European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2020.12.05.54

IEBMC 2019
9th International Economics and Business Management Conference

SOCIO-ECONOMIC FACTORS ON SECTOR-WIDE SYSTEMATIC RISK OF INFORMATION SECURITY BREACHES: CONCEPTUAL FRAMEWORK

Syed Emad Azhar Ali (a)*, Fong-Woon Lai (b), Rohail Hassan (c)
*Corresponding author

(a) Department of Management & Humanities, Universiti Teknologi PETRONAS, 32610 Seri Iskandar, Perak Darul Ridzuan, Malaysia, syed_17007896@utp.edu.my
(b) Department of Management & Humanities, Universiti Teknologi PETRONAS, 32610 Seri Iskandar, Perak Darul Ridzuan, Malaysia, laifongwoon@utp.edu.my
(c) Othman Yeop Abdullah Graduate School of Business (OYAGSB), Universiti Utara Malaysia, 06010 UUM Sintok, Kedah Darul Aman, Malaysia. rohail.hassa39@gmail.com

Abstract

This paper aims to propose a conceptual framework for investigating the impact of Socio-economic Breach Contingency Factors (BCFs) on banking sector's systematic risk. The study adopts an event study methodology comprising 200 global incidents of Information Security (IS) breaches occurring in listed banks. The Socio-economic BCFs will be proxied by (1) Cyber Crime Fear in a Country and (2) Information & Communication Technology (ICT) Penetration in a Country. The proposed framework aims to validate the nexus of socio-economic factors and systematic risk through which shareholders and bank managers can assess the risk of possible market value losses at the incident of IS breach in the banking sector. Considering the scenario of IS breach, this paper will make a significant contribution to the theory of efficient market hypothesis by way of extension and integration of theories. EMH under the context of IS breach has been limited by the BCFs of attack type, firm type, and industry type.

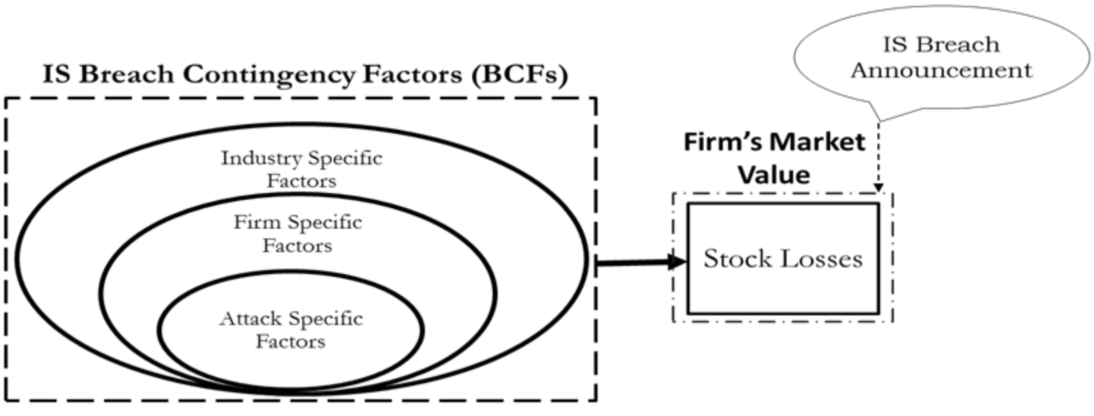
Keywords: Breach contingency factors, systematic risk, banking sector, market value, cyber crime fear, and ICT penetration.

https://doi.org/10.15405/epsbs.2020.12.05.54
Corresponding Author: Syed Emad Azhar Ali
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Cybercrime today is a global risk, as it costs the global economy and business more than $500 billion annually (McAfee, 2018). Apart from the tangible financial losses suffered by business, incidents of cybercrime or IS breaches can also harm the firm's reputation and brand value. Therefore, various studies have examined the impact of IS breaches on the market value (MV) of the breached firms. Most of them concluded a negative impact on stock prices, especially when the breached firm is from the banking sector. In view of, the contagion effect especially within the banking sector, very few studies have examined the impact of IS breach announcements by a bank on the Banking Sectors' Systematic Risk (β_(Banking Sector)) and especially the role of socio-economic breach contingency factors (BCFs) in explaining a change in systematic risk.

