Journal of Management Science and Business Intelligence, YYYY, 0–0
Month. 2018, pages xx-xx
doi: xx.xxxx/xxxxxxxxx/xxxxx
http://www.ibii-us.org/Journals/JMSBI/
ISBN 2472-9264 (Online), 2472-9256 (Print)

Longitudinal analysis of information security incident spillover effects

Justin M. Pelletier, PhD

Department of Computing Security, Rochester Institute of Technology, Rochester, NY, USA

Email: justin.m.pelletier@rit.edu

Received on XXXXX; revised on XXXXX; published on XXXXX

Abstract

When a company is hacked, market participants take notice. This has been observed consistently for at least a decade, mostly through calculating abnormal returns of individual corporate stocks after a company's information security incident announcement. Some researchers have found that information security incidents have had a decreasing effect on stock price over time. Their reports suggest that breach related stock price impacts have become increasingly shallow and short-lived. This has led some information security economists to suggest that market forces are not enough to incentivize sufficient corporate investment to information security. They argue that further regulation is necessary to remedy what seems like a rise in investor apathy toward corporate breaches. Other researchers, though, have cautioned that further examination is required and that other market metrics—beyond individual stock price movements—are available to better understand the effects of an information security incident.

Sector-wide systematic risk is a measure of the sector's exposure to exogenous shock. Here, this risk measurement is applied to measure the spillover effects of a corporate information security incident. I conduct 203 event studies between the years 2006 and 2016, calculating sector-wide systematic risk within American stock markets, to measure the spillover effects of data breaches within finance, healthcare, technology and services sectors. The novel application of a longitudinal analysis of variance between repeated event studies reveals that the sector-wide spillover of an incident is both significant and growing. This suggests that an increasingly compelling market incentive exists for sectors to police themselves. Also, further inquiry into common factors among outliers to these sector-wide trends may reveal best-practice strategies for information security risk management.

Keywords: Information Security Economics, Event Study, Longitudinal Analysis, Systematic Risk

1 Introduction

Increasing rates of data breaches, despite ongoing information security investments, motivate continued research in information security economics (Gordon, Loeb, Lucyschyn, & Zhou, 2015). Attacks span industries (consumer electronics, retail, etc.) and market categories (government, public, private, not-for-profit) (Hinz, Nofer, Schiereck, & Trillig, 2015). To better inform information security investment, there have been several analytic attempts to quantify and understand the effects of information security incidents.

Anderson (2001) provided seminal research investigating the difficulties of quantifying the inputs to information security investment decisions through the lens of economics. Estimating changes to the market-generated risk premium, represented by the beta coefficient in modern portfolio theory's capital asset pricing model, as shown in Equation 1, where α represents the intercept of the regression, β represents the slope of the regression measuring systematic risk, R_m represents the expected market return, R_f represents the risk-free rate, and ε represents the random error accounting for unsystematic risk (Cardenas, Coronado, Donald, Parra & Mahmood, 2012).

$$\text{Expected Return} = a + b(R_m - R_f) + e \quad (1)$$

This model is a necessary component of a manager's decision calculus regarding capital allocations (Anderson, 2001). Managers of publicly traded firms seek to positively impact share prices and are thereby influenced by changes to the risk premiums applied within capital markets. Anderson's 2001 investigation of difficulties with quantifying the inputs to information security investment decisions remains unresolved. For example, Hinz et al. (2015) conclude that the effects of information security incidents on risk premium are poorly understood, which creates uncertainty for the methods used to determine a firm's capital costs through risk premium.

