UNDERSTANDING THE COST ASSOCIATED WITH DATA SECURITY BREACHES

Kholekile L. Gwebu, Associate Professor of Decision Sciences, Peter T. Paul College of Business and Economics, University of New Hampshire, NH, USA, khole.gwebu@unh.edu

Jing Wang, Associate Professor of Decision Sciences, Peter T. Paul College of Business and Economics, University of New Hampshire, NH, USA, jing.wang@unh.edu

Wenjuan Xie, Assistant Professor of Finance, Peter T. Paul College of Business and Economics, University of New Hampshire, NH, USA, wenjuan.xie@unh.edu

Abstract

To estimate the cost of a data breach to the inflicted firm, this study examines the relationship between a breach incident and changes in the inflicted firm's profitability, perceived risk, and the inflicted firms' information environment transparency. Profitability is measured as reported earnings and analysts' earnings forecasts. Perceived risk is measured as reported stock return volatility and dispersion among analysts' forecasts. Although a number of studies have investigated the stock market reaction surrounding the disclosure of a breach incident to quantify the cost associated with breaches, we argue that there exists information uncertainty and deficiency in the disclosure of the breach incident and stock market reaction surrounding a security breach announcement date may not be the best measure for the cost of security breaches. And research using other complementary measures is warranted. Our preliminary finding suggests that data breaches negatively impact firm profitability, perceived risk and information transparency. Nevertheless, the damage of a breach most likely stems from direct costs such as compensation and litigation costs rather than indirect costs such as tarnished reputation and a decrease in market share and sales. More sophisticated analysts are also found to add value in estimating the real cost of a security breach.

Keywords: Data Security Breaches, Financial Impact, Profitability, Risk, Information Transparency.

1 INTRODUCTION

The popular press is replete with high profile data security failures. In some incidents, the breached firms clearly paid a dear price for their data security debacles. For instance, after criminals accessed over 163,000 consumer credit reports, Choicepoint was forced to pay $15 million in penalties and the company's stock price fell from $46.01 to $37.64. However, some press reports suggest that breaches are simply becoming an inevitable part of conducting business and are hence nuisances with inconsequential economic effects on the afflicted firms (Campbell et al. 2003). To quantify the economic costs due to a data security breach, a number of studies have examined the stock market responses to the disclosure of data breaches at publicly traded US corporations. Although some have found evidence that the stock market responds negatively to news of a data security breach (Cavusoglu et al. 2004; Garg et al. 2003), others suggests that the news of such incidents does not necessarily portend a drop in the breached firm's stock price (Campbell et al. 2003; Hovav & D'Arcy 2003).

In addition to societal costs, a data security breach results in both direct and indirect costs for the inflicted firm. Direct costs of data breaches include the cost of damage restitution and litigation. Indirect costs include the increased cost of conducting business, loss of brand image, loss of customer trust, and ultimately a loss in market share and sales. While some costs are easier to quantify, others are not. Information deficiency and uncertainty often plague investors amidst data security breach, given the lengthy delay for the real magnitude of the breach to be known and the general absence of meaningful disclosure about the estimated economic consequences of the breach. This raises the question of whether investors are able to accurately estimate the economic impact of a breach at time of the announcement. Thus, studies using other measures to quantify the economic costs associated with data security breaches are thus warranted.

Therefore, instead of examining the stock market reaction via cumulative abnormal returns surrounding a security breach announcement date, this study examines whether a data security breach would lead to expected changes in profitability (measured as reported earnings and analysts' earnings forecasts), risk (measured as dispersion among analysts' forecasts), and the inflicted firms' information environment (disclosure transparency). The profitability measures capture the impact of a security breach on cash flow due to legal costs and the adverse financial consequences from customers, investors, employees, and business partners. The risk and information environment measures, on the other hand, capture the impact of a security breach on the cost of capital due to new uncertainties with regard to the magnitude and implication of future legal sanction, possible restructuring costs, executive turn over, and changes in the terms with customers and suppliers.

