firm, IS implementations are initiated to deliver business value to the firm. However, there is always a risk that the firm may not be able to gain the intended benefits from the IS/IT, and investors are keenly aware of the risks associated with IT [9]. There are many causes of this risk, including implementation challenges, unmanaged complexity (scope creep), IT governance issues, or poorly specified project requirements to name a few. As previous studies have shown, there are severe consequences to a firm's stock price when IT risks materialize and an IT failure occurs [4], [5], [10].

We argue that, if an existing IT system or a newly implemented IT project has a significant risk of failure to achieve its performance goals and to deliver value to the firm, managers will attempt to hide the information from outside investors for as long as possible to avoid damage to the firm's value. This hoarding of bad news about the IT systems of a firm will eventually reach a tipping point, and the information will be released to the market all at once and induce a stock price crash. The bubble "bursting" can occur when investors recognize that the expected progress has not been achieved for ongoing projects or intended performance improvements have not been delivered for the existing IT. The bad news could also be revealed to the market if the IT risk is materialized (e.g. the firm experienced a data breach) or an IT failure occurs (e.g., the firm experienced an IS/IT related outage). In this way, IT risk factors can be viewed as an early indicator for future bad news announcements related to a firm's information systems that cause stock price crashes. We postulate that, due to the requirements of the SEC to disclose any and all risk factors, IT-related risk factor disclosures in a firm's 10-K would cut through the veil of opacity and reveal that the firm's IS/IT may not deliver its intended business value or be well protected. Hence, we hypothesize:

***H1**: IT-related risk factor disclosures are positively correlated with a firm's stock price crash risk.*

As discussed previously, IT has an inherent risk in failing to deliver its full value to the firm. A firm's inability to leverage its IT resource can cause the firm to fail to appropriate the intended value of IT, but not all IT failures can be explained through that theoretical lens. A firm can possess necessary competencies to implement IT systems successfully, derive value from its IT investments, and gain a competitive advantage as a result, while it may also fail to protect against cybersecurity attacks such as Denial-of-Service attacks. Additionally, a cyber attack may not always affect a firm's ability to operate, especially if only a data breach is involved; the subsequent news of the breach will certainly temporarily affect the company's market value and/or goodwill but will not affect the company's ability to function.

We point out these two distinct modes of failure and risks, thus we break down IT risk into two types: IT cybersecurity risk and IT value risk. First, IT value risk is the risk that the firm will not be able to realize the full-intended value of the IT systems. This risk *originates* from the firm's (lack of) skills and competencies in implementing and running an IT system and deriving its full-intended value. The lack of maturity in the firm's IT strategy, governance, and management processes is often to blame. Second, IT cybersecurity risk is any risk that the confidentiality, availability, or integrity of a firm's IT and data assets can be adversely affected, often through attacks from adversaries [11] and that causes harm to the firm's business objectives either through negative press or a loss of function of the firm's IT systems. Importantly, we differentiate the two types of IT risk based more so

on the *sources* of the risk rather than the impact on firm's operations when the risk is materialized.

We theorize that IT value risk disclosures will reflect the firm's inability to fully utilize their IT systems. That is, the more IT value risks the firm disclosures, the more informed the investors will be about the firm's increasing inability to capture the full value from their IT systems and the more informed the investors will be about the state of the firm's IS. The information that suboptimal IT/IS generates would be inaccurate, incomplete, or not timely. The managers and executives relying on the information from these systems would make suboptimal decisions, resulting in performance degradation and increasing the risk of a major stock price crash. Furthermore, as IS/IT is ingrained in all aspects of businesses, suboptimal IS/IT would cause inefficiencies in the business processes, resulting in further performance degradation. Thus, we postulate that:

H1a*: IT value risk disclosures are positively correlated with a firm's stock price crash risk.*

Vulnerabilities in IS/IT that an organization possesses are liability for the firm. Malicious internal users and external hackers would exploit these vulnerabilities. We argue that IT cybersecurity risk disclosures will reflect the firm's lack of protection for their IT assets from cybersecurity risks. That is, the more cybersecurity risks the firm disclosures, the more informed the investors will be about the firm's increasing inability to protect its IT infrastructure and underlying key business data. Hence, we posit that:

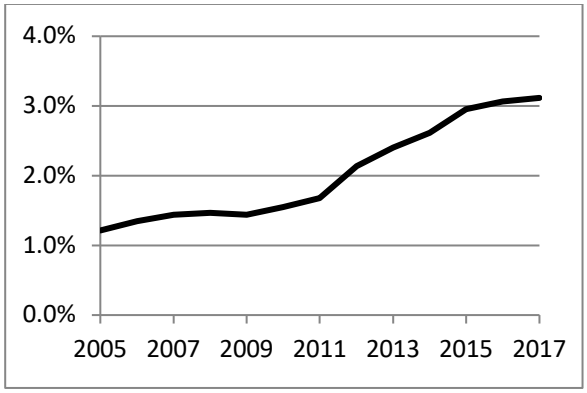
H1b*: IT cybersecurity risk disclosures are positively correlated with a firm's stock price crash risk.*

4 Data Collection

We collect and analyze the data on U.S. publicly traded firms to examine the relationship between risk factor disclosure and stock price crash risk. We obtain risk factor disclosures from Item 1A of Form 10-K annual reports filed by publicly traded companies to the U.S. Securities and Exchange Commission (SEC). The SEC mandated companies to include Item 1A in their 10-K filings since December 2005. Hence, our data sample includes 10-K filings submitted from December 2005 to July 2017. We collected 96,223 annual reports with reporting periods ranging from fiscal year 2005 to fiscal year 2016.

To extract IT-related risk factor disclosures from the annual reports, we wrote a heuristic algorithm that uses the HTML structure of a 10-K filing to identify and collect individual risk factors in Item 1A of the filing. Specifically, the algorithm parses the HTML filing and builds a Document Object Model (DOM) of the filing. Using this algorithm, we managed to extract 1.72 million risk factors from 62,324 10-K filings. Overall, risk factors were extracted from 85.864.8% of all available 10-K filings in our sample period.

Figure 1. Percentage of Risk Factor Disclosures in Item 1A that are IT Related for Years 2005 to 2017



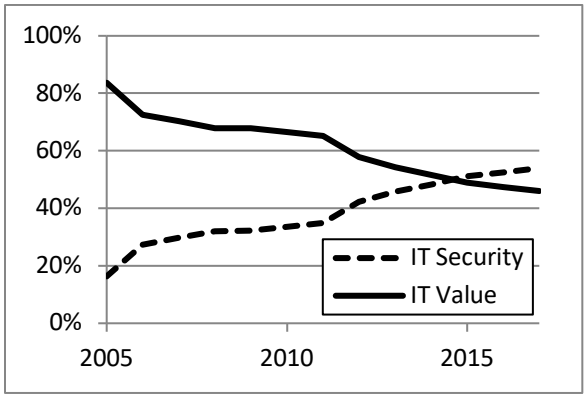
We use latent Dirichlet allocation (LDA) [12] to extract 40 risk factor topics from our corpus of 1.72 million risk factors. We used a model fitness statistic commonly used in the topic modeling literature called the perplexity score to tune our number of topics. We manually labeled the 40 topics according to the words with the highest word weights for each topic and identified one risk factor topic that was IT related. The LDA algorithm assumes a generative process through which each document in corpus was created. In particular, each document is characterized as random mixture over latent topics and each topic is characterized by a distribution over all the words in the corpus. The LDA algorithm reverse engineers the generative process and results in document-topic distribution matrix and topic-word distribution matrix. Using the topic weights of each risk factor (i.e. a row in the first matrix)[1], we identified 30,987 IT related risk factors.

Consistent with the strategic management literature [13] , our theory postulated that there are two distinct broad classes of IT-related risk. To identify IT

[1] If a topic has the highest weight, the risk factor is considered to be related to the corresponding topic and that topic only. We used other cut-off values of 0.05 and 0.1 (in which case a risk factor can have multiple topics) and our qualitative results have not changed.

value and IT cybersecurity risk factor disclosures from 10-K reports, we run another LDA again using the 30,987 IT related risk factors as a corpus. We specified a 5-topic LDA model and manually mapped each topic to either IT value related or IT cybersecurity related according to the top keywords in the topic. Each IT risk factor was classified as an IT value risk factor or IT cybersecurity risk factor according to a simple majority of the sum of its topic weights belonging to IT value or IT cybersecurity, respectively, and we plot the proportion of IT value risk factors and IT cybersecurity risk factors disclosed per year in Figure 2 below.

Figure 2 Number of IT Cybersecurity Risk Factors and IT Value Risk Factors as a Percentage of Total IT-Related Risk Factor Disclosures



We obtain firm-related data from Compustat and stock return data from CRSP. After excluding observations with missing data, our final dataset includes 11,857 unique firms across 30,347 firm-year observations.