Information security economists continue to investigate optimal investment expenditures and hypothesize on the mechanisms available to motivate further expenditure (Gordon et al., 2015). In 2015, Gordon et al. built on previous work to extend the Gordon-Loeb Model (Gordon & Loeb, 2002) to evaluate the optimal information security investment as a function of risk management function. The authors considered the monetary loss, vulnerability, and probability to determine the expected loss after an investment in security. The extended Gordon-Loeb Model, shown in Equation 2, includes the calculation of losses arising from externalities like those described by the within-industry spillover effect of perceived risk, hypothesized by Etredge and Richardson (2003) and confirmed by later research (Kashmiri, Nicol & Hsu, 2017). The extended Gordon-Loeb Model presents an inequality, shown in Equation 2, that calculates the maximum a risk-neutral firm should invest in information security protections, taking into account both internal and external costs, where z^{sc} represents the socially optimal level of firm investment in information security, v represents the underlying vulnerability as a probability that a breach attempt will be successful without further information security investment, L^P represents expected private losses resulting from an information security incident, L^E represents expected externality losses, and $\gamma = L^E/L^P$ represents the ratio between externality losses and private losses when an information security incident occurs (Gordon et al., 2015). This equation builds on previous findings that establish the economically optimal maximum investment as 36.79% of expected loss (Gordon & Loeb, 2002).

$$z^{sc}(v) < (1/e)(1+g)vL^P \approx 0.3679(1+g)vL^P \quad (2)$$

The concept of a within-industry spillover effect is an extension of previous efforts to document information followership patterns in capital markets (Anderson & Holt, 1997), and convergent behavior herding (Zhou & Lai, 2009). This is further confirmed by recent investigation by Lee, Hall and Cegielski (2018), who consider the theoretical characteristics among companies that may create similarities and probably influence contagion effects after an information security event.

According to Hinz et al. (2015), it was unclear how data breach effects on capital market participants have changed over time. This was important because, in 2011, Gordon, Loeb, and Zhou concluded that information security breaches may have a diminishing effect on a firm's systematic risk over time, implying that capital market participants see exposure to data breaches as decreasingly important. In 2015, Gordon et al. used Gordon, Loeb and Zhou's 2011 findings to postulate the argument that additional government regulation is necessary to create economically optimal information security purchasing decisions. This was especially relevant given the recent push for research on within-industry spillover effects of the breach of an individual company (Kashmiri et al., 2017; Martin, Borah, & Palmatier, 2017), and the 2015 argument by Gordon et al. that these spillover effects represent social costs that require regulatory mitigation.

However, Hinz et al. (2015) reviewed the available evidence and found that further research is necessary to better characterize the changing impact of a data breach on risk measurements in capital markets. This impacts all companies seeking to finance through public investment markets, and probably has greater impact when companies are economically similar.

2 Methods

This study quantitatively describes the changes over time of information security incident spillover effects. This study analyzed the variance across repeated measurements of event studies, each of which calculated sector-wide systematic risk using the capital asset pricing model, to inform the ongoing debate between extrinsic vs. intrinsic market incentivization, as well as the necessity of further information security investment within those sectors most prone to data breaches.

Event studies allow the measurement of changes in financial data that can be statistically attributable to a specific event. The event study method relies on the calculation of the abnormal returns (MacKinlay, 1997), using the capital asset pricing model (CAPM) regression equation, shown in Equation 1 and described above. The inputs to CAPM were publicly available at Yahoo! Finance (2017), Google Finance (2017), and several other public sites. The data for information security incidents were available at PrivacyRights.org (PrivacyRights, 2017).

Table 1. Summary of Breaches Selected for Sample

Screening criterion	Number of breaches available for study
Total breaches reported (2006-2016)	5325
Even-year stratification	2059
Traded on NYSE or NASDAQ	285
Most frequent sectors (87% of breaches)	228
Stock data available around breach dates	203

The 203 investigated breaches were spread across the Healthcare, Finance, Technology and Services sectors.