This study differs from prior studies in several important ways. First, given that the real magnitude and economic implication of a data security breach may only be known several months following the breach, it is important to examine the longer term (cumulative change in reported quarterly earnings for the one year following the announced security breach) as well as the immediate (revisions in analysts' quarterly earnings forecast in proximity to the announced security breach) economic consequences of a security breach. Second, this study examines financial analysts' earnings forecast rather than stock market responses. It is reasonable to assume that financial analysts have the potential to compensate for information deficiencies and their forecasts of earnings incorporate information not included in the breach announcement disclosed to the investors. Thus, the use of analysts' forecasts of earnings may add additional value in the estimation of the economic cost associated with data security breaches. Finally, the study argues that a full understanding of the cost associated with security breaches requires the inclusion of the risk measure because when a risky firm incurs higher cost of capital. Given these differences, this research makes two important contributions to the literature on data security breaches. By using complementary dependent variables, this research has the potential to confirm the internal and ecological validity of the findings from prior studies. Second, the use of multiple rather than a single measure will provide a deeper and fuller understanding of the economic damages associated with security breaches.

2 THE LITERATURE AND EMPIRICAL PREDICTION

Losses and damages due to data security breaches are remarkably complex to measure (Acquisti et al. 2006; Kannan et al. 2007). In their effort to help firms quantify such damages, several studies have adopted an event study approach and examined market responses to firms' data security breaches announcements. However, the results are mixed and the losses associated with data security breaches remain unclear.

Telang and Wattel (2007) conduct a study on the disclosure of the vulnerabilities of software and show that software vendors lose around 0.6% of their market value when the vulnerability is reported. Garg et al. (2003) and Goel and Shawky (2009) include a broader category of breaches and observe a statistically significant negative return around the breach event date. Focusing on events involving the potential exposure of confidential data, Acquisti et al. (2006) and Gatzlaff and McCullough (2010) suggest that the overall effect of a data breach on shareholder wealth is negative and statistically significant. Acquisti et al. (2006) also suggest that the cumulative negative effect increases in magnitude over the day following the breach announcement, but then decreases and loses statistical significance. Focusing on internet breaches, Cavusoglu et al. (2004) demonstrate that announcing an Internet security breach is negatively associated with the market value of the announcing firm.

By contrast, Hovav and D'Arcy (2003) examine the stock market's response to denial of service attack announcements and do not find any significant loss in value for the breached firms. Focusing on malicious breaches, Campbell et al. (2003) do not find evidence for an overall negative stock market response to public announcements of information security breaches. However, they do find a highly significant negative market reaction for information security breaches involving unauthorized access to confidential data, but no significant reaction when the breach does not involve confidential information. Focusing on a broad category of breaches, Kannan et al. (2007) suggest that the breached firms do not earn significantly negative long or short term abnormal returns. They also find that during the dot.com era breached firms experienced higher negative short-term abnormal returns. However, investor reactions do not differ between smaller and large firms or between confidentiality, integrity, and availability related breaches.

Unlike other studies, Ko and Dorantes (2006) use a matched-sample comparison analysis to investigate the impact of security breaches on a variety of accounting measures. Similarly, Ko and Dorantes's (2006) study yielded mix results. The adverse impacts of the breach incidents are only observed in some measures (return on asset), but not in others (sales and operating income).

Researchers attribute the conflicting evidence observed to the relatively small sample sizes used in many studies and the diversity of breaches examined by prior studies (Gatzlaff & McCullough, 2010). Indeed, prior studies suggest that the magnitude and direction of the stock price response to the news of data security breaches depends on contextual factors such as the nature of the breach (the severity of the breaches, confidentiality vs. non-confidentiality related breaches), firm characteristics (small vs. large firms, internet vs. brick-and-motor firms), and the incident date (earlier years vs. recent years) (Acquisti et al. 2006; Campbell et al. 2003; Gatzlaff & McCullough, 2010; Hovav & D'Arcy, 2003; Telang, 2007). Given that risk assessment is a fundamental component in establishing data security policies and controls (Hovav & D'Arcy, 2003), these conflicting findings call for more research to provide more comprehensive measurement of the economic consequences and validate whether data security breaches do indeed lead to negative economic consequences for the inflicted firms.

Inferred from past research on the economic impacts of security breaches, we conjecture that a breach incident will negatively impact the inflicted firm's profitability, perceived risk, as well as the perceived information transparency.