With the evolution of Internet of Things (IoT) and Industrial Revolution (IR4.0), there are many, who rejoices the progressively connected world, but others have shown serious concerns with the enormous risks linked with all that virtual data, an ideal target for cybercrime. According to Global Risks Perception Report (GRPR) by the World Economic Forum (WEF) (2018), incidents of IS breach in the form of cyber-attacks are among the most prominent threats globally. Global Losses from IS breach incidents have taken a high rise from $445 billion to $600 billion during 2014-2018 (McAfee, 2018). The pain from these incidents is most frequently felt by the financial sector with tangible losses (labor, material, and services) ranges from $2.8 million to $6 million on each breach (Ponemon Institute, 2018). While intangible costs are difficult to estimate, such as loss of trust, reputation, and confidence by business stakeholders for future transactions. Underpinned by the Efficient Market Hypothesis in its semi-strong form (Fama, 1991; Fama et al., 1969; Malkiel & Fama, 1970) researches have tried to examine the impact of IS breach announcements on stock prices for effected firms (Berkman et al., 2018; Bianchi & Tosun, 2018; Campbell et al., 2003; Cavusoglu et al., 2004; Ettredge & Richardson, 2001; Hovav & D'Arcy, 2004; Kannan et al., 2007; Malhotra & Kubowicz Malhotra, 2011; Pirounias et al., 2014; Sangvinatsos, 2017; Sinanaj & Muntermann, 2013; Smith et al., 2018; Tweneboah-Kodua et al., 2018). Most of these studies have concluded a negative impact on stock price by considering the effect of un-systematic risk factors surrounding the breach such as factors specific to that type of attack (Arcuri et al., 2017; Bose & Leung, 2014; Hovav & D'Arcy, 2003), type of firm (Cavusoglu et al., 2004; Goel & Shawky, 2009; Rosati et al., 2017) and type of industry (Pirounias et al., 2014; Yayla & Hu, 2011) as shown in Figure 01.



Source: Author

Figure 01. IS Breach Contingency Factors as described in Literature

The conceptual framework presented in this paper is based on one of the most fragile sectors, i.e., the banking sector, the performance of which is always associated with economic events (Dosi et al., 2015; Ghosh, 2016; Korkmaz, 2015). In addition to its higher vulnerability to IS breach losses, it is a sector, which has the most rapid spill over effect for a piece of news (Fiordelisi et al., 2013). Due to brisk information transfer effect in banking, incident at one bank can affect the performance and risk indicators of other banks as well (Dreyer et al., 2018). In the event of an unexpected negative event like IS breach announcement by a listed bank will not only influence its unsystematic risk by way of their stock losses but also their systematic risk, i.e., Beta. Due to its spill over and contagion effect of IS, especially within the banking sector (Mee & Schuermann, 2018), the systematic risk of the overall banking sector might get influenced. However, most of the past studies have limited examination on the impact of IS breach announcement on the sector-wide systematic risk, especially in banking. Also, limited exposure has been given on the BCFs from Socio-economy that can cause an influence on sector-wide systematic risk. Socio-economic factors play its part while causing a change in the level of influence to systematic risk (Chakraborty & Das, 2018; Miletić, 2009). In the light of IS breach contingency, we are proposing two socio-economic factors such as Fear of Cyber Crime and the level of ICT penetration. Based on theories of economic crime and investor protection theory, these socio-economic factors can explain the change in the banking sector's systematic risk.

Contrary to the arguments presented above, most of the prior studies examined the effect of IS breach events for the US stock markets by considering the unsystematic risk factors of a firm (Bose & Leung, 2014; Cavusoglu et al., 2004; Hovav et al., 2017). Therefore, this study, at one end, will extend its dimension by examining the impact of IS breach announcement on the banking sectors' systematic risk. Secondly, by extending the BCFs to socio-economy. Thirdly, by having a broader sample of firms, even outside the United States allow future studies to have an international evaluation of stock markets based on macro or socio-economic indicators. This study proposes the following two socioeconomic indicators of a country be annexed within the BCF (1) Cyber Crime Fear (2) Information & Communication Technology Penetration. Fourthly, by concentrating on the banking sector, this paper makes a new contribution to a wide range of persuasive works (Acharya & Yorulmazer, 2008; Al-Sukkar, 2005; Fiordelisi & Marques-Ibanez, 2013) in the banking sector.

The rest of the paper continues in the following way. In Section 2, 3 & 4, problem statement, research questions, and purpose of the study are presented respectively. Section 5 will cover the research methodology along with the conceptual framework, research hypothesis, and has been designed. Whereas, section 6 will shed light on the theoretical and practical contribution to this study.