5 Dependent and Independent Variables

Our main independent variables are related to the risk disclosures. We used the topic of each risk factor disclosure found in the 10-K document to calculate the risk disclosure variables of interest for each firm year observation. Subscripts *i* and *t* denote the 10-K filing for firm *i* in year *t*. IT risk disclosure (i.e., $ITRFD_{it}$) is the count of risk factors associated with the IT topic (i.e., topic 24), found in the 10-K filing for firm *i* in year *t*. Each risk topic disclosure (i.e., $RFTOPIC_{it}^{n}$ where $n \in [1,40]$) is the count of risk factors associated with topic *n*. When the model of interest aims to disentangle the impacts of different classes of IT risk, we used IT risk topic assignment. In particular, IT value risk disclosure (i.e., $ITPERFORM_{it}$) and IT cybersecurity risk disclosure (i.e., $ITSECURITY_{it}$) are obtained as the counts of IT value risk factors and IT cybersecurity risk factors disclosed in the 10-K filing for firm *i* in year *t*.

Our dependent variable is $CRASH_{it+1}$ and it refers to the stock price crash risk for the one-year window following firm *i* filing a 10-K in year *t*. Following prior studies on crash risk [8], [14]–[17], we use the negative skewness of abnormal daily stock return (i.e., *NCSKEW*) as our stock price crash risk measure. Theoretically, the use of negative skewness as a measure for stock price crash risk stems from the dual observation that large movements in the market tend to be negative rather than positive, giving stock returns a negative skew and that volatility tends to go up with negative returns. Additionally, high volatility leads to a high-risk premium, which impairs the impact of good news while enhancing the impact of bad news. Crash risk is linked to negative skewness based on the notion that volatility is a proxy for the intensity of investors' disagreement about a firm and that during periods of high disagreement, bearish investors are likely to be at an information advantage [14]. We obtain control variables from Compustat and also include the number of total risk factors disclosed, $NUMRF_{it}$, as a control variable as well as year and industry dummies.

6 Model

Our first hypothesis is intended to answer if IT risk factor disclosures in general have any correlation with a firm's stock price crash risk. We run the following OLS regression model to test H1.

$$CRASH_{it+1} = \beta_0 + \beta_1 ITRFD_{it} + Controls + \epsilon_{it} \quad (1)$$

where $ITRFD_{it}$ is the count of IT-related risk factor disclosures found in Item 1A for firm *i* in fiscal year *t*, and $CRASH_{it+1}$ refers to our crash risk measure.

Controls includes the following control variables for determinants of crash risk identified in previous studies: firm size for firm *i* at the fiscal year-end *t*, $SIZE_{it}$; book-to-market ratio for firm *i* at the fiscal year-end *t*, BM_{it}; stock return momentum for firm *i* in the fiscal year-end *t*, MOM_{it}; abnormal trading volume for firm *i* in the fiscal year-end *t*, $ABVOL_{it}$; stock return volatility of volume for firm *i* in the fiscal year *t*, $SIGMA_{it}$; leverage ratio of firm *i* at the fiscal year-end *t*, LEV_{it}; return over assets for firm *i* in the fiscal year *t*, ROA_{it}; earnings volatility for firm *i* in the fiscal year *t*, ROA_STD_{it}; operating cycle of firm *i* in the fiscal year *t*, OC_{it}; and sales growth of for firm *i* in the fiscal year *t*, SG_{it}. In all regressions, we also include in our controls dummies for industry using the Fama-French 12 industry classification and dummies for fiscal years 2005 to 2016. When the aim is to disentangle impacts of different classes of IT related

risk disclosures and stock price crash risk, we used the following OLS regression model:

$$CRASH_{it+1} = \beta_0 + \beta_1 ITPERFORM_{it} + \beta_2 ITSECURITY_{it} + \beta_3 ITPERFORM_{it} * ITSECURITY + Controls + \epsilon_{it} \quad (2)$$

where $ITPERFORM_{it}$ and $ITSECURITY_{it}$ refer to the measures for IT value risk disclosure and cybersecurity risk factor disclosure in Item 1A of a 10-K annual report for firm *i* in fiscal year *t*, respectively. We used the same *Controls* and *CRASH* in Equation (1).