Table 2. Indexes and Sectors

Sector	Index	Ticker
Financial	Vanguard Financials ETF	VFH
Healthcare	Vanguard Health Care ETF	VHT
Services	VanEck Vectors Retail ETF	RTH
Technology	Vanguard Info. Tech. ETF	VGT
Market Model	S&P 500	GSPC

Of all available indices, the Vanguard exchange traded funds (ETFs) are among the longest running and most widely known. Each corresponds directly to the sector under investigation, with the exception of the services sector. Due to Vanguard's within-sector split between consumer stables and consumer discretionary goods, the VanEck Vectors Retail ETF was selected as an appropriate balance across the industries making up that sector.

The population of firms suffering data breaches was difficult to quantify, due to the active concealment employed by perpetrators employ to conceal breaches. Among the global population of breaches, several types of data compromise existed. These were categorized as fraud involving payment card(s), detection of hacking or other malware, intentional insider breach, physical loss of paper records, loss of portable device(s), loss of stationary device(s), and unintended disclosure (PrivacyRights, 2017). In practice, many initial reports did not contain a full understanding of the breach

vector so the population also contained a category for unknown causes. The number of information security incidents that were not publicly disclosed remains a source of speculation beyond the purview of this investigation.

Publicly traded firms represented only a fraction of the companies who reported breaches during the time span under investigation. Of the available breach records, only every other year of data were considered, which allowed for discrete groupings of the continuous event study regression outputs. Of the 2,059 breach reports occurring in the even years between 2006 and 2016, 285 represented companies traded on the NYSE or NASDAQ exchanges. A frequency analysis revealed that 87% of publicly traded breaches occurred in four core sectors: Financial, Healthcare, Services and Technology. As shown in Table 1, there were enough available data to conduct 203 event studies. Calculation of abnormal returns requires an expected market return, as shown and described in Equation 1, which necessitates the selection of sector and market indexes. These index and market model selection are depicted in Table 2 and represent the best sector-industry fit among available alternatives. The market model used here—the Standard & Poor's 500 list—matches the model used in the systematic risk analysis performed by Hinz et al. (2015). The standardization of market models allows for comparison between findings, which is important when (as in Hinz et al.'s report) there was no significance observed in change to the systematic risk for an individual firm.

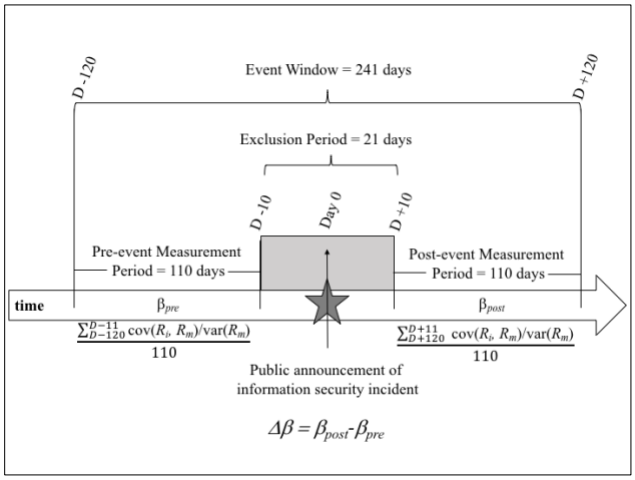

Fig. 1. Event studies of sector-wide systematic risk as a measurement of spillover effect. The primary measurement instrument was used repeatedly across the time-stratified sample to compare pre- and post-event mean covariance of sector and market returns, relative to variance of market returns, over a 241-day event window. An exclusion period of 21 days insulates against short-term share price effects, disparate information dispersion, and other market inefficiencies.