H_1. A security breach will have a significant negative effect on the inflicted firm's profitability.

H_2. A security breach will have a significant negative effect on the perceived risk of the inflicted firm from the investors.

H_3. A security breach will have a significant negative effect on the inflicted firm's information transparency.

3 METHODOLOGY AND MEASURES

We draw data from academic publications listing security breach incidents as well as public databases that collect data security breach incident announcements. The initial search yields an initial sample of 5,008 breach incident announcements. Firms that are not included in the Centre for Research in Security Prices and Standards and Poor's COMPUSTAT databases are eliminated from further analyses because these two databases are the primary data sources for stock returns and financial data. In order to define the cumulative profitability change variables, firms are required to have five consecutive quarters of data starting from the quarter during which the data breach announcement is made. This requirement limits our data to 233 announcements. In analyses requiring analysts' earnings forecasts, firm-quarter observations that are not in the Institutional Brokers' Estimation System database, have no revision of earnings forecast from any analyst for the fiscal period within the designated post-breach announcement period are further removed. [1] Additionally, to ensure that the observed changes in analysts' earnings forecasts are related to the data security breach incident rather than other events, announcements with confounding events during the two week period surrounding the announcement date are removed. The final sample size for the analyses requiring only firm financial data (as in Table 1) is 174 breach cases (870 firm-quarter observations). In analyses requiring analysts' earnings forecasts, the final sample is 57 breach announcements with 951 quarterly earnings forecasts in the 90-day period before the breach announcement and 1,049 quarterly earnings forecasts in the 90-day period after the breach announcement.

The first profitability measure is the quarterly cumulative change in total net earnings for the one year period following the announced security breach. For inflicted firm *i*, the cumulative change of quarterly net earnings is the future fourth quarter's net earnings minus the breach announcement's current quarter's net earnings, normalized by the absolute value of the current quarter's net earnings:

$$\Delta NE_i = \left(NE_{i,Q4} - NE_{i,Q0}\right)/|NE_{i,Q0}|$$

The second profitability measure is the quarterly cumulative change in Earnings per Share before Extraordinary Items (EPSFX) for the one year period following the announced security breach: For inflicted firm *i* the cumulative change of quarterly EPSFX is defined as the future fourth quarter's EPSFX minus the breach announcement's current quarter's EPSFX, normalized by the absolute value of the current quarter's EPSFX:

$$\Delta EPSFX_i = \left(EPSFX_{i,Q4} - EPSFX_{i,Q0}\right)/|EPSFX_{i,Q0}|$$

The last profitability measure is financial analysts' cumulative earnings forecast (EPS before Extraordinary Items, corresponding to the previous EPSFX) revisions of the next fiscal quarter in to the 90-day period following the announced security breach: [2] For inflicted firm *i* that has N analysts' research coverage, the cumulative revision of quarter-ahead net earnings forecast is defined as:

$$Forecast\_Revision_i = \sum_{Analyst\ j=1}^{N} \left(EPS\_Forecast_{j,Q1,last} - EPS\_Forecast_{j,Q1,first}\right)$$

To make this measure more comparable across firms, we standardize the cumulative forecast revision by the absolute value of reported earnings.

[1] This treatment is to ensure that the earnings forecast revisions are meaningful. I/B/E/S observations tend to bias towards relatively large companies, and as a result 178 observations out of the 233 are lost in this treatment.

[2] The choice of 90-day period is due to the fact that the quarter-ahead earnings will be announced and there will not be any forecasts after this period. As robustness checks, we also run the same analysis using a 60-day period and a 30-day period. The sample sizes further decrease, but the results are not qualitatively changed.

$$Standardized\_Revision_i = \left[\sum_{Analyst\ j=1}^{N} \left(EPS\_Forecast_{j,Q1,last} - EPS\_Forecast_{j,Q1,first}\right)\right] |EPS_{i,Q1}|$$

