Winter 12-10-2016

Financial Performance Impacts of Information Security Breaches

Atiya Avery
University of Illinois at Chicago, aavery3@uic.edu

C Ranganathan
University of Illinois at Chicago, ranga@uic.edu

Financial Performance Impacts of Information Security Breaches

Completed Research

Atiya Avery
University of Illinois at Chicago,
Department of Information Systems and Decisions Sciences
aavery3@uic.edu

Ranganathan Chandraskaren
University of Illinois at Chicago,
Department of Information Systems and Decisions Sciences
ranga@uic.edu

ABSTRACT

Previous research has found that information security breaches can impact the market value of the firm because the reputation of the firm has suffered and the market assumes that revenues will decrease and expenses will increase. This impact to market value is usually measured within the 1-2 days after an information security breach disclosure where after things seemingly return to normal, in the context of stock market values. Despite the widely held belief that information security breaches have negative short-term and long-term impacts, researchers are just beginning to understand the relationship to short-term and long-term firm performance. This study investigates the short-term and long-term impacts of information security breaches on firm performance in the first four quarters following an information security breach disclosure. We take both a traditional view and organizational sustainability/resiliency view to hypothesis and theory development and introduce the analysis of two new variables "intangible assets" and "extraordinary losses" to the discussion on the impact of information security breaches to firm performance. We discuss our findings and their implications for practitioners and researchers and suggest next steps.

Keywords: Information Security, Organizational Resiliency, Financial Performance, Data Breach

INTRODUCTION

Despite the widely held belief that information security breaches have negative long-term and short-term impacts to a firm's financial performance, academic researchers are still seeking to better understand the link to both short-term and long-term firm performance. A good portion of extant research on this topic has focused on capturing the short-term impacts of breaches to organizational performance measures such as the market value of the firm. In the market value context, the hypothesis is that stock price changes in the days following a breach disclosure will capture the assessment of a large body of shareholders to the breach event, and would therefore be reflected in the stock price changes following the disclosure about the breach. These effects have typically been measured and captured within 1-3 days after a breach disclosure and some effects have been seen for up to 25 days after a breach disclosure (see Cavusoglu et al. 2004; Chen et al. 2012; Garg et al. 2003; Hovav & D'Arcy, 2003). There is limited research on the more long-term impacts of information security breaches on the firm as measured by changes in the firm's quarterly and annual financial performance with mixed results (Ko & Dorantes, 2006; Zafar et al., 2012; Ko et al., 2009).

Thus far, most of the extant the literature treats the breach event and its consequences as perpetually negative, value declining to the organization. We do know that the impacts of information security breaches on organizations are not equal. For example, firms such as Home Depot, T-Mobile and Anthem have not only recovered after an information security breach but have thrived whereas Target as of 2016 has continued to post periodic performance declines (Associated Press, 2014; Osborne & Day, 2015;McGinty, 2015; T-Mobile, 2016; Legere,John, 2015). It is becoming increasingly obvious that just because an information security breach has

occurred that does not necessarily mean that a negative financial outcome has to occur for the organization.

This study investigates the short-term and long-term financial performance of firms after a public information security breach disclosure. We advance two contrasting theoretical propositions to examine the financial impacts of information security breaches. The first proposition follows from the traditional literature on information security economics that views information security breaches as perpetually value declining to an organization. The second, contrasting proposition follows from studies on crisis management and organizational resiliency. Here, we argue that information security breaches can be construed as an opportunity to build organizational resiliency and thus breaches can serve as potential catalyst to improve long-term financial performance. We integrate the traditional economic perspective and the resiliency views to examine changes in common firm financial performance measures in the short-term and long-term following an information security breach event.

We seek to make three important contributions to literature on information security breaches. First, unlike many prior studies, we examine both short term (first quarter after the breach) and long-term impacts (2-4 quarters after the breach) of breaches on financial performance. Second, we extend the extant literature by throwing light on two critical measures of financial performance viz. "intangible assets" and "extraordinary losses". Changes to intangible assets will allow us to gauge the impact of the information security breaches on the firm brand reputation and intellectual capital reserves. The measurement of changes to extraordinary losses allows us to better understand if the breached firms considered information security breaches truly detrimental to their operations, in that associated losses and expenses rose to the level of "extraordinary" and not an event that was easily incorporated into routine operational expenses.