The reliability of the event study relies on a rolling beta factor to examine covariance of sector and market returns, and variance of market returns, during an event window. As shown in Figure 1, the event window consists of a 241-day period (-120, 0, +120). The main threat to reliability existed with the potential conflation of short-term effects resulting from the breach announcement on the firm or sector returns. This corresponded to a potential for temporary skew in the intercept (α), which could have confounded the slope calculation (β) in the regression model. In accordance with the recommendation and practice by Hinz et al. (2015), this study excluded a period of 21 days (-10, 0, +10) around the breach announcement, which partially controls for bias resulting from cumulative abnormal returns associated with the breach itself (Hinz et al., 2015; Yayla & Hu, 2011). Further, the exclusion period helps offset potential market inefficiencies resulting in uneven information dispersion about the information security incident itself. Finally, specific deviation from the CAPM equation for the event study calculations in this study included omission of R_f, and ε, which follows precedents set by Hinz et al. (2015) and Schatz and Bashroush (2016), in accordance with the market model method recommended by Dyckman, Philbrick and Stephan (1984), that instead favors the derivative shown in Equation 3.

$$b_i = \text{cov}(R_i, R_m) / \text{var}(R_m) \tag{3}$$

Each event study is conducted using Equation 4, where β_{post} and β_{pre} each represent the mean slope of 110 regressions, where each regression examines 120 days of returns as described in Equation 3, when R_i represents the return of the sector and R_m represents the market index return.

$$\Delta b = b_{post} - b_{pre} \tag{4}$$

To maintain the quality of data, each $\Delta\beta$ was manually screened to only consider those records that demonstrated statistically significant differences between the pre- and post-breach regression means. All event study records that failed to exceed a 95% confidence ($p > .05$) were rejected, leaving 140 breach reports that showed significant differences when comparing the sector's risk profile before and after the breach.

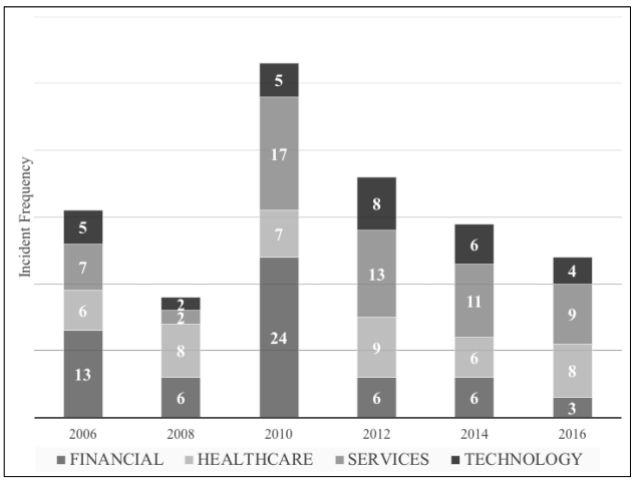

Fig. 2. Information security incidents of publicly traded companies by year and sector. In this repeated measures ANOVA, each sector is treated as a subject and the event studies measuring sector-wide spillover from each breach provides the means for within-subjects analysis of variance over time.

The measure of change to sector systematic risk over time ($\delta\beta/\delta\tau$) was calculated to inform repeated measures analysis of variance (ANOVA) using restricted maximum likelihood (REML) and applied compound symmetry for covariance structure determination. The use of REML eliminates the effect of nuisance parameters, thereby allowing for unbiased estimates of variance and covariance (Harville, 1977; Patterson & Thompson, 1971). The model also employed a fixed intercept that set 2006 as a baseline control group against which each other year was compared. The repeated measures ANOVA allows for examination of the effects of multiple breaches within the same sector over time. The

repeated measures ANOVA is most appropriate to test equality of means under several different conditions involving repeated measures within the same subject (Dien, 2017). As shown in Figure 2, I treat each sector as an individual subject, where each event study is a measurement of that sector's risk-response to an information security incident.

3 Results

There was a significant relationship observed between year of a breach (IV) and the change in sector systematic risk (DV), representing information security incident spillover effect. The overall model fit is significant at p = 0.015, with increasing significance over time, as demonstrated in Table 3 and illustrated in Figure 3.

As enumerated in Table 4 and depicted in Figure 4, significant results existed only for the year of the breach (p = 0.036), not for firm sector (p = 0.344) or covariance effects between year and sector (p = 0.574).