Our risk metric is the pre- to post-announcement change in the dispersion of analysts' quarter-ahead earnings forecasts. As in Diether et al. (2002), we take every analyst's last forecast of the current fiscal quarter's EPS in the 90-day period ending on the breach announcement date and define these forecasts' standard deviation to be the pre-announcement dispersion ($Dispersion_{Q0,\ 90\text{-}day\ prior}$). We take every analyst' last forecast of the quarter-ahead earnings in the 90-day period following the breach announcement and define these forecasts' standard deviation to be the post-announcement dispersion ($Dispersion_{Q1,\ 90\text{-}day\ after}$). Both standard deviations are normalized by the respective absolute value of reported earnings. The change in dispersion is defined as the difference between the two dispersions:

$$\Delta Dispersion_i = Dispersion_{Q1,90-day\ after} - Dispersion_{Q0,90-day\ prior}$$

where:

$$Dispersion_{Q1,90-day\ after} = Std.Dev.(EPS\_Forecast_{j,Q1,last})/|EPS_{i,Q1}|$$
$$Dispersion_{Q0,90-day\ prior} = Std.Dev.(EPS\_Forecast_{j,Q0,last})/|EPS_{i,Q0}|$$

The first measure of information transparency is the same as the risk metric. While some financial economists argue that forecast dispersion can serve as a firm risk measure (Johnson 2004), other studies suggest that it is a precise measure of the differences of opinion regarding firm earnings, which mostly reflect the information transparency of the firm (Diether et al. 2002).

The second measure of information transparency is the pre- to post-announcement change in analysts' earnings forecast accuracy: Forecast accuracy is a measure of analysts' experience, capability, and complexity of coverage, as well as the clarity of the firm's information disclosure (Clement 1999). Specifically, we take the analyst that is most active in covering the inflicted firm (the analyst issuing the most number of earnings forecasts) and study the pre- to post-announcement change in her forecast accuracy. Forecast accuracy, similar to the treatment in Clement (1999), is defined as the absolute difference between the last forecast the analyst issues for a fiscal period and the reported earnings for that fiscal period, normalized by the absolute value of the reported earnings. That is, for inflicted firm *i*, assuming the most active analyst is k, the change of accuracy for firm *i* is defined as:

$$\Delta Accuracy_i = ForecastError_{Q1,90-day\ after} - ForecastError_{Q0,90-day\ prior}$$

where:

$$ForecastError_{Q1,90-day\ after} = |NE\_Forecast_{k,Q1,last} - NE_{i,Q1}|/|NE_{i,Q1}|$$
$$ForecastError_{Q0,90-day\ prior} = |NE\_Forecast_{k,Q0,last} - NE_{i,Q0}|/|NE_{i,Q0}|$$

4 PRELIMINARY FINDINGS AND DISCUSSION

In Table 1, we provide the descriptive statistics of the final sample of 174 breach cases, 870 firm-quarter observations. We summarize the following two groups of variables in two separate panels: Panel A presents firm-specific variables (which include control variables to be employed in regression analyses to follow) and Panel B presents breach incident-specific variables.

We observe that the average firm in our sample has a book total asset of $109 billion, book total equity of $22 billion, market value of total equity of $27 billion, and in the quarter during which the breach incident is publicly announced a net earnings of $404 million. In addition, on a per share diluted basis,

net quarterly earnings excluding extraordinary items is $0.51, and earnings including extraordinary items is $0.55. [3]

Variable	Unit	N	Mean	Std. Dev.	Min.	1st Quartile	Median	3rd Quartile	Max
Total Assets	$Billion	174	108.7	366.7	0.03	2.0	8.9	44.3	2364.5
Total Book Equity	$Billion	67	21.7	43.2	-3.6	0.7	2.8	15.5	233.2
Total Market Value of Equity	$Billion	143	26.7	56.8	0.006	1.4	5.5	24.1	393.0
Total Long-Term Debt	$Billion	169	18.5	64.9	0.00	0.2	1.8	7.5	490.1
Total Cash	$Billion	128	2.0	4.0	0.00	0.1	0.3	1.6	25.7
Current Quarter Total Net Earnings	$Billion	174	0.4	1.0	-2.8	0.01	0.1	0.3	5.0
Current Quarter EPS before Extraordinary Items	$	174	0.51	1.00	-2.40	0.15	0.36	0.71	7.31
Current Quarter EPS including Extraordinary Items	$	174	0.55	1.02	-2.40	0.17	0.37	0.74	7.31

