Impact of Cyberattacks on Stock Performance: A Comparative Study

Article *in* Information and Computer Security · July 2018

DOI: 10.1108/ICS-05-2018-0060

CITATIONS
0

READS
310

3 authors:

Samuel Tweneboah-Koduah
Aalborg University
7 PUBLICATIONS **22** CITATIONS
SEE PROFILE

Francis Atsu
Ghana Institute of Management and Public Administration
7 PUBLICATIONS **20** CITATIONS
SEE PROFILE

William J Buchanan
Edinburgh Napier University
440 PUBLICATIONS **953** CITATIONS
SEE PROFILE

Impact of Cyberattacks on Stock Performance: A Comparative Study

[1]Samuel Tweneboah-Koduah, [2]Francis Atsu, [3]William J. Buchanan

[1]Department of Computer Science| [2]Department of Accounting and Finance, Ghana Institute of Management and Public Administration, Accra, Ghana| [3]Edinburgh Napier University, Edinburgh, UK

Abstract

The recent spate of cyberattacks against critical infrastructure systems have necessitated the quest to examine the impact of such events on stock values. The question is 'what is the impact of cyberattack on stock values'? To address the question, data on cyberattacks announcements from 96 firms that are listed on S&P 500[1] between January 03, 2013 and December 29, 2017 were reviewed to draw some conclusions. The empirical analysis was performed in two ways: cross-section and industry level. The study employs statistical tests that account for the effects of cross-section correlation in returns, returns series correlation, volatility changes, and skewness in the returns, indicating the following results: For cross-section analysis, the outcome shows that markets do not significantly react to cyberattacks for all the event windows except [-30, 30], while for the sector-level assessment, the analysis offers two main results. First, while some firms react to cyber-attacks for long event window for retail sector, there is no significant evidence of a cumulative firm reaction to cyberattacks for both short and long event windows for the industrial, information technology and health sectors. Second, there is a strong evidence of cumulative reaction to cyberattacks (i.e. for [-1, 1]) for the financial industry, and the reactions disappear for relatively longer event windows. These outcomes imply that (1) studying the cumulative effects of cyberattacks on prices of listed firms without grouping them into the various sectors may be non-informative, (2) the financial sector firms tend to react cumulatively to cyberattacks over a 3-day period than other sectors, (3) technology firms tend to be less reactive to the announcement of a data breach; possibly such firms could have the necessary tools and techniques to address large-scale cyberattacks.

Keywords

Impact of Cyberattack, Stock Performance, Event Study Methodology, Abnormal Returns, Cumulative Average Returns

[1]The Standard and Poor's 500: An American stock market index which is based on the market capitalizations of 500 large companies having common stock listed on the New York Stock Exchange (NYSE)

1.0 Introduction

Without any doubt, the year 2017 will go into the records book as the year, newsworthy of cyberattacks. The first half of the year (2017), experienced an unprecedented high-profile cyberattacks on firms and other corporate institutions across the globe in the history of universal digital migrations. Undoubtedly, cybersecurity remains one of the major concerns of many CEOs and heads of major state-owned institutions in modern times. Cyber threats have become a pervasive concern for all companies which depend on information resources, and for state-owned institutions, the challenge could even be more. According to a report by Price Waterhouse Coopers (PwC) [1], there was nearly 66% year-on-year compound annual growth rate of detected security incidents since 2009. The report further estimated global cost of cybercrime in 2014 to be more than USD$23 billion (excluding undetected compromises). Additionally, it's estimated that the total number of cybersecurity attacks against critical infrastructure systems is ultimately unknown because many attacks are either not truly reported and/or the real (quantifiable) value of information resources is just too difficult to compute. In a related study, Ponemon Institute (involving 257 US multi-national companies) valued the mean annualised cybercrime cost for the year 2014 to be around US$12.7 million [2].

It is admitted, the actual value of the financial impact of a cyberattack on global firms may not be known, if such estimate is to include decreased revenues, disruption of business operations, regulatory penalties and erosion of customers' confidence. Moreover, breached firms suffer other non-financial impacts such as reputational damages, diversion of research and development information, loss of customer business, court settlements and other legal defence costs. To most investors, it is the reaction of the market (stock values) to the announcement of the attack that is very concerning.