The standard measures of firm performance via common cost and profit ratios are utilized just as with previous research. Third, our efforts advance theory development in this domain as we bring forth the notion of organizational resiliency to understand the long-term financial performance impacts of security breaches. We believe the organizational resiliency lens, when complemented by the traditional economic lens, will provide a better understanding of how breaches impact the financial performance of firms.

In the following sections, we discuss the literature review, theoretical framework, and hypothesis. This is followed by a discussion on our research methodology including our matched sample selection technique and statistical analysis. We follow this by our results and discussion. We conclude with next steps and limitations.

LITERATURE REVIEW

Event study methodology has been a popular method to evaluate the impacts of information security breaches on organizations. The general findings from the literature regarding the impact of information security breaches to organizations are that they are negative value declining events ; especially in the context of market value measures, such as stock prices. Research in this area spans the period from about 2003 to the present. In a comprehensive review of prior studies, Spanos and Angelis (2016) identified 37 research studies that have assessed the impacts of security information security breaches on firms; 25 of these studies reported negative stock market impacts; 7 indicated neutral reactions and 5 found positive impacts to the breached firm. Despite the large number of studies that adopt a market-value approach using an event study methodology to assess economic consequences of information security breaches, there are limitations to this method. Event studies are intended to capture investor reactions and their assessment of the event, rather than the true financial impact of a breach. Also, the small window sizes typically utilized by event studies do not capture impacts over a longer duration. As an

alternate to event study approaches, some researchers have used more long-term measures of firm financial performance, which include evaluating changes to the breached firms profits and costs. A summary of published literature in this area is presented in Table.1. Following this stream, we also use more traditional accounting-based measures to assess the short and long term financial impacts of information security breaches. We believe measures derived from the financial statements and the ensuing analysis allows us a better understanding of the potential recovery processes for firms after an information security breaches; as well as insights into what may have occurred before and during the information security breach event. This is an important, unbiased, source of information on the true impacts of information security breaches disclosures to organizations.

Collectively, the literature review suggests the following. (1) There seems to be significant gaps in our understanding of the true financial impacts of information security breaches on organizations (2) There are very few studies in recent years that have examined the short term and long term impacts of information security breaches. (3) There is only limited insights into how organizations recover and rebound from information security breaches in order to improve their overall financial performance. Our study is intended to address the aforementioned gaps.

DEVELOPMENT OF HYPOTHESES

Ko & Dorantes (2006, p 14-15.) posit that the impacts of information security breaches can be classified as short-term impacts or long-term impacts. Examples of short-term impacts include costs of repairs. Long-term impacts include the loss of existing customers, and legal liabilities and payment of damages to injured third parties. These losses are likely to be reflected in the firm performance measures as a decrease in profits and an increase in costs.

Table.1. Studies that examine financial performance impacts of information security breaches

Ko & Dorantes 2006	What is the impact of information security breaches on firm financial performance?	This study utilizes firm financial performance to evaluate the impact of information security breaches to 19 publicly traded companies in the four quarters following a information security breaches disclosure.
Table.1. Continued.		
Ko et al 2009	What is the impact of information security breaches on organizational performance?	This study evaluates the impact of information security breach on firm financial performance utilizing three performance ratios including ROA, ROS, and COGS/S. Utilizing information security breaches from 1997-2004 the researchers found that breached firms experienced long-term negative impacts to organizational performance following an information security breach.
Zafar et al 2012	What is the impact of information security breaches on the competitors of breached firms?	This study evaluates the impact of information security breaches from 1997-2004 for 69 breached firms who on average had approximately 422 competitor firms. The researchers found evidence of network effects particularly for firms in the technology industry.