Table 1. Descriptive Statistics - Panel A: Firm Characteristics

Variable	Unit	N	Mean	Std. Dev.	Min.	1st Quartile	Median	3rd Quartile	Max
Time lag from customer notification to public announcement	# days	174	7.76	34.65	-8	0	0	1	364
Severity (# of transaction records breached in an incident)	# Records	80	151642.29	958103	1.00	121	1500	21000	8500000
Dummy variable: Malicious (accident 0; malicious attack1)	1 or 0	174	0.60	0.49	0	0	1	1	1
Dummy variable: Sensitivity (confidential data 1 otherwise 0)	1 or 0	174	0.89	0.32	0.00	1.00	1.00	1.00	1.00

Table 1 Descriptive Statistics - Panel B: Breach Characteristics

[3] In describing the smaller sample (57 cases) with the analyst earnings forecast requirement, we find little qualitative difference in variables between this smaller sample and the final sample as in Table 2, except the smaller sample have larger firm size in terms of total assets and market value.

We further conduct univariate analyses on each of the aforementioned measures to examine our empirical predictions. Table 2 presents the three profitability measures. First, as the first column suggests, we find that on average, the cumulative change in net earnings including extraordinary items in the four quarters following a breach announcement is a 22.54% decrease, indicating deteriorated earnings performance. The distribution of the cumulative change is rather symmetric, with the median value being exactly 0%. With a very large standard deviation within the 174 cases, a two-tail test yields a t-statistic of -0.43 and fails to reject the null hypothesis that there is no change from the breach current quarter to four quarters following the breach announcement. As an interesting contrast, in the second column we present the cumulative change in net earnings excluding extraordinary items in the four quarters following a breach announcement and find an average 87.84% increase. The distribution of this change variable is heavily skewed towards the positive end and the t-statistic, though lacking statistical significance, is a more pronounced 1.05. The different findings from these two columns suggest that although a breach does impose a financial expense to the inflicted firms, the cost of a security breach most likely stems from the direct cost including damage compensation and litigation rather than indirect cost including cost due to damaged reputation, reduced market share, and sales etc.. This is because damage compensation and litigation are normally categorized as extraordinary items and when the extraordinary expenses are excluded, the cumulative change in net earnings actually increased, albeit not statistically significant.

The last column of Table 2 is the cumulative analyst revision of their earnings forecasts about the inflicted firms for the following quarter. We document an average of 15.26% increase in forecast revisions, though statistically insignificant, which indicate a slightly increased optimism among analysts regarding the inflicted firms' post-breach earnings performance. This phenomenon may have two explanations. First, analysts' forecast is more about the "street earnings" number that excludes extraordinary items and focuses on the main line of business that generates revenue. Thus consistent with the findings from the cumulative change in net earnings, the upward revisions from the analysts suggest that they in general do not believe that a security breach will impact the breached firm's main line of business. In other words, they do not believe that a security breach will lead to indirect cost including damaged reputation, decreased sales and market share etc. Second, the company's acknowledgement of breach and offered means to mitigate the effect of breach actually result in an improved confidence in the company's future earnings performance.

Measure	Cumulative Change in Net Earnings	Cumulative Change in Earnings before Extraordinary Items	Financial Analysts' Cumulative Earnings Forecast Revision
N of obs.	174	174	57
Mean	-22.54%	87.84%	15.26%
Std. Dev.	695.98%	1100.24%	380.91%
Min.	-7501.35%	-3411.11%	-1400.00%
1st Quartile	-46.74%	-38.24%	-17.00%
Median	0.00%	5.57%	23.00%
3rd Quartile	43.70%	48.15%	70.00%
Max	2800.00%	13300.00%	1354.00%
t-statistics of Two-tail test	-0.43	1.05	0.30

Table 2. Profitability Measures: All three measures are standardized by the current quarter respective earnings

Table 3 combines the risk measure and information transparency measure and presents the change in analysts' earnings forecast dispersion and accuracy. As argued previously, the dispersion of forecasts may represent the business risk of a firm as well as the quality and transparency of information that the firm provides. In the first column, we observe a statistically significant increase in forecast dispersion

from the 90-day period prior to the breach announcement to the 90-day period after the announcement. On average, the post-breach dispersion is 19.14% larger as a percentage of the actual earnings, illustrating a higher business risk perceived by professional investors (represented by analysts) or a less transparent information environment due to the chain effect following a breach or the lack of agreement regarding the scale, severity and influence of the breach incident itself.