The questions this paper seeks to answer are '(1) does stock values react to cyberattacks and if so, (2) does stocks of different industries react to cyberattacks differently'? Appropriate answers to these questions may offer much insight to how an equity investor does industrial level diversification. To answer the question, attempt is made to estimate the impact of the announcement of a cyberattack on the firms' stock values with the emphasis on the firms' abnormal returns (AR) and cumulative abnormal returns (CAR).

The objective of the paper is to examine how the stock market reacts to the announcement of a cyberattack on the breached firms. The study's analysis is based on the stock data of Six

S&P 500 companies (extracted from Yahoo finance [10]) between January 2013 and December 2017. In each case, the public announcement date of the breach event was used as the event window date [8]. Breach Level Index (BLI) [11] provides the basis for establishing public announcements dates of recorded breach events. The purpose of using BLI is to limit the likelihood of information inconsistencies and asymmetries about cyberattack events.

Extant studies have suggested a positive correlation between stock prices and the public announcement of a cyberattack by the breached firms [3], [4], [5], [6] and [7]. How much of this impact on average abnormal returns (AAR), and cumulative average abnormal returns (CAAR), has not been well explored using statistical tests that adjust for the effects of cross-section correlation, within-firm correlation, volatility changes, and skewness in the returns.

The paper contributes to literature in two folds. First, cross-section analysis was performed, where all the 96 firms are considered in one sample. Estimating the cumulative firms' reaction to the cyber-attacks, test statistics Patell Z ([36]), Cross-sectional T, Generalized Sign Z ([37]), StdCSect Z **(**[38]**),** Generalized Rank Z ([39]), Adjusted Patell Z **(**[40]), Generalized Rank T ([39])**,** and Skewness Corrected T ([41]) were performed. These tests produce estimates that are robust to the above estimation problems. Second, sector-level analysis for the industrial, information technology, financial and health sectors using the above test statistics was also performed. From these analysis, the authors are able to explore how firms in various sectors react to cyber-attack announcements in a varied manner as opposed to the cross-section analysis that assumes a homogenous firms reaction.

The empirical analysis delivers the following main results. For the cross-section analysis, the outcome shows that the market does not significantly react to cyberattacks for all the event windows except [-30, 30], while for the sector-level analysis, the analysis offers two main results. First, while there is reaction to cyberattacks for long event window for retail sector, there is insignificant evidence of a cumulative firms' reaction to cyberattacks for both short and long event windows for the industrial, information technology and health sectors. Second, for the firms in the financial sector, there is a strong evidence of cumulative reaction to cyberattacks for over a three-day period ([-1, 1] event window), and the reactions disappear for relatively longer event windows.

The rest of the paper is structured as follows. Section 2 looks at the state of the art of the subject matter from extant studies. Section 3 discusses the study methodology as the basis of

the research approach. Section 4 examines the source data and analysis the expected results. Section 5 concludes the paper.

2.0 State of the Art

Between January 2013 and June 2017, BLI [11] database records over 5791 cases of cybersecurity breaches against both private and public institutions, firms and other agencies globally. The year 2014 was historic in a high-profile cyberattack that resulted in the theft of over one billion records worldwide [11]. This is not to imply that the years 2015 and 2016 were relatively easy for information security. In 2015, there were special cases of damaging and highly publicised attacks. Most of these events consistently maintained cyber security in the headlines. According to the BLI database, there was a reported case of about 1,673 data breaches in 2015. Identity theft or stealing of Personally Identifiable Information (PII) outweighs all the other types of data theft, accounting for about 53% of all data breaches [11]. Furthermore, malicious outsiders accounted for nearly 58% of the data breaches incidents [11]. In the same year, it was estimated that over one million nine hundred thousand (1,938,383) data records were either lost or stolen per day. This amounts to over eighty-thousand (80,766) stolen records per hour, and more than one thousand three hundred (1346) records per minute. Thus, the period it takes to read the previous sentence, about 400 data records would have been stolen or lost without notice. The statistics corroborate the argument that the actual number of compromised data is mostly understated. Could the high rate of cyberattack globally over the period be attributed to the high level of insecure computing practices? How do the events of cyberattack impact on firm's performance? In the USA, several States have enacted laws on data breach disclosure. The aim is to encourage safe reporting practices. As Romanosky, et al. suggest, the implementation of the disclosure laws and similar regulations do not necessarily reduce the impact of cyberattack [12]. Rather, the affected firms suffer a negative impact on market values. Unfortunately, this negative market reaction does not become the only consequence of a data breach event.

