The Impact of IT Investment and IT Security Intensity on Firm Performance

Completed paper

Abdulaziz Alharbi
University of Colorado Denver
abdulaziz.2.alharbi@ucdenver.edu

Dawn Gregg
University of Colorado Denver
dawn.gregg@ucdenver.edu

ABSTRACT

IT investments can generate value for businesses, but ignoring security risks can cause firms to lose value. This study investigates the impact of IT investment and IT security intensity on the financial performance of firms. Anchoring to prior research on firm performance, we employ the resource-based view (RBV) as the theoretical lens for this study. We conducted an OLS regression analysis on a cross-sectional dataset of 360 United States firms. The findings of this study indicate that IT investments and the strategic alignment of IT and security investments generate strategic business value, resulting in improved firm performance. However, IT security investments have a marginally negative impact on firm performance, suggesting that they may be viewed more as "insurance" to protect against security threats rather than strategic investments. The study suggests that IT security investments can generate short- and long-term business value for firms if they are viewed as strategic investments.

Keywords

IT investment, IT security intensity, firm performance, resource-based view (RBV), security investment.

INTRODUCTION

Investing in Information Technology (IT) is a critical component of modern organizations' digital business strategy (Mithas & Rust, 2016), and the business value of IT is receiving more consideration from Information Systems (IS) scholars (Devaraj & Kohli, 2003; McAfee & Brynjolfsson, 2008). Prior research indicates that IT investment creates value for business firms when synergistically entrenched in value creation (Kohli & Grover, 2008). IT projects are capital intensive. As a result, IT investment decisions become complex and multi-faceted, requiring justification before getting management approval and funding support (Xue et al., 2008). IT literature demonstrates that IT investment decisions are influenced by organizational factors (Law & Ngai, 2007). IT investment decisions can differ by business attributes like the firm type (Cobanoglu et al., 2013) and influence the firm financial performance.

In the current digital era, most business activities are enhanced by IT-enabled capabilities. Businesses are increasingly vulnerable to costly information security breaches (Bose & Luo, 2014). Due to the total integration of technology (such as big data, artificial intelligence, and the internet of things) into business, these information security breaches have a significant impact on enterprises (Berkman et al., 2018), and ignoring them will result in a significant loss of business value. Prior literature demonstrates that a firm's information security investments (e.g., firewalls, biometric authentication, intrusion detection system, etc.) reduce security breaches (Angst et al., 2017; Kwon & Johnson, 2014). Therefore, information security investments safeguard the business value and protect vital assets of organizations. However, the evidence on the relationship between information security investments and their impact on a firm's bottom line is scarce. As a result, there is a need to assess the business value of information security investments to understand their impact on organizations.

This study differs from prior research on IT investment and firm performance as it focuses on the relationship between information security investments and a firm's financial performance. Prior security literature recognized that firms vary in terms of their IT security motivation and intensity (Li et al., 2021; Kwon & Johnson, 2018). Most firms invest in IT in response to security breaches, which is proportional to the severity of the breach (Gordon & Loeb, 2002). However, this reactive approach is not effective enough to prevent security breaches (Kwon & Johnson, 2014). Security breaches are likely to take place if security is segregated from IT investment in the business planning process (Glavach, 2019). Integration of IT and security investments enables early identification of security risks, reduces mismanagement of security systems, builds effective technology infrastructure, enables better data management, and enhances security administration (Alkasasbeh, 2014; Spears & Barki, 2010). Prior research indicates that companies with effective IT resources are better prepared to deal with security threats (Chang & Lin, 2007; Hsu et al., 2012; Tu & Yuan, 2014). Integration of IT and security can advance the security planning process of an organization (Weixun et al., 2022). Security experts have also advocated for the alignment of the IT and security goals (Coltman et al., 2015; Rutherford, 2018). Therefore, we argue that a firm's IT security intensity would create a safe technology environment and improve the effectiveness of a firm's IT investments, which would lead to more firm profitability. Therefore, in this research, we examine: *How does IT security intensity and IT investments combine to impact the performance of a firm?*

To examine this question, we used a resource-based view (RBV) (Barney, 1991) to develop a synergistic framework for IT investment and IT security intensity. This is because RBV can help understand the links between the management of IT and security resources, their alignment, and the performance of the firm (Erkmen et al., 2020; Farrell, 2014; Fink & Neumann, 2009; Mao et

al., 2016; Weixun et al., 2022). We test our theoretical framework through an empirical analysis of a cross-sectional dataset of 360 United States firms.

The rest of the paper is organized as follows. Section 2 discusses the prior literature and theory related to this study. Section 3 is dedicated to the development of the hypotheses used in this study. Section 4 explains the methods used in this study. Section 5 presents the results of the research. Section 6 discusses the results of the research. Finally, section 7 concludes and presents the study's implications.

LITERATURE REVIEW

Information Security Investments

Existing literature suggests that information security is an essential consideration for firms' performance (Al-Sartawi & Razzaque, 2020; Bose & Luo, 2014; Juma'h, & Alnsour, 2020). Information security breaches can cause significant losses to firms (Al-Sartawi & Razzaque, 2020). Information security attacks have a detrimental effect on firm performance because they result in negative market reactions (ranging from 1% to 2.1%), reputational harm, lawsuits, and government sanctions (Georg, 2017). Accenture (2020) estimates that firms risk losing 5.2 trillion USD in value creation opportunities from the digital economy in the next 5 years due to cyber-attacks (Abbosh & Bissel, 2020)—negatively influencing the firm performance (Juma'h, & Alnsour, 2020).