As we compare the pre-breach and post-breach forecast error of the most active analysts following an inflicted firm, expertise and personal experience are naturally controlled for, and the comparison of forecast error is directly related with the most active analysts' perception and interpretation of the signals regarding the inflicted firm's earnings. We document that while the overall information seems less transparent after the data breach announcement and hence more disagreement among analysts, the most active analyst seems to be able to detect more accurate information regarding the inflicted firm's earnings and thus able to reduce his forecast error in the post-breach announcement period. An average of 13.30% reduction in the forecast error from the 90-day period prior to the breach announcement to the 90-day period after the announcement is observed. This finding of improved accuracy from the most active analyst, together with the deteriorated information transparency, poses a conjecture that breach announcement may conveys more uncertainty and invites more diverse interpretation of the breach's impact on earnings, but it also contains specific information regarding the scale of the impact on earnings that only analysts who actively follow the company and have expertise in understanding the cost of the breach incident can decipher and incorporate to improve their forecast accuracy. In other words, more sophisticated analysts have the potential to add value in estimating the real cost of a data security breach.

Measure	Change in Financial Analysts' Quarterly Earnings Forecast Dispersion	Change in Financial Analysts' Quarterly Earnings Forecast Accuracy
N of obs.	51	57
Mean	19.14%	-13.30%
Std. Dev.	73.50%	68.43%
Min.	0.00%	-450.00%
1st Quartile	1.78%	-12.02%
Median	4.45%	-4.30%
3rd Quartile	7.80%	2.62%
Max	522.81%	196.79%
t-statistics of Two-tail test	1.86	-1.47

Table 3. Risk and Information Transparency Measures: The original dispersion and accuracy variables used to construct both measures are standardized by corresponding earnings.

5 CONCLUSIONS

To this end, this research yields several interesting and encouraging findings. First, confirming the findings of some prior studies, our preliminary univariate analyses illustrate multiple evidence of the negative effect breach incidents have on profitability, risk and information transparency. However, the employment of multiple measures enables a fuller and richer understanding on the economic implication of data security breach incidents. Specifically, the financial damage of a data security breach mostly likely stems from direct cost including damage compensation and litigation rather than indirect costs including tarnished reputation, decreased sales and market share etc. Second, in addition

to its direct cost, data security breaches also negatively impact the perceived risk of the breached firm and the transparency of the firm's information disclosure environment. Finally, more sophisticated analysts have the potential to add value in estimating the real cost of a data security breach. Despite these intriguing findings, future research could consider (1) comparing all profitability, risk and information environment measures with the industry median value and (2) running regressions that attempt to explain the direction and scale of profitability and risk change by the attributes of the firm, analysts, and the data breach incidents.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. Paper presented at the Proceedings of the 27th International Conference on Information Systems,

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.

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), 69-104.

Clement, Michael B. (1999). Analyst forecast accuracy: Do ability, resources, and portfolio complexity matter? Journal of Accounting and Economics, vol. 27, 285-303.

Diether, Karl B., Christopher J. Malloy, and Anna Scherbina (2002). Difference of Opinion and the Cross-Section of Stock Returns, Journal of Finance, vol. 57, 2113–2141.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. Information Management & Computer Security, 11(2), 74.

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

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. Information & Management, 46(7), 404-410. doi:10.1016/j.im.2009.06.005.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. Risk Management & Insurance Review, 6(2), 97-121. doi:10.1046/J.1098-1616.2003.026.x.

Johnson, Timothy C. (2004). Forecast Dispersion and the Cross-Section of Expected Returns, Journal of Finance, vol. 59, 1957–1978.

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. doi:10.2753/JEC1086-4415120103.

Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. Journal of Information Technology Management, 14, 13-22.

Telang, R., Wattel, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. IEEE Transactions on Software Engineering, 33(8), 544-557.