2. Problem Statement

The announcements of IS breach by a listed bank a has a contagion effect and can augment the banking sector's systematic risk by 1% to 5% (Hinz et al., 2015; Pelletier, 2017). Consequently, the level of augmentation in banking sector's systematic risk is explained by the prevalent socio-economic factors of breach contingency of that country such as (1) Fear of Cyber Crime and (2) ICT Penetration.

3. Research Questions

1. Does the IS breach announcement by a listed Bank augments banking sector's systematic risk?
2. How does the change in the sector's systematic risk after an announcement of IS breach is explained by the Socio-economic factors?

4. Purpose of the Study

This paper aims at developing a conceptual framework for the impact of IS breach announcements on the systematic risk of the banking sector. Moreover, a secondary purpose is to examine the role of socio-economic factors in influencing the change in systematic risk after an announcement of IS breach by Banks. The study was meant to contribute to ongoing research regarding the nature and extent of the statistical relationships between the firm's risk premium, and the systematic risk for firms after the event of IS breach. By characterizing the variation in socio-economic factors, this study also partially assesses the risk and the need for information security regulation and meta-regulation in the banking sector for different countries.

5. Research Methods

5.1. Hypothesis Development

a) IS Breach Announcement and Changes in Sector-wide Systematic Risk

To achieve the first objective of this study, the respective hypothesis will examine the impact of IS breach announcement by one Bank on the systematic risk of the Banking sector. Therefore, H1 will be formulated as:

H1: Announcement of IS Breach by a Bank will augment the Banking sector's systematic risk.

b) Breach Contingency Factors and Changes in Systematic Risk

In line with the second objective, i.e., to evaluate the impact of contingency factors of socio-economy, i.e. (1) Cyber Crime Fear (2) ICT Penetration in explaining the change in systematic risk of the Banking sector, H2 will be formulated as:

H2: After an announcement of IS breach, changes in banking sector's systematic risk will be influenced by the socio-economic factors of a country.

The level of cybercrime fear in society will also affect the risk perception for shareholders of a breached firm. In studies from socio-psychology, a higher level of crime fear triggers less societal protection and augments concern about the social and moral disorder (Hummelsheim et al., 2010; Vieno et al., 2013) and slumps the overall level of trust in the society (Pickett & Wilkinson, 2009). Thus, pumps up the frustration and violence in the general population and shoot up the crime rate and thus, crime fear. The increased crime fear can affect the behavior and psychology of the whole society in general (Hale, 1996; Lane, 2014). Therefore, the chaotic behavior triggered by criminal incidents will influence the financial markets as well because investors perceive more risk and thus expect higher returns (Camerer et al., 1989; Ellsberg, 1961; Tversky et al., 1990). Aforesaid, level of crime, fear differentiate between different countries (Lancee & Van de Werfhorst, 2012; Paskov & Dewilde, 2012). Growing incidents of IS breaches in a country will trigger a higher level of crime fear and investor's risk premium not only for the breached firm but for the whole banking industry. Therefore, influenced systematic risk triggered through the announcement of IS breach will be higher for breached banks in countries with a higher level of cyber-crime fear. Backed by the economic theory of crime, H2 will be broken down into:

H2A: After an announcement of IS breach, changes in banking sector's systematic risk will be greater for Breached Banks in countries with higher cyber-crime fear.

c) ICT Penetration and Changes in Systematic Risk

A higher level of ICT penetration leads to easy and quick access of information to investors, and thus, stock prices of breached firms might behave immediately in the event of IS breach announcement. ICT has played its role in reducing the information asymmetries in financial markets at different countries (Liang & Guo, 2015; Srivastava, 2011) mainly due to the eradication of transitionary or brokerage cost. Moreover, the significant positive impact was found between ICT penetration and stock market development and thus giving rise to the free flow of data (Aral & Weill, 2007; Lechman & Marszk, 2015; Perez, 2011; Shamim, 2007; Singh, 1997). Backed by the Investor Protection Theory, variant level of ICT penetration will also affect the overall sensitivity of stock prices and systematic risk factors. So, an announcement of IS breach of the same type in different countries might lead to a different level of market responses in different countries i.e. different behaviour of market efficiency. Thus, a higher level of ICT penetration advocates higher contagion effect, especially with respect to the banking sector. Consequently, the change in systematic risk in higher ICT penetration countries will be more sensitive to the medium or low ICT penetration countries at the event of IS breach. As a result, the investors in low ICT penetration countries might not react immediately after an announcement of an Internet security breach by a firm. Based on these grounds, this study proposes the next hypothesis as:

H2B: After an announcement of IS breach, changes in banking sector's systematic risk will be quicker for Breached Banks in countries with higher ICT Penetration.