Business processes, intellectual property, and customer data are valuable corporate assets in the digital economy (Ocean Tomo, 2015). These valuable assets are jeopardized by information security breaches, resulting in a loss of business value. Information security breaches impair the firm performance, and it takes companies time to recover from them (Jang-Jaccard & Nepal, 2014). Juma'h & Alnsour (2020) have found that information security breaches have a negative impact on the cumulative returns of publicly traded companies. Information security breaches pose a significant threat to financial markets, necessitating that organizations devote a substantial amount of time and resources to protect against security attacks and preserve business value (Pelley, 2019). In addition to financial consequences, information security breaches

also have non-financial repercussions (Brody et al., 2018). Information security attacks also threaten intangible assets such as corporate knowledge, data privacy, reputation, trust, and brand, in addition to tangible assets such as financial instruments (World Economic Forum, 2015). Consequently, industries, including healthcare, logistics, power generation, and transportation, consider information security investments vital to their survival and the protection of tangible and intangible assets (College of Healthcare Information Management Executives, 2018).

Gordon and Loeb (2002) point out that protecting information is very expensive. Nevertheless, firms should focus on information security assets and reduce vulnerabilities to safeguard business value (Juma'h, & Alnsour, 2020). The negative implications of security breaches on firm performance drive firms to enhance their IT security investments (D'Arcy et al., 2020). These IT security investments are essential to ensure the privacy and integrity of sensitive firm data and protect against loss of customer goodwill and financial penalties (Bose & Luo, 2014). Moreover, government regulations drive firms to invest in information security (Karanja & Zaveri, 2014). Thus, security breaches and government regulations drive organizations to invest in information security (Kwon & Johnson, 2014).

Resource-Based View

During the last three decades, the resource-based view (RBV) has been firmly established as a predominantly used theoretical lens to investigate firm performance (Alexy et al., 2017). Prior literature suggests that the RBV can help to understand the links between IT resource management and firm performance (Erkmen et al., 2020; Fink & Neumann, 2009; Mao et al., 2016). RBV can help to explain the effect of the alignment of IT and security investments on firm performance (Farrell, 2014; Weixun et al., 2022).

The RBV theory posits that a firm's strategic resources or capabilities ownership determine its superior performance or competitive advantage (Chen et al., 2021). A strategic resource or capability should be valuable enough to either reduce costs or augment value for customers, rare enough so that competitors cannot deploy the same resource to generate comparable value, and difficult to imitate or substitute, making it hard for rival firms to compete (Barney, 1991; Chen et al., 2021). These resources and capabilities include

a firm's management skills, organizational processes, routines, and the information and knowledge it controls (Barney et al., 2001). Firms that own more strategic resources show proportionately better performance over competitors (Chen et al., 2021) and create economic value (Alexy et al., 2017). According to Nevo & Wade (2011), IT resources are valuable, rare, and non-inimitable; therefore, according to RBV, they lead to strategic benefits for firms. RBV suggests that resources are heterogeneously dispersed over firms (Barney, 1991). The heterogeneous resources allow firms to pursue different strategies to maintain competitiveness (Desarbo et al., 2007).

Prior research on RBV and IT has focused on investments in Customer Relationship Management (CRM) (Mithas et al., 2012), digital business environments (Park & Mithas, 2020, strategic IT alignment (SITA) (Sabherwal et al., 2019), big data (Ghasemaghaei et al., (2021), etc. The impact of IT investments in CRM systems that facilitate customer access by communicating with the customer and contributing to the flow of revenues has been extensively studied using RBV (Mithas et al., 2012). Mithas et al. (2012) found that investing in IT resources contributes to increasing the firm's revenues by establishing new sales channels that improve customer management. Similar studies found that IT resources investments meet the customer's needs in customizing products and offers, leading to more significant customer response (Ansari & Mela, 2003) and enhanced one-to-one marketing efficacy (Mithas et al., 2006).

A study across education, health, manufacturing, and service sectors in the United States demonstrated the significance of RBV as a theoretical lens for assisting organizations in configuring their resources to achieve competitive advantage in complex digital environments (Park & Mithas, 2020). This study provided a reinterpretation of RBV by depicting firm resources as configurations of capabilities, as opposed to summative or multiplicative considerations of firm capabilities. A study by Sabherwal et al. (2019) shows the contribution of RBV in considering IT investment as a resource that SITA can help to leverage. In addition, the RBV-based study contends that environmental uncertainty (represented by complexity, dynamism, and munificence) complements the SITA effect on the relationship between IT investment and firm performance. The study results show that SITA directly affects firm performance and moderates the relationship between IT investment and firm performance. Ghasemaghaei (2021) used RBV to depict the

impact of big data characteristics (data volume, velocity, and variety) on firm performance as well as the complementary role of data value and veracity on these relationships. The study demonstrates that IT resources, such as big data, should be conceptually differentiated based on their characteristics to properly assess their impact on the firm's performance. The study underscores the value of RBV as a theoretical lens to examine the utility of big data as a vital IT resource to generate higher firm performance.