Profit Measures We use three common measures from the literature; to assess the firm's profitability these measures are Return on Sales (ROS), Return on Assets (ROA) and Changes to Sales (Ravichandran & Lertwongsatien, 2005; Santhanam & Hartono, 2003). We utilize two alternate measures of ROS and ROA; substituting operating income for net income to better gauge if there were any negative impacts to the firms operations.

- **Hypothesis 1A:** Breached firms will experience a decrease in return on owner's assets in the short-term and long-term.
- **Hypothesis 1B:** Breached firms will experience a decrease in return on owner's assets as measured by operating income, following an information security breach event.
- **Hypothesis 2A:** Breached firms will experience a decrease in return on sales in the short-term and long-term following an information security breach event.
- **Hypothesis 2B**: Breached firms will experience a decrease in return on sales in the short-term and long-term as measured by operating income, following an information security breach event.

- **Hypothesis 3**: Breached firms will experience a decrease in sales in the short-term and long-term following an information security breach event.

Costs Measures: We utilize two cost ratios from the literature. These measures are costs of goods sold over sales and the operating ratio (Santhanam & Hartono, 2003; Hitt & Brynjolfsson, 1996). We devise the following three hypotheses:

- **Hypothesis 4:** Breached firms will experience an increase in the costs of goods sold ratio in the short-term and long-term following an information security breach event.

- **Hypothesis 5:** Breached firms will experience an increase in the operating ratio in the short-term and long-term following an information security breach event.

Intangible Assets: Intangible assets includes items such as patents, trademarks, copyrights, business methodologies, goodwill and brand recognition (Gibson 2007, pg 492). Tsoukas (1999) posits that crises negatively impact the ability of an organization to formulate an influential voice and thus its symbolic power is reduced A information security breach is likely to affect the firm's goodwill, brand reputation and intellecutal property reserves in both the short-term and long-term. We present the following hypothesis.

- **Hypothesis 6:** Breached firms will experience a decrease in the value of their intangible assets in the short-term and long-term following an information security breach event.

Extraordinary Losses:. The measurement of extraordinary losses allows us to better understand if the focal firms considered information security breaches truly detrimental to their operations that it rose to the level of "extraordinary" and not an event that was easily incorporated into its usual operating expenses. We present the following hypothesis:

- **Hypothesis 7:** Breached firms will incur an increase in extraordinary loss expenses in the short- term and long-term following an information security breach event.

Sustainability and Organizational Resiliency: All organizations are prone to crises event with some organizations declining after a crises and others becoming sustainable and resilient(Mishra, 1996;Bunderson & Sutcliffe, 2002). Our organizational resiliency view relies on the notion that firm investments due to information security breaches if managed correctly have the ability to become resources that may allow the firm to attain long-term advantages. The firm may also develop capabilities over and above peer firms that did not have an information security breach event thereby surpassing that firm in terms of performance. We develop the following hypotheses:

- **Hypotheses 8A & 8B**: Short-term costs will increase within the firm and short-term profitability will decrease within the firm and between peer firms following an information security breach event.

- **Hypotheses 9A & 9B:** In the short-term, sales, and intangible assets will decrease within the firm and between peer firms following an information security breach event.

As breached firms expend additional resources on the information security breaches event organizational capabilities become enhanced allowing the firm to not only recover and return to sustainability but also to be resilient.

- **Hypothesis 10:** Long-term profitability will remain the same or increase within the firm and between peer firms following an information security breach event.

RESEARCH METHODOLOGY

Identification Strategy: We utilize matched paired comparative analysis as our research method. This method is considered a type of quasi-experimental method. Essentially, this method relies on an identification strategy in which a carefully selected and matched treatment and control group is derived and then differences within and between the treatment and control

groups are statistically tested to isolate the impact of the treatment; if any. According to Morgan and Winship,2007, pg 87, “"Matching represents an intuitive method for addressing causal questions, primarily because it pushes the analyst to confront the process of causal exposure as well as the limitations of available data”. In the information systems research domain matched paired comparative analysis has been utilized by Santhanm et al 2003 and Bharadwaj 2000, to study the impacts of IT capability on firm performance and more recently by Zafar et al 2012, to study the impacts of information security breaches on competitor firms.