Based on the hypothesis formulated, Socio-economic factors of breach contingency will influence the banking sector's systematic risk after an event of IS breach. In line with the objective of this paper and the hypothesis formulated, BCFs are conceptualized here according to the dimensions of socio-economy. Controlling for other BCFs, i.e., breach type, firm type, and industry type, Figure 3 presents a conceptual framework for this paper.

In this framework, it is demonstrated that an independent variable, i.e., BCFs will influence the dependent variable i.e., banking sector's systematic risk. BCFs are elaborated through two market's information asymmetries. It is hypothesized that crime fear in a country and the ICT penetration as Socio-Economy Breach Contingency Factors can influence the systematic risk of the banking sector.

5.2. Methodology

To study the special influence of a range of incidents, from corporate purchases to joint venture establishment to CEO progressions the method of 'event study' has been engaged comprehensively in the accounting, finance and information security literature (Bose & Leung, 2013; Cavusoglu et al., 2004; Hovav et al., 2017; Kannan et al., 2007; Rosati et al., 2017; Smith et al., 2018; Tweneboah-Kodua et al., 2018; Yayla & Hu, 2011). This statistical practise advocates that an unanticipated event is probable to influence (increase or decrease) the script price resulting an abnormal returns on script prices (MacKinlay, 1997).

The assessment of returns as normal or abnormal is done by comparing the price returns which would have been obtained if there was an event or announcement. Such returns are compared with the actual returns which is actually obtained after an event. If the change is positive, then the effect of the incident to the script price is assumed positive and ceteris peri bus. Lastly, repressors in the framework are used to evaluate the normal return embodies the estimation model (Boehmer et al., 1991; Konchitchki & O'Leary, 2011). Similarly, changes in systematic risk, i.e., Beta will be computed accordingly as demonstrated by (Hinz et al., 2015) for IS breach announcements by consumer electronics firms.

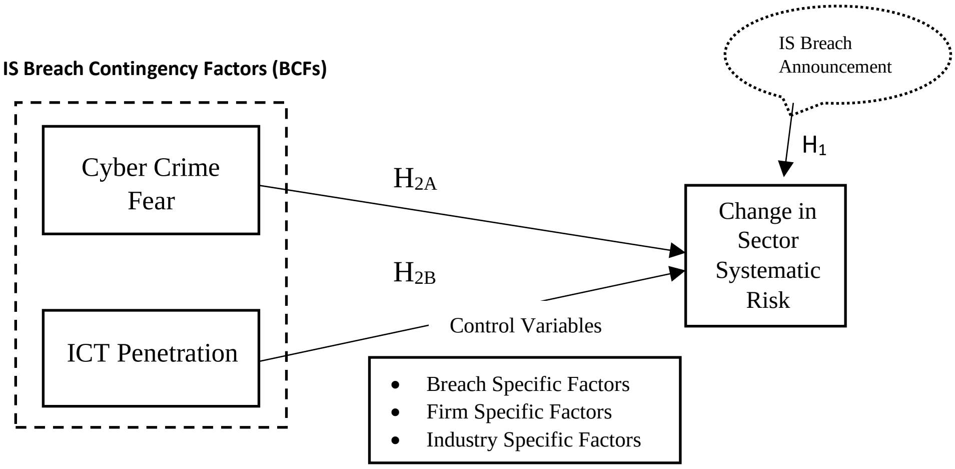


Figure 02. Conceptual Framework

Following the footsteps of IS literature using event study, judgmental sampling is recommended for empirical examination of this framework (Brown & Warner, 1985; Cavusoglu et al., 2004; Corrado, 2011; Konchitchki & O'Leary, 2011; MacKinlay, 1997). Data for breach events will be gathered from secondary sources such as Privacy Rights Clearing House, Lexis/Nexis Database, Factiva, Milermiles, Data loss DB (Bose & Leung, 2014; Cavusoglu et al., 2004; Gatzlaff & McCullough, 2010; Modi et al., 2015; Yayla & Hu, 2011). After further shortlisting of breached firms to listed corporations, the last stage involves tracing of an element of confounding events around the breach date (MacKinlay, 1997). It is usually done to have the stock price independent of those events such as announcements of dividends, mergers, acquisitions, lawsuits, damages, earnings or changes in key executives, etc.