HYPOTHESES DEVELOPMENT

Information Technology Investments and Firm Performance

Prior research on the impact of investments in IT has found a positive relationship between these investments and firms' performance. As per Ilmudeen & Bao (2018), IT investments can generate business value with other business assets and improve firm performance. The business value of the IT paradigm highlights the fact that IT investments yield business value benefits (Tang et al., 2018) and competitive advantage (Saeidi et al., 2019). In addition to tangible financial benefits, IT investments generate intangible benefits, such as increased customer satisfaction and employee motivation, among others (Schniederjans et al., 2004). Liu et al. (2008) and Gupta et al. (2018) suggest that certain IT investments (e.g., computers) may have a direct impact on firm performance, while others may have an indirect impact. Prior research suggests that the benefits of IT investment for firm performance could be manifested in several forms, e.g., increasing market value (Chen et al., 2017; Morimura et al., 2018), higher profitability (Kim et al., 2018), cost reduction (Abdurrahman et al., 2018), higher customer satisfaction (DeGroote & Marx, 2013), etc. Further, IT investments could support businesses in superior decision-making (Loukis, 2019), information dissemination (Oh et al., 2012), resource integration (Oh et al., 2012), administration, and corporate governance (Ilmudeen & Bao, 2018).

RBV research shows a link between investment in IT resources and firm competitive advantage (Fink & Neumann, 2009). Mithas et al. (2012) found that investing in CRM systems contributes to increasing the firm's revenues. Park & Mithas (2020) found that firm investments in resource configurations lead to superior firm performance in complex digital environments. Sabherwal et al. (2019) study showed that SITA improves firm performance and moderates the relationship between IT investment and firm

performance. Ghasemaghaei (2021) study reported that investment in IT resources (such as big data) leads to higher firm performance. Shekarian & Ramirez (2021) found that the intensity of IT and managerial experience increased the firm's revenue during the COVID-19 crisis.

These examples show the strength and importance of investing in IT and how firms can develop their resources and capabilities that lead to better firm performance. Therefore, we hypothesize:

Hypothesis 1*. A higher level of IT investment is associated with an increase in firm performance.*

IT Security Intensity and Firm Performance

Information security breaches have financial (Pelley, 2019) and non-financial (Brody et al., 2018) implications. Information security breaches threaten firms' tangible and intangible assets (College of Healthcare Information Management Executives, 2018). Information security breaches can cause both short-term economic shocks (e.g., a temporary decrease in market value) and long-term business value erosion (Furnell et al., 2020). Since security breaches cause significant financial harm to businesses, firms invest in security to protect against security threats and safeguard business value (Bohme & Moore, 2010). Information security investments can reduce the likelihood of security breaches (Srinidhi et al., 2015). Investing in information security safeguards the privacy and integrity of a company's sensitive data and protects against the loss of customer goodwill and the threat of monetary penalties (Bose & Luo, 2014). Therefore, security investments can safeguard firms' vital information and financial assets (Kwon & Johnson, 2014). The study by Bose & Luo (2014) expects the various kinds of firm security investments (such as network security, platform security, application security, mass storage security, file, and data security, etc.) to have a positive effect on firm performance.

IT security resources are expected to be the source of competitive advantage and firm performance in the current digital era. RBV suggests that firms with greater IT security resources will improve their security capabilities and display an increase in firm performance (Kwon & Johnson, 2014). Accordingly, we hypothesize:

Hypothesis 2*. A higher level of IT security intensity is associated with an increase in firm performance*

Moderation Effect of Security Intensity

Prior research suggests that firms could face security issues if security planning is segregated from the IT planning process (Doherty & Fulford, 2006; Glavach, 2019). IT practices of a firm could affect its security investments (Angst et al., 2017). IT investments should be strategically guided to control workflow and prevent misuse of IS (Spears & Barki, 2010). Security experts suggest alignment of IT and security objectives (Rutherford, 2018). Due to this, recent information system research recommends that IT and security investments should be integrated to obtain better firm performance (Weixun et al., 2022).

According to Nevo & Wade (2011), IT resources are considered valuable, rare, and non-inimitable. IT security investments are non-substitutable as they are essential to safeguard vital information assets and prevent costly security breaches (Kwon & Johnson, 2014). Alignment of IT and security investments can lead to higher firm performance, leading to valuable, rare, inimitable, and non-substitutable advantages (Farrell, 2014; Weixun et al., 2022). Investments in security safeguard the business value of IT by identifying and reducing various security threats (Pelley, 2019), which reduces business risks and can lead to superior firm results (Ilmudeen & Bao, 2020). Security integration with IT reduces firm risk when implementing new IT solutions and making IT investments (Spears & Barki, 2010). Integrating security with IT can reduce information system abuse and increase security compliance behavior, which is essential for protecting enterprise value (Spears & Barki, 2010). Strategic security investments elevate the business value of a firm's IT investments (Fazlida & Said, 2015), which can lead to superior firm performance.

The preceding discussion indicates the value of aligning IT and security investments for superior firm performance. The discussion also indicates that the security investments can complement a firm’s IT investments for superior firm performance. Accordingly, we formulate the following hypothesis:

Hypothesis 3*. The security intensity interacts IT investment to positively impact firm performance.*

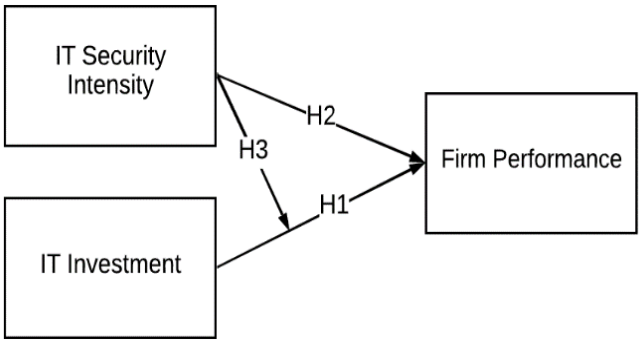

Figure 1. Research model

METHODS

Data

The study use data from two sources: The technology data from the Computer Intelligence Technology database (CITDB) and the financial data from Compustat. Both CITDB and Compustat are considered reliable sources of information, and previous studies have also been used in different business fields (e.g., Johnston & Zhang, 2018; Xue et al., 2021). The data used in this research include information about firms' IT investment and security intensity during the 2017 period. We complemented the CITDB data with firm performance (Profitability) and other industry data from Compustat during the 2018 period.