Treatment and Control Group: We use the data from the Privacy Rights Clearinghouse, which is a California based nonprofit organization that tracks and compiles information security breaches event disclosures from multiple sources. The dataset from Privacy Rights Clearinghouse has been utilized to study information security breaches by Gatzlaff & McCullough, 2010; Goel & Shawky, 2014; Pirounias et al. 2014, among others. To derive our sample of treatment and control groups we utilize the matching technique for firms as previously outlined by Ko & Dorantes, 2006; Zafar et al. 2012; Bharadwaj, 2000; Balakrishnan et al 1996; Barber & Lyon, 1996. We matched our treatment group against firms that were within 30%+- for sales, total assets, and employees in the year prior to the information security breaches event i.e. T-1 based on either the 2, 3, or 4 digit NAIC Code. This left us with a sample of 47 breached firms that we considered our final sample for the treatment group and 47 non-breached firms that we considered our final sample for the control group. Both the T-test and the Wilcoxon sign-rank test indicate that the differences between the treatment firms and the control firms across all three matching variables are not statistically significantly different from 0.

Dependent Variables: Our dependent variables for hypothesizes testing consist of quarterly financial data from COMPUSTAT. For each breached firm in the dataset we first determined the

fiscal year and quarter that the information security breaches occurred and we denoted this period at T0. We then matched the control firm against the breached firms taking into account that the breached firm and the control firms may have different fiscal year start dates. We then collected data for each firm 4 quarters after the breach and 4 quarters before the breach. We measure within firm differences and between firm differences in both the short-term and long-term. We define short -term impacts as effects occurring within one quarter after an information security breach. Effects occurring in any two consecutive quarters or more are considered to be long-term effects.

RESULTS AND DISCUSSION

Results:. Within firm differences are evaluated utilizing a 1-tailed T-Test since we are testing directionality and between firm differences are evaluated utilizing a 2- tailed- T-test since we are testing whether or not the differences between the treatment and control group are statistically significant from 0, regardless of directionality. In addition, the P-value of the Wilcoxon sign-rank test represents whether the tested differences are statistically significant from 0 regardless of directionality. Tables 3-5 provide the mean and median differences within the breached firm, the non-breached firms, and between the breached and non-breached firms as well as the statistical significance of the result. Table 6 provides a summary of the hypothesis testing.

	Quarter 1 *Short Term Impacts	Mean	Median	T	Z
Diff Return on Assets	NonBreachedFirms	-0.005	0.006	-0.736	0.884
	BreachedFirms	-0.009	0.000	-1.3347*	-0.481
	Between	-0.002	-0.002	-0.210	-0.968
Diff Return on Assets(OpsInc)	NonBreachedFirms	-0.002	0.005	-0.386	0.270
	BreachedFirms	0.006	0.000	0.265	-0.164
	Between	0.001	-0.005	0.201	-0.799
Diff Return on Sales	NonBreachedFirms	-0.029	0.009	-0.987	1.090
	BreachedFirms	0.037	0.000	-1.032	-0.413
	Between	0.008	-0.001	0.220	-0.561
Diff Return on Sales(OpsInc)	NonBreachedFirms	-0.018	0.005	-0.703	0.640
	BreachedFirms	0.006	0.000	0.489	-0.101
	Between	0.013	-0.005	0.493	-0.577
Diff COGS to Sales Ratio	NonBreachedFirms	-0.003	-0.003	-0.158	-0.148
	BreachedFirms	-0.012	-0.001	-0.118	-0.720
	Between	-0.038	-0.001	-1.185	-0.603
Diff Operating Ratio	NonBreachedFirms	0.022	-0.005	0.675	-0.370
	BreachedFirms	-0.005	0.002	-0.430	0.233
	Between	-0.034	0.005	-1.068	0.222
Intangible Assets % Change	NonBreachedFirms	96.693	99.968	-0.966	-0.141
	BreachedFirms	114.242	100.501	1.337	1.754*
	Between	186.538	99.667	1.730	0.882
Diff Extraordinary Losses	NonBreachedFirms	-0.287	0.000	-0.246	0.905
	BreachedFirms	-0.245	0.000	-0.357	-1.301
	Between	-0.934	0.000	-0.707	-1.225
Sales % Change	NonBreachedFirms	104.212	103.248	1.319	1.989**
	BreachedFirms	105.168	104.240	2.675	2.804***
	Between	105.530	98.465	1.023	0.085