5.2.1. Sector-wide systematic risk (∆β, "DELTAs")

Defined as $\Delta\beta = \Delta(\text{post}) - \Delta(\text{pre})$, where $\Delta(\text{post})$ and $\Delta(\text{pre})$ each represent the average slope of 200 regressions each examining 120 days of returns.

$$B_i = \frac{Cov(R_i\ R_m)}{Var\ R_m}$$

Where, Ri = return of the sector, Rm = market index return). The 200 regressions consist of calculations for [d-120…d-10] (pre) and [d+10…d+120] (post) the breach event, where d = the date of the breach itself. After very thorough filtering from these data sources, as mentioned above, the systematic risk for 200 breach events within the banking sector will be examined. Literature has witnessed various sample sizes to test the effect of BCFs on stock returns. Such as (Cavusoglu et al., 2004) 37 firms, 79 firms (Acquisti et al., 2006), 123 firms by (Yayla & Hu, 2011), 125 firms by (Pirounias et al., 2014), 226 by (Arcuri et al., 2017), 306 (Morse et al., 2011). A time interval of 2011 to 2018 will be used as this period has witnessed a sudden rise in internet crime (Baker & Lewis, 2013; McAfee, 2018; Ponemon Institute, 2018; Wueest, 2014).

The wave of cybercrime in society will function the measurement for cybercrime fear. As if, the increasing incidents of crime will augment the crime fear in society (Chiricos et al., 1997; Jackson & Gray, 2009; Zhao et al., 2015). Therefore, the growing environment of cybercrime events will also affect the overall trust and confidence of users thereby triggering the level of cybercrime fear (Baker & Lewis, 2013; Saini et al., 2012). Thus, it is proposed that cybercrime fear can be measured by the yearly percentage change in cybercrime incidents in a country.

Whereas ICT penetration will be measured by the number of internet users among every 100 unit of population (Asongu et al., 2016). As with higher level of ICT penetration, there will be reduced information asymmetry which will benefit the investors to have easy access to information changes in the market (Aral & Weill, 2007; Lechman & Marszk, 2015; Perez, 2011; Shamim, 2007; Singh, 1997). Whereas, the endogenous construct, i.e., sector systematic risk, will be measured by a change in Sector Beta of Banking β_Sector. In the light of operationalization of variables, Figure 3 presents the Path Diagram for the proposed conceptual framework.

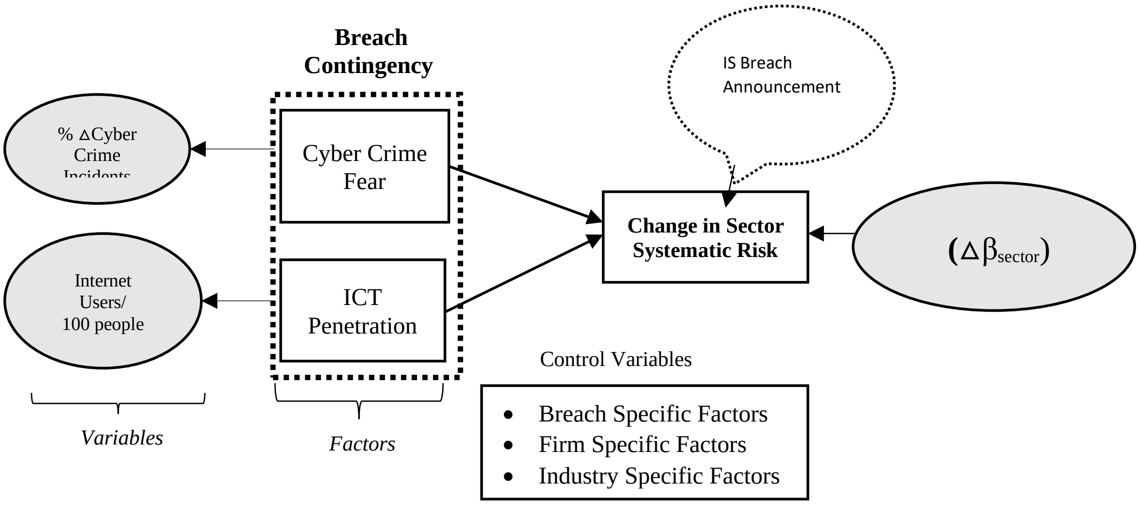


Figure 03. Path Diagram of Conceptual Research Framework

https://doi.org/10.15405/epsbs.2020.12.05.54
Corresponding Author: Syed Emad Azhar Ali
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