Variables

Table 1 summarizes the variables and data, including definitions of the variables, measurements, and sources used in this study. The dependent variables for this study are profitability. Profitability is the extent to which a firm achieves profit or financial returns. We measured profitability by calculating the income ratio before depreciation on firm sales (Mithas & Rust, 2016). We define IT security intensity as the number of IT security systems used by a firm, such as a cloud computing, anti-virus software, data encryption, monitoring software, and cyber security software. We gauge a firm's information security investments through its IT security intensity. We expect the IT security intensity to positively influence the firm performance in line with Bose & Luo (2014).

The study aims to reveal the main and complementary effects of IT investment and security intensity on profitability. Therefore, our independent variables are the IT investment and security intensity. IT

investment is the total IT budget, including hardware, software, PC, server, storage, terminal, and communication services. We measured IT investment by aggregate IT investments as a percent of revenues. The security intensity is the total number of security-related products implemented by the firm. This includes cloud computing and other security software, including anti-virus software, data encryption, monitoring software, and cyber security software. We measured the security intensity by the total number of security software and cloud computing divided by the natural log of employees.

We also consider other control variables. Firm performance can be influenced by these contextual variables rather than those at the base of this study. First, we control for Asset Intangibility measured as the total of intangible assets divided by net sales. Second, Capital Intensity is the ratio of capital expenditures divided by total assets. Third, Firm Size is measured as the natural log of the firm's market value. Finally, the cost of goods sold (COGS) has been measured as the ratio of the cost of goods sold to sales.

Variable	Definition	Measurement	Source
Firm Performance	Operating income before depreciation divided by sales (expressed in percentage)	The ratio of income before depreciation on sales	Compustat
IT Investment	The total IT budget includes hardware, software, PC, server, storage, terminal, and communication services.	Aggregate IT investments as a percent of revenues	CITBD
IT Security Intensity	Total of cloud computing and the IT security software includes anti-virus software, data encryption, monitoring software, and cyber security software.	The total number of security software and cloud computing divided by the Natural log of employees	CITBD
Asset Intangibility	Intangible assets over sales	Sum of intangible assets divided by net sales.	Compustat
Capital Intensity	Funds used by a firm to acquire physical assets, scaled by assets.	The ratio of capital expenditures divided by total assets.	Compustat
Firm Size	The market value of a firm.	Natural log of the firm's market value.	Compustat
COGS	The direct costs associated with producing goods.	The ratio of cost of goods sold to sales	Compustat

Table 1. Description of variables

Estimation equation

We use the following cross-sectional models:

$$Y_i = X_i\beta + \varepsilon_i \qquad (1)$$

Where Y represents dependent variables which is Profitability; X represents a vector of firm features, such as IT investment, security intensity, and control variables, β is a parameter vector to be estimated; and ε is the error term associated with each observation i.

We used ordinary least squares (OLS) to estimate equations the explanatory variables (IT investment and security intensity) are considered external in terms of the econometric model (Wooldridge, 2022). We conducted two diagnostic tests to ensure the strength of our results. First, we check multicollinearity by calculating the variance inflation factor (VIF). The highest mean VIF for our model was less than 2.0. Thus, our models indicate the absence of multicollinearity concerns (Gómez et al., 2016; Thompson et al., 2017; Kutner et al., 2005). The second diagnostic test examines heteroscedasticity using White's and the Breusch-Pagan tests (Fox, 2020). These tests can not reject the null hypothesis of constant variance, indicating the absence of heteroscedasticity.

Results

Table 2 demonstrates the descriptive statistics and correlations between variables. As we expected, the IT investment shows a significant positive correlation with profit. It is observed that the security intensity has a positive correlation with profit.

Table 3 shows the Ordinary Least Squares (OLS) results for the sample of 360 firms. The direct and the indirect models are used to test our exogenous variables on profit. As hypothesized in H1, there is a significant and positive relationship between IT Investment and profitability (Table 3, column 1, $\beta = 0.180$ $p<0.01$). Therefore, the higher the level of IT investment within a firm, the higher will be its performance. Thus, **H1 is supported.**

Variables	Mean	SD	Min	Max	1	2	3	4	5	6	7	8
Profit	0.20	0.13	-0.03	0.64	1							
IT Investment	0.09	0.14	0.00	2.22	0.22	1						
Security Intensity	175.65	471.01	0.25	4115.92	0.01	0.05	1					
Asset Intangibility	0.53	0.59	0	2.89	0.35	0.16	-0.01	1				
Capital Intensity	0.03	0.02	0	0.17	0.04	-0.12	-0.01	-0.31	1			
Firm Size	9.07	1.78	0.78	13.57	0.38	-0.18	0.33	0.14	0.03	1		
COGS	0.56	0.22	0	0.97	-0.63	-0.18	0.06	-0.37	0.10	-0.18	0.03	1

Table 2. Descriptive Statistics and Correlation Matrix (n= 360)