p<.10; p<.05**, p<.01***
T-Test is for hypothesized directionality represented by column "T"
Wilcoxon Sign Rank tests that Ho!=0 represented by column "Z"

Table 2- Quarter 1 (Short-Term) Results

	Quarter 2	Mean	Median	T	Z
Diff Return on Assets	NonBreachedFirms	-0.001	0.001	-0.251	0.810
	BreachedFirms	0.000	0.000	0.034	0.503
	Between	0.003	0.000	0.598	-0.407
Diff Return on Assets(OpsInc)	NonBreachedFirms	-0.002	0.002	-0.551	0.333
	BreachedFirms	0.001	0.001	0.674	0.799
	Between	0.007	0.005	1.297	-0.037
Diff Return on Sales	NonBreachedFirms	0.003	0.002	0.244	,222
	BreachedFirms	0.004	-0.001	0.388	0.582
	Between	0.012	-0.004	0.439	-0.423
Diff Return on Sales(OpsInc)	NonBreachedFirms	0.002	0.004	0.135	0.249
	BreachedFirms	0.011	0.001	0.873	0.899
	Between	0.027	0.000	0.956	0.233
Diff COGS to Sales Ratio	NonBreachedFirms	0.023	-0.004	1.236	-0.201
	BreachedFirms	-0.020	0.004	-1.466	-0.889
	Between	-0.025	-0.004	-0.884	-0.466
Diff Operating Ratio	NonBreachedFirms	0.017	-0.001	0.818	0.413
	BreachedFirms	-0.028	-0.005	-1.494	-1.365
	Between	-0.021	0.009	-0.789	0.317
Intangible Assets % Change	NonBreachedFirms	104.897	100.791	1.422	1.709**
	BreachedFirms	117.612	106.438	1.306	2.041**
	Between	176.692	81.482	1.374	0.694
Diff Extraordinary Losses	NonBreachedFirms	-0.709	0.000	-1.218	-0.097
	BreachedFirms	-0.281	0.000	-0.749	-0.916
	Between	0.420	0.000	1.077	0.097
Sales % Change	NonBreachedFirms	107.789	104.905	3.091	2.868***
	BreachedFirms	105.426	107.992	1.553	2.656***
	Between	104.445	100.208	0.803	0.603

p<.10; p<.05**, p<.01***
T-Test is for hypothesized directionality represented by column "T"
Wilcoxon Sign Rank tests that Ho!=0 represented by column "Z"