As identified by the PwC report, the estimated financial cost of cyberattacks over the period runs over billions of dollars. Admittedly, it is impossible to truly quantify the actual cost of cybersecurity breach, and a method of doing so is worth exploring. The impacts of a cyberattack on firms' values differ from one firm to firm (depending on the industry and nature of attack). In the financial markets, investors are more concerned about the reaction of the market to the announcement of cyberattacks. Thus, the impact an attack has on the values of

the stock values. Tsiakis and Stephanides argue that "*the concept of investment has one purpose*: to generate a return" (either in the capital, time or benefits) [13]. Similarly, Goel and Shawky on their part posit, public announcement of security breaches can have a significant economic impact on firm stock values [5]. In this study, it is argued, "with public disclosure laws passed, security breaches involving disclosure of clients' information can both damage firms' reputation and lead to Federal fines by government agencies" [5].

The relationship between cyberattack and stock values has been well explored by existing studies. For instance, Ko and Dorantes applied a matched-sample comparison analysis to investigate the impact of security breaches on firm performance [6]. Their study concludes that while breached firms' sales and operating income did not decrease in the subsequent quarters following the breach, return on assets decreased in the third quarter. There are other related studies which appear to corroborate the positive correlation between the announcement of a cyber breach and a firm's performance (see [14], [15], [16], [17] and [18]).

The focus of this study is to determine the impact of data breach on the affected firms' abnormal profit and cumulative average abnormal profit. This approach provides the opportunity to assess the situational analysis of multiple firms' behaviour, providing a better result than the single firm window.

3.0 Event Study Methodology

Event-study methodology (ESM) has widely been used in the accounting and finance strands of literature [20], [21], [22], [23] and [24]. Notwithstanding, the model's application in cybersecurity research is in its elementary stage. Very few studies have applied the methodology in cybersecurity studies [25], [14], [26] and [6]. Following the IT strand of literature, the study investigates the effects of public announcements of cyberattacks on stock markets. Specifically, examining how stock prices of firms (in S&P 500) which have experienced cyberattacks (during the study period) react after the events have been made public. According to Boehmer [27] and Fama et al. [28], ESM is premised on the semi-strong form efficient market hypothesis: new publicly available information is instantly and rationally incorporated into the prices of equities. It is expected that stock prices react to cyberattack announcements, and hence the study captures this behaviour and the overall markets impact using two methods; naïve benchmark approach and the risk-adjusted or market model. For the naïve benchmark approach, market index was used to capture the market effects. The market

model (single-factor model) on the other hand uses the capital asset pricing model (see [29], [25] and [30]) stated as:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}, \tag{1}$$

where R_{it} is the return on equity *i* on day *t*, R_{mt} is the return of the market index *m* on day *t*. β_i, and ε_{it} are the intercept, gradient, and the residuals, respectively. Using the S&P 500 market index and an estimation window of 250 daily returns of each stock ([29], [33], and [25]), parameters of equation (1) was estimated. For instance, to estimate the parameters of equation (1) for the event window [-10, 10] (i.e. 10 days before the announcement and 10 after the announcement), an estimation window from day 260 to day 11 before the cyberattack announcement was used to avoid parameter contamination by the event under study. The abnormal return (AR) on a different day within the event window is computed as the difference between the actual return and the estimated return of equation (1) ($\hat{\alpha}_i + \hat{\beta}_i R_{mt}$) as follows:

$$AR_{it} = R_{it} - \left(\hat{\alpha}_i + \hat{\beta}_i R_{mt}\right) \tag{2}$$