7 Results

7.1 Effects of IT Risk Factor Disclosure

Table 1. Effects of IT Risk Disclosure on Stock Price Crashes

	Coefficient	[t-stat]
Intercept	0.630	[4.75]***
ITRFD	**0.069**	**[6.52]***
SIZE	0.007	[0.91]
BM	0.060	[3.72]***
MOM	-0.409	[-6.55]***
SIGMA	-7.875	[-5.70]***
ABVOL	0.003	[2.39]**
ROA	-0.147	[-2.10]**
ROA_STD	0.000	[6.32]***
LEV	-0.017	[-0.26]
SG	0.000	[-0.74]
OC	0.000	[-0.03]
Industry Dummies	Yes	
Year Dummies	Yes	
Obs.	30347	
R^2	0.0445	

H1 is concerned with whether IT risk factor disclosures in general have any effect on a firm's stock price crash risk. To test this, we regressed the number of IT-related risk factors disclosed against the crash risk measures following Equation (1). We run the regression on the crash risk measure (i.e., $NCSKEW_{it+1}$). The regression results are found in **Error! Reference source not found.** and show that IT-related risk factor disclosures are significantly positively related to stock price crash risk for the one-year window following the release of a 10-K annual report. The coefficient (*t*-statistic) for $ITRFD_{it}$ is 0.069 (6.52).

One concern might be that the result that IT related risk factor disclosure is associated the higher stock price crash risk can be affected by the other risk factor disclosures. As a robustness check, we ran the same regression but included the counts of the other 39 risk factor topics into the model specified in (1). That is:

$$CRASH_{it+1} = \beta_0 + \sum_{n=1}^{40} \beta_n RFTOPIC_{it}^n + Controls + \epsilon_{it} \quad (3)$$

where $RFTOPIC_{it}^n$ refers to the count of risk factors of topic *n* for firm *i* in year *t*. $RFTOPIC_{it}^{24}$ is equivalent to $ITRFD_{it}$. The regression results are found in Table 2 and show that the significant coefficient in Model (1) reported in Table 1 remained significant even after controlling for all other risk factor topics.

Table 2. Effects of All Risk Disclosure types on Stock Price Crashes

	Coefficient	[t-stat]
Intercept	0.666	[4.85]***
RFTOPIC1	0.042	[3.85]***
⋮	⋮	⋮
RFTOPIC24 (ITRFD)	**0.058**	**[4.66]***
⋮	⋮	⋮
RFTOPIC40	-0.008	[-0.88]
SIZE	0.004	[0.56]
BM	0.067	[4.04]***
MOM	-0.407	[-6.49]***
SIGMA	-8.223	[-5.80]***
ABVOL	0.002	[1.89]*
ROA	-0.144	[-1.97]**
ROA_STD	0.000	[6.75]***
LEV	-0.034	[-0.46]
SG	0.000	[-0.42]
OC	-0.004	[-0.25]
Industry Dummies	Yes	
Year Dummies	Yes	
Obs.	30347	
R^2	0.0627	

7.2 Cybersecurity and IT Value Risk Disclosures

To examine the relation between IT risk disclosures on stock price crash risk more closely, we look at IT value risk disclosures and IT cybersecurity risk disclosures separately and measure their effect on a firm's stock price crash risk. We followed Equation (2) in regressing the number of IT cybersecurity and IT value risks disclosed against the stock price crash risk and the results are reported in Table 3. The coefficient (*t*-statistic) for $ITSECURITY_{it}$ is 0.051 (2.20), indicating that IT cybersecurity related disclosures are significantly and positively correlated with a firm's stock price crash risk in the one year following such a disclosure. However, the coefficient for $ITPERFORM_{it}$ is not significant. This is not in line with our theoretical expectation.

We believe that differential effects can be explained by how much risks are within the control of

the companies. Since IT value creation is within the purview of the leadership and management teams of the companies, the market can interpret the IT value risk as a risk of doing business. This is also consistent with organizational errors notion of [18] that avoiding an organizational error is "a hygiene or parity factor" not a source of competitive advantage. Since cyber security is often characterized as an arm race between security practitioners and malicious actors [19], even if the organization investments in security technologies to bring the cyber risk to an acceptable level, the ability of the firm to deal with the constantly-evolving vulnerabilities and attack vectors deteriorates very quickly. Therefore, cybersecurity risk disclosure can be viewed as an admission of deteriorating conditions of the cybersecurity risks that the firm is exposed to beyond the acceptable level.

Table 3. Effects of IT Value Risk Disclosure and IT Security Risk Disclosure on Stock Price Crashes

	Coefficient	[t-stat]
Intercept	0.627	[4.76]***
ITPERFORM	0.032	[0.86]
ITSECURITY	**0.051**	**[2.20]****
*ITPERFORM*ITSECURITY*	-0.028	[-0.82]
SIZE	0.008	[1.08]
BM	0.053	[3.29]***
MOM	-0.411	[-6.56]***
SIGMA	-8.049	[-5.81]***
ABVOL	0.003	[2.51]***
ROA	-0.130	[-1.85]*
ROA_STD	0.000	[5.79]***
LEV	-0.081	[-1.23]
SG	0.000	[-0.89]
OC	-0.009	[-0.62]
NUMRF	0.004	[4.90]***
Industry Dummies	Yes	
Year Dummies	Yes	
Obs.	30347	
R^2	0.0434	