Table 3. BY-YEAR spillover effects

Effects	Num *df*	Den d*f*	*F*	*p*
BY YEAR	5	27	3.491	**0.015**
Source	Δβ Value	Std Error	*T*	*p*
Intercept	0.000			
2006	0.00%			
2008	-0.04%	0.004	-0.093	0.926
2010	0.48%	0.003	1.402	0.172
2012	0.84%	0.004	2.268	**0.032**
2014	1.21%	0.004	3.183	**0.004**
2016	1.08%	0.004	2.672	**0.013**

The analysis of variance between the repeated measures within each sector revealed a statistically significant overall effect on beta across all sectors—the sector-wide systematic risk calculation used here to measure spillover effects from an information security incident.

Table 4. BY-YEAR-BY-SECTOR spillover effects

Effects	Num *df*	Den d*f*	*F*	*p*
YEAR	5	12	3.470	**0.036**
SECTOR	3	104	1.120	0.344
YEAR*SECTOR	15	12	0.911	0.574

The covariance displayed in under by-year-by-sector breach effects on the mean change in systematic risk, was nearly as likely to occur under the null hypothesis as the alternative. This covariate analysis was revealed by a null model likelihood ratio test ($\chi 2$ = 0.024, p = 0.878).

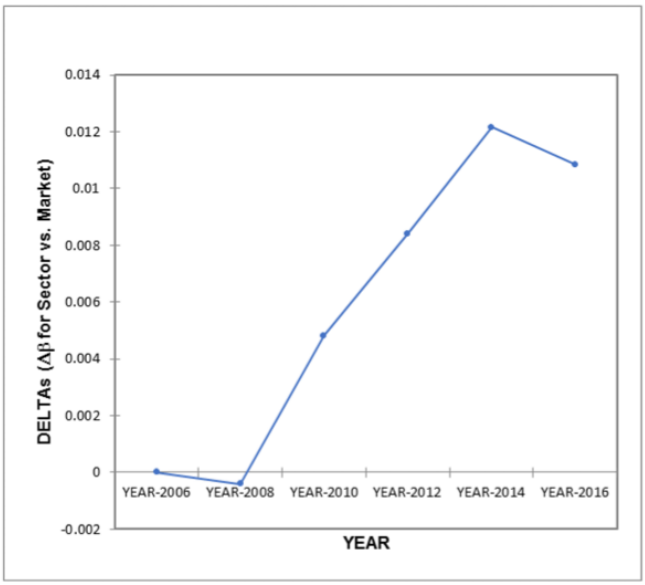

Fig. 3. Significant changes to sector systematic risk over time reveal an increasing information security spillover effect on sector as time increases.

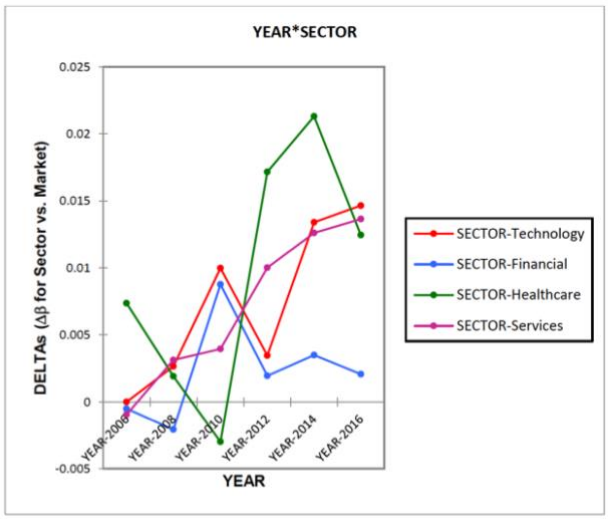

Fig. 4. Spillover effects did not show significant differences between sectors.