Table 3- Quarter 2 Results

	Quarter 3	Mean	Median	T	Z
Diff Return on Assets	NonBreachedFirms	-0.007	0.000	-0.538	-0.566
	BreachedFirms	-0.003	0.000	-1.227	-0.397
	Between	0.000	0.000	0.007	-0.164
Diff Return on Assets(OpsInc)	NonBreachedFirms	0.003	0.004	0.380	-0.608
	BreachedFirms	-0.005	-0.004	-1.7598**	-1.169
	Between	-0.002	-0.003	-0.289	-0.037
Diff Return on Sales	NonBreachedFirms	-0.069	0.002	-0.862	-0.011
	BreachedFirms	-0.007	0.002	-0.551	-0.423
	Between	0.031	-0.008	0.905	-0.476
Diff Return on Sales(OpsInc)	NonBreachedFirms	0.013	0.004	0.395	-0.317
	BreachedFirms	-0.012	-0.004	-1.032	-0.772
	Between	0.008	-0.003	0.371	0.159
Diff COGS to Sales Ratio	NonBreachedFirms	0.002	-0.001	0.138	-0.042
	BreachedFirms	0.005	0.003	0.196	0.698
	Between	-0.048	-0.029	-1.512	-1.312
Diff Operating Ratio	NonBreachedFirms	-0.039	-0.004	-1.079	-0.159
	BreachedFirms	0.010	0.004	0.334	0.751
	Between	-0.022	0.003	-0.798	-0.021
Intangible Assets % Change	NonBreachedFirms	109.666	100.467	1.418	1.431
	BreachedFirms	123.519	104.684	0.064	1.769**
	Between	180.872	76.030	1.445	0.502
Diff Extraordinary Losses	NonBreachedFirms	-3.058	0.000	-1.475	0.178
	BreachedFirms	-10.338	0.000	-1.017	-0.998
	Between	0.314	0.000	0.982	-0.859
Sales % Change	NonBreachedFirms	131.907	108.824	1.433	2.773***
	BreachedFirms	105.159	104.246	1.345	2.206**
	Between	100.283	94.464	0.057	0.021

p<.10; p<.05**, p<.01***
T-Test is for hypothesized directionality represented by column "T"
Wilcoxon Sign Rank tests that Ho!=0 represented by column "Z"

Table 4- Quarter 3 Results

	Quarter 4	Mean	Median	T	Z
Diff Return on Assets	NonBreachedFirms	-0.016	0.000	-1.208	-1.251
	BreachedFirms	0.000	0.000	-0.071	-0.693
	Between	0.018	0.000	1.312	0.704
Diff Return on Assets(OpsInc)	NonBreachedFirms	-0.002	0.001	-0.766	-0.180
	BreachedFirms	-0.005	-0.001	-1.787	-1.191
	Between	0.004	0.007	1.045	0.799
Diff Return on Sales	NonBreachedFirms	-0.044	0.000	-1.031	-0.587
	BreachedFirms	0.008	-0.001	0.324	-0.587
	Between	0.075	0.001	1.555	1.143
Diff Return on Sales(OpsInc)	NonBreachedFirms	-0.002	0.001	-0.178	0.217
	BreachedFirms	-0.016	-0.001	-1.4047*	-0.937
	Between	0.026	0.007	1.099	0.921
Diff COGS to Sales Ratio	NonBreachedFirms	0.007	0.000	0.319	0.058
	BreachedFirms	-0.034	0.000	-1.350	0.005
	Between	-0.046	0.000	-1.264	-0.593
Diff Operating Ratio	NonBreachedFirms	0.019	0.000	0.574	0.122
	BreachedFirms	-0.051	0.000	-1.602	-0.524
	Between	-0.041	-0.005	-1.085	-0.698
Intangible Assets % Change	NonBreachedFirms	116.220	100.806	1.341	1.361
	BreachedFirms	144.399	114.574	2.349	2.769***
	Between	198.702	83.013	1.783	1.005
Diff Extraordinary Losses	NonBreachedFirms	-1.397	0.000	-1.652	-0.371
	BreachedFirms	-2.154	0.000	-1.135	-0.869
	Between	0.334	0.000	0.956	-0.414
Sales % Change	NonBreachedFirms	112.444	111.444	2.340	2.524**
	BreachedFirms	104.799	108.157	1.063	0.085
	Between	103.840	100.661	0.582	0.519

p<.10; p<.05**, p<.01***
T-Test is for hypothesized directionality represented by column "T"
Wilcoxon Sign Rank tests that Ho!=0 represented by column "Z"

Table 5- Quarter 4 Results

Hypothesis Testing Results	
Profit Measurements	
Hypothesis 1A	Partial Support
Hypothesis 1B	Partial Support
Hypothesis 2A	No Evidence
Hypothesis 2B	No Evidence
Hypothesis 3	Reject Hypothesis
Cost Measurements	
Hypothesis 4	No Evidence
Hypothesis 5	No Evidence
Other Internal Measures	
Hypothesis 6	Reject Hypothesis
Hypothesis 7	No Evidence
Sustainability and Resiliency	
Hypothesis 8	Partial Support
Hypothesis 9	Reject Hypothesis
Hypothesis 10	Partial Support