Variables	(1) Direct	(2) Indirect
DV: Profit		
IT Investment	**0.18*** (0.03)**	0.16*** (0.03)
Security Intensity	**-0.01* (0.01)**	-0.01*** (0.01)
IT Investment× Security Intensity		**0.01* (0.01)**
Asset Intangibility	0.03*** (0.01)	0.03*** (0.01)
Capital Intensity	0.68*** (0.17)	0.67*** (0.17)
Firm Size	0.02*** (0.01)	0.02*** (0.01)
COGS	-0.30*** (0.02)	-0.30*** (0.02)
Constant	0.10*** (0.03)	0.10*** (0.03)
Observations	360	360
R-squared	0.54	0.55

Table 3. Direct and Interaction Effects

Next, we examine the impact of security intensity on the performance of the firm. We found a significant but negative relationship between security intensity and profit (Table 3, column 1, β= -0.01, $p<0.1$). Therefore, the higher the level of firm security intensity, the lower its performance will be. Thus, **H2 is not supported.**

Additionally, as hypothesized in H3, security intensity is significant and positively interacts with the relationship between IT investment and firm's profitability (Table 3, column 2, β= 0.01, $p<0.1$). Therefore, security intensity complements IT investment for a positive performance impact. Thus, **H3 is supported.**

DISCUSSION

Ordinary least squares (OLS) results provide support for the first hypothesis, which states that IT investment positively impacts firm performance. This is in line with the prior research, which states that investing in IT contributes to firm revenues. Based on assertions of RBV (Barney, 1991; Erkmen et al., 2020; Fink & Neumann, 2009; Mao et al., 2016), we can state that IT investments create strategic benefits for firms leading to an increase in firm performance.

OLS results also show support for our third hypothesis, which states that IT security intensity positively moderates the relationship between IT investment and firm performance. This indicates that IT security intensity is a crucial component of technological capability. Moreover, these two inputs combine to positively impact firm performance. This demonstrates that aligning IT and security investments allows businesses to better manage their security systems, build effective security infrastructure, improve data management, and enhance security administration. Therefore, such technology capabilities can result in enhanced firms' performance. This aligns with prior research on the role of IT and security capabilities in organizations (Alkasasbeh, 2014; Coltman et al., 2015; Rutherford, 2018; Weixun et al., 2022; Spears & Barki, 2010). Based on assertions of RBV (Farrell, 2014; Weixun et al., 2022), we can argue that alignment of IT and security investments create strategic advantages for organizations, resulting in enhanced firm performance.

OLS results do not support our second hypothesis. The results show that the relationship between IT security intensity and firm performance is marginally negative, indicating firms having higher IT security intensity have relatively lower profitability. This result is contrary to our expectations and prior research (Bose & Luo, 2014). So, the question arises why IT security intensity marginally reduces the firm performance? We believe that it could be because IT security investments may not be considered as strategic investments, unlike other IT investments. Rather the firms consider security investments as insurance investments to protect against costly cyberattacks. This indicates that firms invest in IT security to protect against data breaches, loss of sensitive customer data, and damage to their market reputation; however, IT security investments may not be integrated into the strategic value creation process of organizations. In addition, IT security intensity cannot ensure that employees and organizations will actually use the implemented security technology. Also, security intensity cannot guarantee that organizations will actually spend the IT budget on security related infrastructures. This suggests that additional research is needed to better assess the strategic value of IT security investments to firms.

CONCLUSION, IMPLICATIONS, AND LIMITATIONS

Researchers have become increasingly cognizant of the business value of IT investments over time. The potential for organizations to face costly security threats has increased the importance of protecting against security threats to safeguard the business value of IT. It is possible to state that security investments safeguard the business value of IT and protect organizations' essential assets. This study sheds light on the strategic nature of IT and security investments in organizational performance. The study results show that investing in IT create strategic benefits for firms, which positively influences firm performance. Moreover, results suggest that a strategic alignment between IT and security investments is critical. Because such alignment can enable firms to identify security risks early and enhance their ability to manage and prevent security breaches through better management of security systems, effective technology infrastructure, superior data management, and enhanced security administration. IT-security alignment can deter security breaches and enhance the business value of IT. This then can lead to positive firm performance. The study

also suggests that unlike IT investments, IT security intensity, do not directly impact profits. Rather, they could be viewed as "insurance" by firms to protect against costly cyber-breach, which could cause long-term harms to future profitability. The implication is that businesses may not be incorporating IT security intensity into their overall strategic value creation procedures. IT security intensity can't guarantee that organizations will use security technology and spend IT budget on developing strategic security infrastructures.

The study has practical as well as theoretical implications. The study suggests that like IT investments, IT security investments can create short- and long-term business value for organizations if they are considered strategic investments. In addition, the study contributes to the literature on strategic management (Erkmen et al., 2020; Weixun et al., 2022; Farrell, 2014; Mao et al., 2016; Fink & Neumann, 2009) by demonstrating that RBV is an appropriate framework understanding how aligning IT and security investments provides firm performance.

Our research has a few limitations. First, this study employs a cross-sectional analysis, and although we have conducted multiple analyses, the analysis can still be improved. Associational longitudinal studies with multiple years of panel data would assist in validating our findings, thereby increasing their generalizability and allowing for stronger causal claims. Second, we utilized one of the numerous possible firm performance measures. Future research should employ a more inclusive methodology for evaluating the impact of IT investments and security intensity on firm performance. Thirdly, the information security intensity variable was measured in terms of the number of security software used by businesses, which is the only information available regarding information security. Future research may determine the level of information security using variables other than cloud computing, anti-virus software, data encryption, monitoring software, and cyber security software.

This research contributes to IS research about the critical role of IT-security alignment paradigms in relation to firm performance. Future research can shed additional light on the factors influencing IT-security alignment and their effect on firm performance. In addition, future research can identify the specific types

of IT and security investments and their effects on firm performance. It would be beneficial to conduct research with a larger dataset that also includes private companies.