8 Conclusion

In this study, we investigated the long-term effect of IT-related risk factor disclosures in 10-K filings. We documented that IT cybersecurity disclosures specifically have a significant relation with a firm's crash risk in the one-year window after the disclosure. This result supports but does not prove the notion that IT risk factors reflect the liability of a firm, which later materializes as an IT failure/issue that causes a severe stock price drop. Altogether, we provided supporting empirical evidence that risk disclosures are not boilerplate and contain relevant information about a firm's long-term performance. This study also advanced our understanding by separating IT-related risk into two categories – IT value risk and IT cybersecurity risk – and shows that the latter type of risk disclosure is associated with stock price crashes. We also make methodological contributions by providing a framework for conducting textual analysis on risk factors contained in 10K annual reports and by providing Java and Python source code to aid future researchers in extracting risk factors.

9 Bibliography

[1] M. Benaroch and A. Chernobai, "Operational IT Failures, IT Value Destruction, and Board-Level IT Governance Changes," *MIS Q.*, 2017.

[2] A. Masli, V. J. Richardson, M. Weidenmier Watson, and R. W. Zmud, "Senior Executives' IT Management Responsibilities: Serious IT-Related Deficiencies and CEO/CFO Turnover," *MIS Q.*, 2016.

[3] H. Cavusoglu, B. Mishra, and 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.*, vol. 9, no. 1, pp. 70–104, 2004.

[4] A. Bharadwaj, M. Keil, and M. Mähring, "Effects of information technology failures on the market value of firms," *J. Strateg. Inf. Syst.*, 2009.

[5] J. Goldstein, A. Chernobai, and M. Benaroch, "An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories," *J. Assoc. Inf. Syst.*, 2011.

[6] B. L. A. Gordon, R. H. Smith, and M. P. Loeb, "Market Value of Voluntary Disclosures Concerning Information Security," *MIS Q.*, vol. 34, no. 3, pp. 567–594, 2010.

[7] T. Wang, K. N. Kannan, J. R. Ulmer, T. Wang, K. N. Kannan, and J. R. Ulmer, "The Association Between the Disclosure and the Realization of Information Security Risk Factors," *Inf. Syst. Res.*, vol. 24, no. 2, pp. 201–218, 2012.

[8] S. C. Myers and L. Jin, "R-Squared Around the World: New Theory and New Tests," 2004.

[9] S. Dewan and F. Ren, "Risk and return of information technology initiatives: Evidence from electronic commerce announcements," *Inf. Syst. Res.*, 2007.

[10] K. Kannan, J. Rees, and S. Sridhar, "Market Reactions to Information Security Breach Announcements: An Empirical Analysis," *Int. J. Electron. Commer.*, vol. 12, no. 1, pp. 69–91,

2007.

[11] M. Benaroch, A. Chernobai, and J. Goldstein, “An internal control perspective on the market value consequences of IT operational risk events,” *Int. J. Account. Inf. Syst.*, 2012.

[12] D. Blei, M. Jordan, and A. Y. Ng, “Latent Dirichlet allocation,” *J. Mach. Learn. Res.*, vol. 3, pp. 993–1022, 2003.

[13] G. Page West and J. DeCastro, “The Achilles heel of firm strategy: Resource weaknesses and distinctive inadequacies,” *J. Manag. Stud.*, vol. 38, no. 3, pp. 417–442, 2001.

[14] J. Chen, H. Hong, and J. C. Stein, “Forecasting crashes: Trading volume, past returns, and conditional skewness in stock prices,” *J. financ. econ.*, 2001.

[15] A. P. Hutton, A. J. Marcus, and H. Tehranian, “Opaque Financial Reports , R-square , and Crash Risk,” *SSRN Electron. J.*, 2008.

[16] J. B. Kim, Y. Li, and L. Zhang, “Corporate tax avoidance and stock price crash risk: Firm-level analysis,” *J. financ. econ.*, 2011.

[17] J. B. Kim, Y. Li, and L. Zhang, “CFOs versus CEOs: Equity incentives and crashes,” *J. financ. econ.*, 2011.

[18] T. C. Powell and J.-L. Arregle, “Firm Performance and the Axis of Error,” *J. Manag. Res.*, vol. 7, no. 2, pp. 59–77, 2007.

[19] H. Cavusoglu, H. Cavusoglu, and S. Raghunathan, “Economics of ITSecurity Management: Four Improvements to Current Security Practices,” *CAIS*, vol. 14, p. 3, 2004.