6. Contribution

6.1. Theoretical Contribution

Considering the scenario of IS breach, this paper will make a significant contribution to the theory of efficient market hypothesis by way of extension and integration of theories. EMH under the context of IS breach has been limited by the BCFs of attack type, firm type, and industry type. However, this study advocates that socio-economic factors prevalent in society will further explain the change in stock market behaviour after an announcement of IS breach. Moreover, a noteworthy extension is also expected to the theory of crime fear. The theory postulates that a higher crime fear gives rise to proactive precautionary planning among society's individuals. In this regard, this paper proposes to extend this theory to the uncertain environment of a stock market. This research argues that the level of crime fear and precautionary planning will affect the investor's confidence and thus, the systematic risk of sector. This is the pioneer and widespread research which can gauge the effect of IS breach incidents on the systematic risk of banking firms, globally. In addition to increasing the scope of the study to firms outside the United States, the study has mainly opened a new dimension of Socio-Economic Factors within BCFs. Thus, providing a significant extension to the theory of efficient markets.

6.2. Practical Contribution

This study aims to help investors to assess the risk of their investments when their funds are in the banking sector for different stock markets. By considering the systematic risk factors from socio-economy, investors can assess and minimize their possible losses at the event of IS breach. As per finance literature, banks cannot minimize the systematic risk but can plan IS investments along with the designing of appropriate security protocols and measures in their information systems.

6.3. Limitation of the Study and Future Direction

The study only covers the breach announcement by listed banks only. In most of the countries, cyber security laws and reporting requirements are very much at the early stage. For instance, reporting of an IS breach incidents is mandatory in the United States only. Whereas most of the IS breaches within Banks and with other firms go unnoticed or was announced by non-listed firms. Thus, the lack of sufficient data been the major limitation of this study.

Future studies in this area can be conducted by incorporating other systematic risk factors which can be theorized with the IS breach contingency. Furthermore, the role of systematic risk factors of socio-economy can also be examined directly with the stock losses of the breached firm through some moderation or mediation.

7. Conclusion

Incidents of IS breaches are gravely aching the businesses and economies around the world. This paper presents a conceptual framework that scrutinizes the influence of IS breach announcement on the banking sector's systematic risk. Studies in the past albeit showed evidence that IS breach announcements can cause a significant negative influence on the share prices of breached firms. However, limited light has been shed on the impact of such IS breach announcement on the systematic risk of a sector such as banking. However, most of the studies are limited as they have examined the BCF of firms from the USA. Based on socio-economic factors, this paper has introduced a conceptual framework which can assess the sector's systematic risk after the event of IS breach.

The proposed conceptual framework aims to help investors at the international level to avoid the risk of abnormal stock losses in the event of a breach. Secondly, this study also intends to help the credit rating agencies, lenders and especially the insurance firms to evaluate the degree of cyber risk involved in a firm of a country which will aid them while fixing their premium.

From the firm's point of view, this study proposes to assist firms in harmonizing the monitoring expenses with the paybacks of improved security. A sector's systematic risk will affect the overall market value or net worth of a firm in the eyes of investors. The worth of a firm can be influenced by various factors which also include the risk management methods being adopted by a firm (Shad et al., 2019; Woon et al., 2011). Therefore, cyber security regulators in a country are required to frame policies and necessary reporting requirements for firms which can help to boost up the confidence of shareholders.

Acknowledgments

The authors would like to acknowledge Universiti Teknologi PETRONAS (UTP), Department of Management, and Humanities to facilitate this research study. The authors would also like to thank the reviewers for their valuable suggestion in order to enhance the manuscript.

References

Acharya, V. V., & Yorulmazer, T. (2008). Information contagion and bank herding. *Journal of Money, Credit and Banking*, *40*(1), 215–231.

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94.

Al-Sukkar, A. S. (2005). The application of information systems in the Jordanian banking sector: a study of the acceptance of the internet.

Aral, S., & Weill, P. (2007). IT assets, organizational capabilities, and firm performance: How resource allocations and organizational differences explain performance variation. *Organization Science*, *18*(5), 763–780.

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017). How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns. In *ITASEC* (pp. 175–193).

Asongu, S. A., Nwachukwu, J. C., & Tchamyou, V. S. (2016). Information asymmetry and financial development dynamics in Africa. *Review of Development Finance*, *6*(2), 126–138.

Baker, S. A., & Lewis, J. A. (2013). The Economic Impact of Cybercrime and Cyber Espionage. *Center for Strategic and International Studies*, (July), 20. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

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

Bianchi, D., & Tosun, O. (2018). Cyber Attacks and Stock Market Activity.

Boehmer, E., Masumeci, J., & Poulsen, A. B. (1991). Event-study methodology under conditions of event-induced variance. *Journal of Financial Economics*, *30*(2), 253–272.