where AR_{it} is the abnormal return for stock *i* on day *t*. Furthermore, the cumulative market reaction for the event window for individual firms and groups of firms was also captured. For individual firms, cumulative abnormal return (as the accumulation of price reactions over the event window) was calculated as follows:

$$CAR_{a,b} = \sum_{t=a}^{b} AR_t, \tag{3}$$

$CAR_{a,b}$ is the cumulative price reaction to an attack between day '*a*' and day '*b*', and AR_t is the corresponding abnormal return on day *t*. For the group level, equation (2) controls for the contemporaneous market-level fluctuations (see [30]). This effect was controlled by computing the average abnormal return (AAR) for the period under consideration which is given by

$$AAR_t = \frac{\sum_{i=1}^{N} AR_{it}}{N}, \tag{4}$$

where AAR_t is the average abnormal return on day *t* for *N* firms, AR_{it} is the abnormal return for firm *i* on day *t*. Further, the cumulative average abnormal return (CAAR), which measures the accumulated stock prices reaction to the cyberattacks over a given event window was estimated using:

$$CAAR_{a,b} = \sum_{t=a}^{b} AAR_t \,, \tag{5}$$

where $CAAR_{a,b}$ is the CAAR from day *a* to *b*, and AAR_t is the average abnormal return at day *t*.

3.1 Test of Significance

To evaluate the statistical significance of the cyberattacks on equity returns, the paper adopts various parametric and non-parametric tests of significance. First, classical cross-section t-test (under the null hypothesis, $H_0 : AAR = 0$) was applied as follows ([23]; [26, p. 200] ; [24]; [30]; among others).

$$t_{AAR_t} = \sqrt{N}\frac{AAR_t}{S_{AAR_t}}, \tag{6}$$

Where S_{AAR_t} is the standard deviation across firms at time *t*:

$$S^2_{AAR_t} = \frac{1}{N-1}\sum_{i=1}^{N}\left(AR_{i,t} - AAR_t\right)^2 , \tag{7}$$

The cross-section t-statistical for CAAR ($H_0 : CAAR = 0$) is given by

$$t_{CAAR} = \sqrt{N}\frac{CAAR}{S_{CAAR}}, \tag{8}$$

These simple tests are prune to cross-sectional correlation and volatility changes, among others, and as such lack power ([34]; [35]; among others). Given the weakness of the simple test for AAR and CAAR, the study employs statistical tests that account for the effects of cross-section correlation in returns, returns series correlation, volatility changes, and skewness in the returns. Specifically, the study uses Patell Z ([36]), Cross-sectional T, Generalized Sign Z ([37]), StdCSect Z **(**[38]), Generalized Rank Z ([39]), Adjusted Patell Z **(**[40]), Generalized Rank T ([39])**,** and Skewness Corrected T ([41]).

3.2 Event Study Timeline

The ESM covers four major time periods (figure 1):

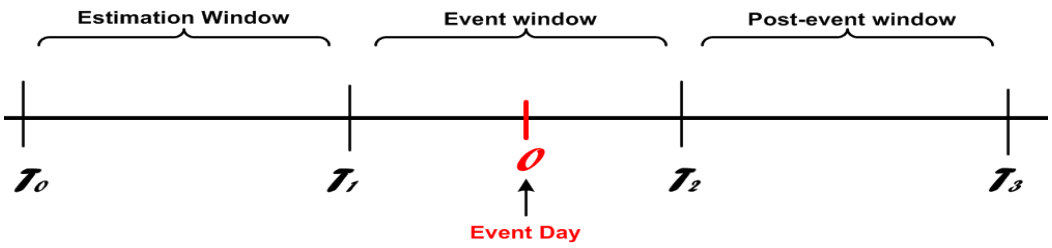

Figure 1: Cyberattack (Event study timeline)

i. The interval t_0 to t_1 illustrates the estimation window. It indicates how firms were faring in this period prior to the event window. This is considered to be two hundred (200) days prior to the event period. It is assumed that there will be normal behaviour of firms' market activities during this period.