4 Discussion and Future Research

The findings presented here suggest that the potential exists for a market-based incentive to motivate further information security investment. The results demonstrate that breach effects can be measured across an entire sector and that those sector-wide effects are increasing over time. This study represents the first quantitative observation of those effects. These data suggest that, after a firm is breached, the entire sector is perceived as increasingly risky, which almost certainly raises the risk premium that firms within the sector must pay when they seek financing.

This study revealed three main areas of further investigation: 1) examination of those event studies that did not reveal significant differences in pre- and post- breach systematic risk within the sector; 2) examination of those companies who were somehow immune to the otherwise sector-wide spillover effects; and 3) regulatory regimes best equipped to enforce compliance with market-driven standards for information security risk management.

The 63 information security incidents that did not demonstrate significance in the $\Delta\beta$ calculation, shown in Equation 4, demonstrate opportunity for future research. Specifically, further investigation should consider the common factors among those events that suggest potential organizational protections for spillover. Some theoretical considerations are proposed by Lee, Hall and Cegielski (2018), who discuss the factors that may influence contagion and therefore could suggest company- or sector-specific spillover protections.

Similar suggestions might be harvested from individual investigation of outliers within those event studies that demonstrated significant sector-wide spillover. An analysis of significant common factors among outliers—those companies that are somehow shielded from spillover effects—would suggest company-specific risk management policies and practices that might insulate firms from the breach of a near neighbor.

My findings here, namely that market incentives do exist to motivate sector-wide information security investment, present an evidentiary challenge to the suggestion that further regulation is necessary to account for the extrinsic costs of a breach. Taking these market incentives into consideration, future research could consider regulatory regime options that balance mandate and enforcement with sector- or industry-defined standards. For example, Hemphill and Longstreet (2016) described a model for meta-regulation that includes a compulsory mandate for compliance with industry-defined information security standards. This is in line with a body of research into standard setting initiatives within those organizations most affected by the standard (eg. Romanosky, Hoffman, & Acquisti, 2012; Aggarwal, Dai & Walden, 2011; and Khoo, Harris, & Hartman, 2010). Also, the growing option for risk transfer through cyber liability insurance and suggests that firms should consider this mechanism for information security risk management. Finally, Figure 4 demonstrates that there were no significant differences in spillover effects across sectors, but it is interesting to observe the potential influence of the financial sector on the overall analysis, as well as that sector's changing regulatory environment during the 2010-2012 time-span. While beyond the scope of this investigation, a multicollinear analysis of regulatory events and information security incidents within the financial industry may demonstrate significance in follow-on inquiry.

Acknowledgements

The author is grateful to the Creator for all the blessings He gives, especially the love of family.

Conflict of Interest: none declared.

References

Aggarwal, B., Dai, Q., & Walden, E.A. (2011). The more, the merrier? How the number of partners in a standard-setting initiative affects shareholder's risk and return. *MIS Quarterly, 35*, 445-462. Retrieved from http://www.misq.org/

Anderson, R. (2001). Why information security is hard: An economic perspective. Proceedings of ACSAC 2001: *17th Annual Computer Security Applications Conference*. New Orleans, LA: December 10-14, 2001. doi:10.1109/ACSAC.2001.991552

Anderson, L. R. & Holt, C. A. (1997). Information cascades in the laboratory. *The American Economic Review, 87*, 847-862. Retrieved from http://www.jstor.org/stable/2951328

Cardenas, J., Coronado, A., Donald, A., Parra, F., & Mahmood, M.A. (July 29, 2012). The economic impact of security breaches on publicly traded corporations: An empirical investigation. *AMCIS 2012 Proceedings*, 7. Retrieved from http://aisel.aisnet.org/amcis2012/proceedings/StrategicUseIT/7

Dien, J. (2017). Best practices for repeated measures ANOVAs of ERP data: Reference, regional channels, and robust ANOVAs. *International Journal of Psychophysiology, 111*, 42-56. http://dx.doi.org/10.1016/j.ijpsycho.2016.09.006