Bose, I., & Leung, A. C. M. (2013). The impact of adoption of identity theft countermeasures on firm value.

Decision Support Systems, *55*(3), 753–763.

Bose, I., & Leung, A. C. M. (2014). Do phishing alerts impact global corporations? A firm value analysis. *Decision Support Systems*, *64*, 67–78.

Brown, S. J., & Warner, J. B. (1985). Using daily stock returns: The case of event studies. *Journal of Financial Economics*, *14*(1), 3–31.

Camerer, C., Loewenstein, G., & Weber, M. (1989). The curse of knowledge in economic settings: An experimental analysis. *Journal of Political Economy*, *97*(5), 1232–1254.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70–104.

Chakraborty, B., & Das, S. (2018). Evaluation Criteria of Project Risk and Decision Making Through Beta Analysis and TOPSIS Towards Achieving Organizational Effectiveness. In *International Conference on Computational Intelligence, Communications, and Business Analytics* (pp. 155–164). Springer.

Chiricos, T., Eschholz, S., & Gertz, M. (1997). Crime, news and fear of crime: Toward an identification of audience effects. *Social Problems*, *44*(3), 342–357.

Corrado, C. J. (2011). Event studies: A methodology review. *Accounting & Finance*, *51*(1), 207–234.

Dosi, G., Fagiolo, G., Napoletano, M., Roventini, A., & Treibich, T. (2015). Fiscal and monetary policies in complex evolving economies. *Journal of Economic Dynamics and Control*, *52*, 166–189.

Dreyer, J. K., Schmid, P. A., & Zugrav, V. (2018). Individual, Systematic and Systemic Risks in the Danish Banking Sector. *Finance a Uver*, *68*(4), 320–350.

Ellsberg, D. (1961). Risk, ambiguity, and the Savage axioms. *The Quarterly Journal of Economics*, 643–669.

Ettredge, M., & Richardson, V. J. (2001). Assessing the risk in e-commerce. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences* (pp. 11-pp). IEEE.

Fama, E. F. (1991). Efficient capital markets: II. *The Journal of Finance*, *46*(5), 1575–1617.

Fama, E. F., Fisher, L., Jensen, M. C., & Roll, R. (1969). The adjustment of stock prices to new information. *International Economic Review*, *10*(1), 1–21.

Fiordelisi, F., & Marques-Ibanez, D. (2013). Is bank default risk systematic? *Journal of Banking & Finance*, *37*(6), 2000–2010.

Fiordelisi, F., Soana, M.-G., & Schwizer, P. (2013). The determinants of reputational risk in the banking sector. *Journal of Banking & Finance*, *37*(5), 1359–1371.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*(1), 61–83.

Ghosh, S. (2016). Political transition and bank performance: how important was the Arab Spring? *Journal of Comparative Economics*, *44*(2), 372–382.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*(7), 404–410.

Hale, C. (1996). Fear of crime: A review of the literature. *International Review of Victimology*, *4*(2), 79–150.

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, *52*(3), 337–347.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, *6*(2), 97–121.

Hovav, A., & D'Arcy, J. (2004). The impact of virus attack announcements on the market value of firms. *Information Systems Security*, *13*(3), 32–40.

Hovav, A., Han, J., & Kim, J. (2017). Market Reaction to Security Breach Announcements: Evidence from South Korea. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *48*(1), 11–52.

Hummelsheim, D., Hirtenlehner, H., Jackson, J., & Oberwittler, D. (2010). Social insecurities and fear of crime: A cross-national study on the impact of welfare state policies on crime-related anxieties. *European Sociological Review, 27*(3), 327–345.

Jackson, J., & Gray, E. (2009). Functional fear and public insecurities about crime. *The British Journal of Criminology*, *50*(1), 1–22.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce, 12*(1), 69–91.

Konchitchki, Y., & O'Leary, D. E. (2011). Event study methodologies in information systems research. *International Journal of Accounting Information Systems*, *12*(2), 99–115.

Korkmaz, S. (2015). Impact of bank credits on economic growth and inflation. *Journal of Applied Finance and Banking*, *5*(1), 51.

Lancee, B., & Van de Werfhorst, H. G. (2012). Income inequality and participation: A comparison of 24 European countries. *Social Science Research*, *41*(5), 1166–1178.

Lane, J. (2014). *Fear of crime in the United States: Causes, consequences, and contradictions*. Carolina Academic Press.

Lechman, E., & Marszk, A. (2015). ICT technologies and financial innovations: the case of Exchange Traded Funds in Brazil, Japan, Mexico, South Korea and the United States. *Technological Forecasting and Social Change*, *99,* 355–376.