REFERENCES

Abbosh, O., & Bissel, K. (2020). Reinventing the Internet to Secure the Digital Economy. Retrieved March 26, 2022, from https://www.accenture.com/sa-en/insights/cybersecurity/reinventing-the-internet-digital-economy

Abdurrahman, L., Langi, A. Z., Suhardi, & Simatupang, T. M. (2018). Information Technology Value Engineering Model and Cost Efficiency in IT-Based Firms. *IEEE Systems Journal, 12*(3), 2925–2936. https://doi.org/10.1109/jsyst.2017.2663418

Alexy, O., West, J., Klapper, H., & Reitzig, M. (2017). Surrendering control to gain advantage: Reconciling openness and the resource-based view of the firm. Strategic Management Journal, 39(6), 1704–1727. https://doi.org/10.1002/smj.2706

Alkasasbeh, A. A. (2014). The Effect of Information Technology Capabilities in Implementing Information Security Management Systems. European Scientific Journal, 10(18), 377–385. https://eujournal.org/index.php/esj/article/view/3606

Al-Sartawi, A. M., & Razzaque, A. (2020). Cyber Security, IT Governance, and Performance: A Review of the Current Literature. In Albastaki, Y. A., & Awad, W. (Ed.), Implementing Computational Intelligence Techniques for Security Systems Design (pp. 275-288). IGI Global. https://doi.org/10.4018/978-1-7998-2418-3.ch014

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. MIS Quarterly, 41(3), 893–916. https://doi.org/10.25300/misq/2017/41.3.10

Ansari, A., & Mela, C. F. (2003). E-Customization. Journal of Marketing Research, 40(2), 131–145. https://doi.org/10.1509/jmkr.40.2.131.19224

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. Journal of Management, 17(1), 99–120. https://doi.org/10.1177/014920639101700108

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. Journal of Accounting and Public Policy, 37(6), 508-526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Bohme, R., & Moore, T. (2010). The iterated weakest link. *IEEE Security & Privacy Magazine, 8*(1), 53–55. https://doi.org/10.1109/msp.2010.51

Bose, R., & Luo, X. R. (2014). Investigating security investment impact on firm performance. International Journal of Accounting & Information Management, 22(3), 194–208. https://doi.org/10.1108/IJAIM-04-2014-0026

Brody, R. G., Chang, H. U., & Schoenberg, E. S. (2018). Malware at its worst: death and destruction. International Journal of Accounting & Information Management, 26(4), 527–540. https://doi.org/10.1108/ijaim-04-2018-0046

Chang, S. E., & Lin, C. (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438–458. https://doi.org/10.1108/02635570710734316

Chen, M. J., Michel, J. G., & Lin, W. (2021). Worlds Apart? Connecting Competitive Dynamics and the Resource-Based View of the Firm. Academy of Management Proceedings, 2021(1), 11635. https://doi.org/10.5465/ambpp.2021.11635abstract

Chen, Y., Wang, Y., Nevo, S., Benitez, J., & Kou, G. (2017). Improving Strategic Flexibility with Information Technologies: Insights for Firm Performance in an Emerging Economy. Journal of Information Technology, 32(1), 10–25. https://doi.org/10.1057/jit.2015.26

Cobanoglu, C., Ayoun, B., Connolly, D., & Nusair, K. (2013). The Effect of Information Technology Steering Committees on Perceived IT Management Sophistication in Hotels. International Journal of Hospitality & Tourism Administration, 14(1), 1-22. https://doi.org/10.1080/15256480.2013.753801

College of Healthcare Information Management Executives (2018). Healthcare's Most Wired 2018. Ann Arbor: CHIME.

Coltman, T., Tallon, P., Sharma, R., & Queiroz, M. (2015). Strategic IT Alignment: Twenty-Five Years on. Journal of Information Technology, 30(2), 91–100. https://doi.org/10.1057/jit.2014.35

D'Arcy, J., Adjerid, I., Angst, C. M., & Glavas, A. (2020). Too Good to Be True: Firm Social Performance and the Risk of Data Breach. Information Systems Research, 31(4), 1200–1223. https://doi.org/10.1287/isre.2020.0939

DeGroote, S. E., & Marx, T. G. (2013). The impact of IT on supply chain agility and firm performance: An empirical investigation. *International Journal of Information Management, 33*(6), 909–916. https://doi.org/10.1016/j.ijinfomgt.2013.09.001

DeSarbo, Wayne S., C. Anthony Di Benedetto, and Michael Song. "A heterogeneous resource based view for exploring relationships between firm performance and capabilities." Journal of modelling in management (2007).

Devaraj, S., & Kohli, R. (2003). Performance Impacts of Information Technology: Is Actual Usage the Missing Link? Management Science, 49(3), 273-289. https://doi.org/10.1287/mnsc.49.3.273.12736\

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. Computers & Security, 25(1), 55–63. https://doi.org/10.1016/j.cose.2005.09.009

Erkmen, T., Günsel, A., & Altındağ, E. (2020). The Role of Innovative Climate in the Relationship between Sustainable IT Capability and Firm Performance. Sustainability, 12(10), 4058. https://doi.org/10.3390/su12104058

Farrell, T. (2014, May). The Effects of Port Security Compliance on the Competitiveness of United States and European Union Ports and Maritime Industry Terminal Firms. Texas A&M University. https://oaktrust.library.tamu.edu/bitstream/handle/1969.1/157621/FARRELL-DOCUMENT-2014.pdf?sequence=1

Fazlida, M., & Said, J. (2015, April). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, 243–248. https://doi.org/10.1016/s2212-5671(15)01106-5

Fink, L., & Neumann, S. (2009). Exploring the perceived business value of the flexibility enabled by information technology infrastructure. Information & Management, 46(2), 90–99. https://doi.org/10.1016/j.im.2008.11.007

Fox, J. (2020). Regression Diagnostics: An Introduction (Quantitative Applications in the Social Sciences) (2nd ed.). SAGE Publications, Inc.