Table 6- Results of Hypothesis Testing

Discussion: Generally speaking, we find the traditional view that information security events are value declining to the breached firms to be false for our sample. Surprisingly, breached firms experienced a statistically significant short-term increase in sales compared with a similar period in the previous year and experienced both short term and long term increases in intangible assets. There is no evidence to suggest that breached firms experience changes to their extraordinary loss expenses in the short-term or long-term that are statistically significant from its prior performance and relative to the control group. This suggests to us that information security breaches do not rise to the threshold of being considered "extraordinary", nonrecurring events to the breached firms.

Our organizational sustainability and resiliency view takes the position that information security breaches have the possibility to lead to organizational sustainability and eventually

organizational resiliency, where resiliency would be characterized by enhanced firm performance relative to the previous year within the firm and relative to the peer non-breached firm. In general, we find that firms are financially sustainable but are not financially resilient.

Conclusion

Limitations and Next Steps: This study has a number of limitations that will enable future studies. First, our sample size is small relative to its potential. Second, our measures of short-term and long-term performance measures are derived from the limited but existing literature on the impacts of breaches to firm performance and may need to be adjusted. Third, firm financial performance ratios that measure costs and especially profits can be considered generic measures of firm performance. Publicly traded companies exist for the sole purpose of meeting shareholder goals and will make resource allocations to that effect, regardless of what may actually be occurring within the firm. In future research, we will need to conduct a deeper analysis of the firm's financial statements to understand what may be occurring before, during, and after a information security breaches event. This also leads us to the notion that measuring and assessing operations performance, and measuring and assessing financial performance utilizing the firm's financial statements can be considered two very unique research paradigms. At the moment, the literature equates firm financial performance to firm operation's performance. This perspective will need to be untangled if we are to study the impacts of information security breaches on firms. Fourth, it is possible that breached firms were able to maintain equilibrium because of the network effects of the information security breaches event on similar firms within that industry. The literature has previously documented networks effects (see Hinz, Nofer, Schiereck, & Trillig, 2015;Zafar et al, 2012, Ettredge & Richardson, 2003) . Fifth of special

interest are the dramatic changes to firm's intangible assets, this needs to be explored more and may be due to a number of recent phenomena.

WORK CITED

Anson, W. (2015, February 11). Alternate approaches to the valuation of intellectual property. *IP Watchdog*.

Associated Press. (2014, November 18). Home Depot profit rises despite data breach. *Los Angeles Times*.

Balakrishnan, R., Linsmeier, T., & Venkatachalam, M. (1996). Financial benefits from JIT adoption: effects of customer concentration and cost structure. *The Accounting Review*, 183-205.

Barber, B., & Lyon, J. (1996). Detecting abornormal operating performance: The empirical power and specification of test statistics. *Journal of Financial Economics*, 359-399.

Barney, J. (1991). Firms resources and sustained competitive advantages. *Journal of management, 17*(1), 99-120.

Bharadwaj, A. (2000). A resource based perspective on information technology capability and firm performance: An empirical investigation. *Management Information Systems Quarterly*, 169-197.

Bunderson, J. S., & Sutcliffe, K. M. (2002). Comparing alternative conceptualizations of functional diversity in management teams: Process and performance effects. *Academy of Management Journal, 45*(5), 875-893.

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.

Chen, J. V., Li, H. C., Yen, D. C., & & Bata, K. V. (2012). Did IT consulting firms gain when their clients were breached? *Computers in Human Behavior, 28*(2), 456-464.

Ettredge, M. L., & Richardson, V. J. (2003). Information transfer among internet firms: the case of hacker attacks. . *Journal of Information Systems*, 71-82.

Gandel, S. (2015, January 23). Lloyd's CEO: Cyber attacks cost companies $400 billion every year. *Fortune*.

Garg, A., Curtis, J., & & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security,, 11*(2), 74-83.