Liang, P., & Guo, S. (2015). Social interaction, Internet access and stock market participation—An empirical study in China. *Journal of Comparative Economics*, *43*(4), 883–901.

MacKinlay, A. C. (1997). Event studies in economics and finance. *Journal of Economic Literature*, *35*(1), 13–39.

Malhotra, A., & Kubowicz Malhotra, C. (2011). Evaluating customer information breaches as service failures: An event study. *Journal of Service Research*, *14*(1), 44–59.

Malkiel, B. G., & Fama, E. F. (1970). Efficient capital markets: A review of theory and empirical work. *The Journal of Finance*, *25*(2), 383–417.

McAfee. (2018). Economic Impact of Cybercrime — No Slowing Down, (February).

Mee, P., & Schuermann, T. (2018). How a Cyber Attack Could Cause the Next Financial Crisis. *Harvard Business School Publishing.*

Miletić, I. (2009). Macroeconomic and microeconomic causes for the instability of banks. *Economic Research-Ekonomska Istraživanja*, *22*(1), 47–59.

Modi, S. B., Wiles, M. A., & Mishra, S. (2015). Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management, 35,* 21–39.

Morse, E. A., Raval, V., & Wingender, J. R. Jr. (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective*, *20*(6), 263–273.

Paskov, M., & Dewilde, C. (2012). Income inequality and solidarity in Europe. *Research in Social Stratification and Mobility*, *30*(4), 415–432.

Pelletier, J. M. (2017). *Effects of Data Breaches on Sector-Wide Systematic Risk in Financial, Technology, Healthcare and Services Sectors.* Capella University.

Perez, C. (2011). *Technological Revolutions and Financial Capital.* DELO.

Pickett, K., & Wilkinson, R. (2009). The spirit level: Why more equal societies almost always do better. *Allen Lane*.

Pirounias, S., Mermigas, D., & Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *Journal of Information Security and Applications*, *19*(4–5), 257–271.

Ponemon Institute. (2018). Ponemon Institute – The 2018 Cost of a Data Breach Study by the Ponemon Institute. *IBM Security Services*, (July). https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&

Rosati, P., Cummins, M., Deeney, P., Gogolin, F., van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis*, *49*, 146–154.

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-Crimes and their Impacts : A Review. *International Journal of Engineering Research and Applications*, *2*(2), 202–209.

Sangvinatsos, A. (2017). *A Random Walk Down Wall Street: The Time-Tested Strategy For Successful Investing.* Taylor & Francis.

Shad, M. K., Lai, F.-W., Fatt, C. L., Klemeš, J. J., & Bokhari, A. (2019). Integrating sustainability reporting into enterprise risk management and its relationship with business performance: A conceptual framework. *Journal of Cleaner Production*, *208*, 415–425.

Shamim, F. (2007). The ICT environment, financial sector and economic growth: a cross-country analysis. *Journal of Economic Studies*, *34*(4), 352–370.

Sinanaj, G., & Muntermann, J. (2013). Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis. In *Bled eConference* (p. 29).

Singh, A. (1997). Stock markets, financial liberalization and economic development. *Economic Journal*, *107*(442), 771–782.

Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2018). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society*.

Srivastava, S. (2011). Impact of internet growth on the online stock trading in India.

Tversky, A., Slovic, P., & Kahneman, D. (1990). The causes of preference reversal. *The American Economic Review*, 204–217.

Tweneboah-Kodua, S., Atsu, F., & Buchanan, W. (2018). Impact of cyberattacks on stock performance: a comparative study. *Information & Computer Security*, *26*(5), 637–652.

Vieno, A., Roccato, M., & Russo, S. (2013). Is fear of crime mainly social and economic insecurity in disguise? A multilevel multinational analysis. *Journal of Community & Applied Social Psychology*, *23*(6), 519–535.

Woon, L. F., Azizan, N. A., & Samad, M. F. A. (2011). A strategic framework for value enhancing enterprise risk management. *Journal of Global Business and Economics*, *2*(1), 23–47.

World Economic Forum. (2018). The Global Risks Report 2018. https://www.weforum.org/reports/the-global-risks-report-2018

Wueest, C. (2014). Targeted attacks against the energy sector. *Symantec Security Response, Mountain View, CA.*

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60–77.

Zhao, J. S., Lawton, B., & Longmire, D. (2015). An examination of the micro-level crime–fear of crime link. *Crime & Delinquency*, *61*(1), 19-44.