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. Computer Fraud & Security, 2020(12), 6–12. https://doi.org/10.1016/s1361-3723(20)30127-5

Georg, L. (2017). Information security governance: Pending legal responsibilities of non-executive boards. Journal of Management & Governance, 21(4), 793-814. https://doi.org/10.1007/s10997-016-9358-0

Ghasemaghaei, M. (2021). Understanding the impact of big data on firm performance: The necessity of conceptually differentiating among big data characteristics. International Journal of Information Management, 57(1). https://doi.org/10.1016/j.ijinfomgt.2019.102055

Glavach, D. (2019, January 22). In IT Ops, separate security teams should be a thing of the past. TechBeacon. Retrieved April 12, 2022, from https://techbeacon.com/enterprise-it/it-ops-separate-security-teams-should-be-thing-past

Gómez, R. S., Pérez, J. G., Martín, M. D. M. L., & García, C. G. (2016). Collinearity diagnostic applied in ridge estimation through the variance inflation factor. Journal of Applied Statistics, 43(10), 1831–1849. https://doi.org/10.1080/02664763.2015.1120712

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457. https://doi.org/10.1145/581271.581274

Gupta, S. D., Raychaudhuri, A., & Haldar, S. K. (2018). Information technology and profitability: evidence from Indian banking sector. *International Journal of Emerging Markets, 13*(5), 1070–1087. https://doi.org/10.1108/ijoem-06-2017-0211

Hsu, C., Lee, J. N., & Straub, D. W. (2012). Institutional Influences on Information Systems Security Innovations. Information Systems Research, 23(3-part-2), 918–939. https://doi.org/10.1287/isre.1110.0393

Ilmudeen, A., & Bao, Y. (2018). Mediating role of managing information technology and its impact on firm performance. *Industrial Management & Data Systems, 118*(4), 912–929. https://doi.org/10.1108/imds-06-2017-0252

Ilmudeen, A., & Bao, Y. (2020). IT strategy and business strategy mediate the effect of managing IT on firm performance: empirical analysis. *Journal of Enterprise Information Management, 33*(6), 1357–1378. https://doi.org/10.1108/jeim-03-2019-0068

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

Johnston, J. A., & Zhang, J. H. (2018). Information Technology Investment and the Timeliness of Financial Reports. Journal of Emerging Technologies in Accounting, 15(1), 77–101. https://doi.org/10.2308/jeta-52066

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. International Journal of Accounting & Information Management, 28(2), 275-301. https://doi.org/10.1108/ijaim-01-2019-0006

Karanja, E., & Zaveri, J. (2014). Ramifications of the Sarbanes Oxley (SOX) Act on IT governance. International Journal of Accounting and Information Management, 22(2), 134–145. https://doi.org/10.1108/ijaim-02-2013-0017

Kim, T. H., Wimble, M., & Sambamurthy, V. (2018). Disaggregation of the IT capital effects on firm performance: Empirical evidence from an IT asset portfolio perspective. *European Journal of Information Systems, 27*(4), 449–469. https://doi.org/10.1057/s41303-017-0062-1

Kohli, R., & Grover, V. (2008). Business Value of IT: An Essay on Expanding Research Directions to Keep up with the Times. Journal of the Association for Information Systems, 9(1), 23-39. https://doi.org/10.17705/1jais.00147

Kutner, M. H., Nachtsheim, C. J., Neter, J., & Li, W. (2005). Applied Linear Statistical Models (Vol. 5). McGraw-Hill Irwin Boston.

Kwon, J., & Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. MIS Quarterly, 38(2), 451–471. https://doi.org/10.25300/misq/2014/38.2.06

Kwon, J., & Johnson, M. E. (2018). Meaningful healthcare security: Does meaningful-use attestation improve information security performance? MIS Quarterly, 42(4), 1043–1067. https://misq.umn.edu/meaningful-healthcare-security-does-meaningful-use-attestation-improve-information-security-performance.html

Law, C., & Ngai, E. (2007). IT Infrastructure Capabilities and Business Process Improvements. Information Resources Management Journal, 20(4), 25-47. https://doi.org/10.4018/irmj.2007100103

Li, H., Yoo, S., & Kettinger, W. J. (2021). The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches. Journal of Management Information Systems, 38(1), 222–245. https://doi.org/10.1080/07421222.2021.1870390

Liu, Y., Lu, H., & Hu, J. (2008). IT capability as moderator between IT investment and firm performance. *Tsinghua Science and Technology, 13*(3), 329–336. https://doi.org/10.1016/s1007-0214(08)70053-1

Loukis, E., Janssen, M., & Mintchev, I. (2019). Determinants of software-as-a-service benefits and impact on firm performance. *Decision Support Systems, 117*, 38–47. https://doi.org/10.1016/j.dss.2018.12.005

Mao, H., Liu, S., Zhang, J., & Deng, Z. (2016). Information technology resource, knowledge management capability, and competitive advantage: The moderating role of resource commitment. International Journal of Information Management, 36(6), 1062–1074. https://doi.org/10.1016/j.ijinfomgt.2016.07.001

McAfee, A., & Brynjolfsson, E. (2008). Investing in the IT That Makes a Competitive Difference. Harvard Business Review, 86(7-8), 98-107.