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

Gibson, C. (2007). *Financial reporting and analysis 10th Edition.* Mason, OH: Thompson Higher Education.

Goel, S., & Shawky, H. A. (2014). The impact of federal and state notification laws on security breach announcements. *Communications of the Association for Information Systems,, 34*(1), 37-50.

Hackett, R. (2015, March 27th). How much do data breaches cost big companies? Shockingly little. *Fortune*.

Herman, B. (2016, March 30th). Details of Anthem's massive cyberattack remain in the dark a year later. *ModernHealthcare.com*.

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.

Hitt, L. M., & Brynjolfsson, E. (1996). Productivity, business profitability, and consumer surplus: three different measures of information technology value. *Management Information Systems Quarterly*, 121-142.

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.

IBM. (2015). *Ponemon Institute's 2015 Global Cost of Data Breach Study Reveals Average Cost of Data Breach Reaches Record Levels.* Traverse City, MI: IBM.

Identity Theft Resource Center. (2015). *Data Breaches.* Identity Theft Resource Center.

Kaspersky Lab. (2015). *Damage Control: The Cost of Security Breaches IT Security Risks Special Report Series.* Kaspersky Lab.

Kedmey, D. (2014, August 6th). Target Expects $148 Million Loss from Data Breach. *Time*.

Ko, M. O.-B., M., K., & Dorantes, C. (2009). Investigating the impact of publicly announced information security breaches on three performance indicators of the breached firms. *Information Resources Management Journal, 22*, #2.

Legere,John. (2015). *T-Mobile CEO on Experian's Data Breach.* T-Mobile.

McGinty, K. (2015, February 26th). Target Data Breach Price Tag: $252 Million and Counting.

Mishra, A. (1996). Organizational responses to crisis. Trust in Organizations. *Frontiers of theory and research*, 261-287.

Morgan, S., & Winship, C. (2007). *Counterfactuals and Causal Inference: Methods and Principles for Social Research (Analytical Methods for Social Research).* New York, New York: Cambridge University Press.

Osborne, C., & Day, Z. (2015, February 2015). Anthem data breach cost likely to smash $100 million barrier. *ZDNet*.

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

Rouse, M. (2016). *Data Breach Definition.* http://searchsecurity.techtarget.com/definition/data-breach.

Rowinski, D. (2012, June 1). Infographic. Patent wars turns tech into a battlefield. *readwrite*.

Safdar, K., & Beilfuss, L. (2016, May 16th). Target Gives Weak Forecast as Sales Decline. *The Wall Street Journal*.

Salmela, H. (2008). Salmela, H. (2008). Analysing business losses caused by information systems risk: a business process analysis approach. *ournal of Information Technology,, 23*(3), 185-202.

Santhanam, R., & Hartono, E. (2003). Issues in linking information technology capability to firm performance. *Management Information Systems Quarterly*, 125-153.

Spanos, G., & Angelis, L. (2016). The impact of information security to the stock market: A systematic literature review. *58*, 216-229.

T.Ravichandran, & Lertwongsatien, C. (2005). Effect of Information Systems Resources and Capabilties on Firm Performance: A Resource-Based Perspective . *Journal of Management Information Systems* , 237-276.

T-Mobile. (2016). *T-Mobile Delivers Unparalleled Financial Results – Tops Revenue and Adjusted EBITDA Estimates.* T-Mobile Media Kits.

Tsoukas, H. (1999). David and Goliath in the risk society: Making sense of the conflict between Shell and Greenpeace in the North Sea. *Organization, 6*(3), 499-528.

Vogus, T. J., & Sutcliffe, K. M. (2007). Organizational resilience: towards a theory and research agenda. *2007 IEEE International Conference on Systems, Man and Cybernetics*, pp. 3418-3422.

Wernerfelt, B. (1984). A resource based view of the firm. *Strategic Management Journal*, 171-180.

Zafar, H., Ko, M., & Osei-Bryson, K. M. (2012). Financial impact of information security breaches on breached firms and their non-breached competitors. *Information Resources Management Journal, 25*(1), 21-37.