Dyckman, T., Philbrick, D., & Stephan, J. (1984). A comparison of event study methodologies using daily stock returns: A simulation approach. *Journal of Accounting Research, 22*, 1-30. Retrieved from http://www.jstor.org/stable/2490855

Ettredge, M.L. & Richardson, V.J. (2003). Information transfer among internet firms: The case of hacker attacks. *Journal of Information Systems, 17*, 71-82. http://dx.doi.org/10.2308/jis.2003.17.2.71

Google Finance. (2017). Database of publicly traded companies. *Google Finance*. Retrieved from: https://www.google.com/finance

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

Gordon, L.A., Loeb, M.P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb Model. *Journal of Information Security, 2015*(6), 24–30. http://dx.doi.org/10.4236/jis.2015.61003

Gordon, L.A., Loeb, M.P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*, 33-56. doi:10.3233/JCS-2009-0398

Harville, D.A. (1977). Maximum likelihood approaches to variance component estimation and relatied problems. *Journal of the American Statistical Association, 72* (358), 320-338. doi:10.2307/2286796

Hemphill, T.A. & Longstreet, P. (2016). Financial data breaches in the US retail economy: Restoring confidence in information technology security standards. *Technology in Society, 44*, 30-38. http://dx.doi.org/10.1016/j.techsoc.2015.11.007

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (April 2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management, 52*, 337-347. doi:10.1016/j.im.2014.12.006.

Kashmiri, S., Nicol, C.D., & Hsu, L. (2017). Birds of a feather: Intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science, 45*, 208-228. doi:10.1007/s11747-016-0486-5

Khoo, B., Harris, P., & Hartman, S. (2010). Information Security governance of enterprise information systems: An approach to legislative compliant. *International Journal of Management and Information Systems, 14*, 49-55. http://dx.doi.org/10.19030/ijmis.v14i3.840

Lee, J., Hall, D., & Cegielski, C. (2018). Spillover of Information Security Incidents Impact: The Moderating Role of Social Networks and IT. Retrieved from https://aisel.aisnet.org/amcis2018/

MacKinlay, C.A. (1997). Event studies in economics and finance. *Journal of Economics Literature, 35*, 13-39. Retrieved from http://www.jstor.org/stable/2729691

Martin, K.D., Borah, A., & Palmatier, R.W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*, 36-58. http://dx.doi.org/10.1509/jm.15.0497

Patterson, H.D. & Thompson, R. (1971). Recovery of inter-block information when block sizes are unequal. *Biometrika, 58* (3), 545. doi:10.1093/biomet/58.3.545

PrivacyRights. (2017). Chronology of data breaches. *Privacy Rights Clearinghouse*. Retrieved from http://www.privacyrights.org/data-breach/new.

Romanosky, S., Hoffman, D., & Acquisti, A. (2012). Empirical analysis of data breach litigation. *Journal of Legal Studies*, 1-30. Retrieved from http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf.

Schatz, D. & Bashroush, R. (2016). The impact of repeated data breach events on organizations' market value. *Information & Computer Security, 24*(1), 73-92. http://dx.doi.org/10.1108/ICS-03-2014-0020

Yahoo! Finance. (2017). Historical database of public equities markets. *Yahoo! Finance*. Retrieved from: http://finance.yahoo.com/. Instructions for retrieval retrieved from: http://www.elitetrader.com/et/index.php?threads/c-retrieving-

yahoo-historical-prices.80912/ and http://www.mathworks.com/help/datafeed/retrieve-current-and-historical-data-using-yahoo.html?requestedDomain=www.mathworks.com

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*, 60-77. doi:10.1057/jit.2010.4

Zhou R.T. & Lai, R.N. (2009). Herding and information based trading. *Journal of Empirical Finance*, *16*, 388-393. doi:10.1016/j.jempfin.2009.01.004