Mithas, S., & Rust, R. T. (2016). How Information Technology Strategy and Investments Influence Firm Performance: Conjecture and Empirical Evidence. MIS Quarterly, 40(1), 223-245. https://doi.org/10.25300/misq/2016/40.1.10

Mithas, S., Almirall, D., & Krishnan, M. S. (2006). Do CRM Systems Cause One-to-One Marketing Effectiveness? Statistical Science, 21(2). https://doi.org/10.1214/088342306000000213

Mithas, S., Tafti, A., Bardhan, I., & Goh, M. (2012). Information Technology and Firm Profitability: Mechanisms and Empirical Evidence. MIS Quarterly, 36(1), 205. https://doi.org/10.2307/41410414

Morimura, F., & Sakagawa, Y. (2018). Information technology use in retail chains: Impact on the standardisation of pricing and promotion strategies and performance. *Journal of Retailing and Consumer Services*, 45, 81–91. https://doi.org/10.1016/j.jretconser.2018.08.009

Nevo, S., & Wade, M. (2011). Firm-level benefits of IT-enabled resources: A conceptual extension and an empirical assessment. The Journal of Strategic Information Systems, 20(4), 403-418. https://doi.org/10.1016/j.jsis.2011.08.001

Ocean Tomo (2015). Intangible Asset Market Value Study. Chicago: Ocean Tomo

Oh, L. B., Teo, H. H., & Sambamurthy, V. (2012). The effects of retail channel integration through the use of information technologies on firm performance. *Journal of Operations Management, 30*(5), 368–381. https://doi.org/10.1016/j.jom.2012.03.001

Park, Y., & Mithas, S. (2020). Organized Complexity of Digital Business Strategy: A Configurational Perspective. MIS Quarterly, 44(1), 85–127. https://doi.org/10.25300/misq/2020/14477

Pelley, S. (2019, March 10). Federal Reserve Chairman Jerome Powell: The 60 Minutes interview. Retrieved April 14, 2022, from https://www.cbsnews.com/news/jerome-powell-federal-reserve-chairman-60-minutes-interview-2019-03-10/

Rutherford, R. (2018, May 24). Diversifying IT investment: It's not just cyber-security. Information Age. Retrieved May 3, 2022, from https://www.information-age.com/diversifying-it-investment-its-not-just-cyber-security-123472073/

Sabherwal, R., Sabherwal, S., Havaknor, T., & Steelman, Z. (2019). How Does Strategic Alignment Affect Firm Performance? The Roles of Information Technology Investment and Environmental Uncertainty. MIS Quarterly, 43(2), 453–474. https://doi.org/10.25300/misq/2019/13626

Saeidi, P., Saeidi, S. P., Sofian, S., Saeidi, S. P., Nilashi, M., & Mardani, A. (2019). The impact of enterprise risk management on competitive advantage by moderating role of information technology. *Computer Standards & Interfaces*, *63*, 67–82. https://doi.org/10.1016/j.csi.2018.11.009

Schniederjans, M. J., Hamaker, J. H., & Schniederjans, A. M. (2004). Information Technology Investment - Decision-Making Methodology. *World Scientific Publishing Co. Re. Ltd.* https://doi.org/10.1142/5424

Shekarian, N., & Ramirez, R. (2021). Resilience through Technology Intensity and International Related Management Experience: An Explorative Examination of European Firms during the COVID-19 Crisis. DIGIT 2021 Proceedings, 4.

Spears, & Barki. (2010). User Participation in Information Systems Security Risk Management. MIS Quarterly, 34(3), 503. https://doi.org/10.2307/25750689

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. Decision Support Systems, 75(1), 49–62. https://doi.org/10.1016/j.dss.2015.04.011

Tang, C. P., Huang, T. C. K., & Wang, S. T. (2018). The impact of Internet of things implementation on firm performance. *Telematics and Informatics, 35*(7), 2038–2053. https://doi.org/10.1016/j.tele.2018.07.007

Thompson, C. G., Kim, R. S., Aloe, A. M., & Becker, B. J. (2017). Extracting the Variance Inflation Factor and Other Multicollinearity Diagnostics from Typical Regression Results. Basic and Applied Social Psychology, 39(2), 81–90. https://doi.org/10.1080/01973533.2016.1277529

Tu, Z., & Yuan, Y. (2014). Critical Success Factors Analysis on Effective Information Security Management: A Literature Review. Americas Conference on Information Systems, Savannah, Georgia, USA.

Weixun, L. I., LEUNG, A. C. M., & YUE, W. T. (2022). Where is IT in Information Security? The Interrelationship among IT Investment, Security Awareness, and Data Breaches. MIS Quarterly.

Wooldridge, J. (2022). Introductory Econometrics: A Modern Approach (5th ed.). Cengage Learning.

World Economic Forum (2015). Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats Threats. Davos: World Economic Forum.

Xue, L., Mithas, S., & Ray, G. (2021). Commitment to IT Investment Plans: The Interplay of Real Earnings, Management, IT Decentralization, and Corporate Governance. MIS Quarterly, 45(1), 193–224. https://doi.org/10.25300/misq/2021/14970

Xue, Y., Liang, H., & Boulton, W. (2008). Information Technology Governance in Information Technology Investment Decision Processes: The Impact of Investment Characteristics, External Environment, and Internal Context. MIS Quarterly, 32(1), 67-96. https://doi.org/10.2307/25148829