ii. The interval t_1 to t_2 is the event window(s)

   a. T_1 to 0 is the pre-event window. This illustrates the probability of some people knowing about the attacks (i.e. the event) even before it became public or before the announcement dates (see table 1). T_0 is set to thirty (30) days.

   b. t_2 to t_3 is the post-event window. This illustrates the probability that some people got to hear of the attack later than the day of the announcement. T_3 is set to thirty (30) after the attack (events)

iii. Time 0 is the event date in calendar time (the attacked date for each firm). It represents the actual date when the news about the attack is made known to the public via announcements.

iv. Interval t_0 to t_3 is the observation period. It indicates the overall performance of the firm with respect to the attack. This shows whether the breached firm responded positively or negatively to the attack.

4.0 Result & Discussion

The study uses the information of the announcements of a data breach on firms listed on S&P 500 between the period of January 2013 and December 2017. Specifically, 96 firms that experienced cyberattacks were chosen (see Table 1 in the appendix for the list of the firms). The event dates are considered as the first public announcement of the attacks. The empirical analysis was performed in two ways: cross-section and industry level. Figures 1 and 2 show cross-section and industry level cumulative reaction of firms, respectively. It is obvious from the figures that firms react to cyberattacks in a varied manner.

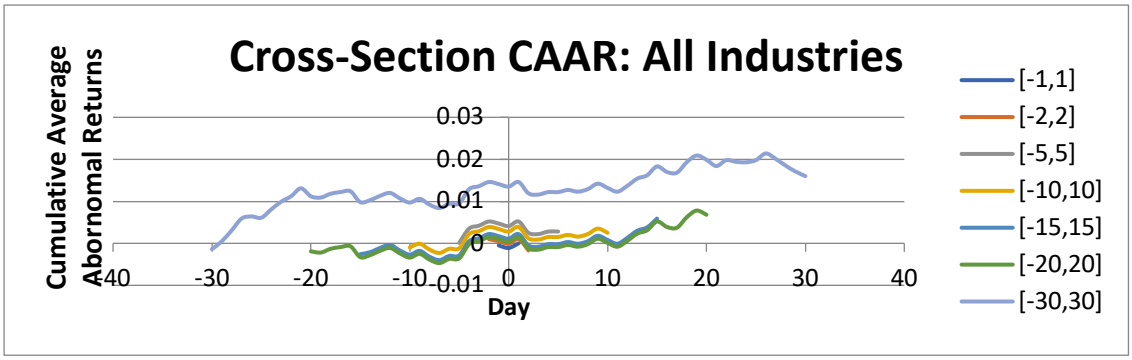

Figure 1a: Cross-section Analysis: Cumulative reaction of all firms – All Industries

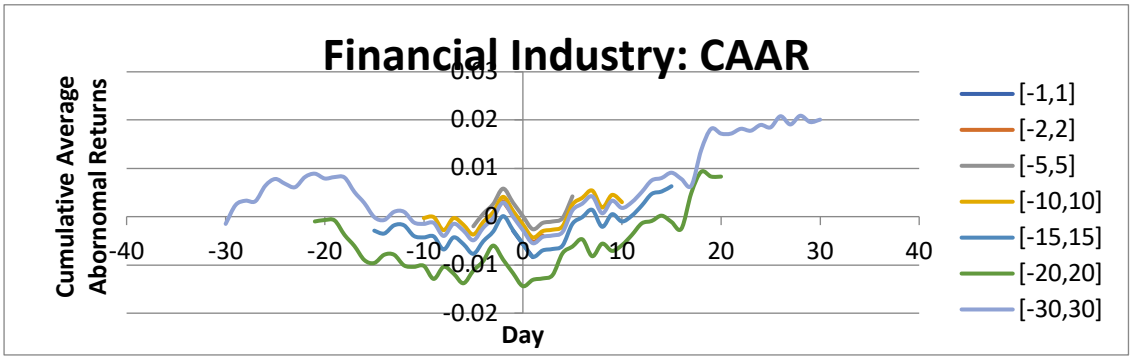

Figure 1b: Industry Level Analysis: Cumulative reactions of Stocks - Financial Sector

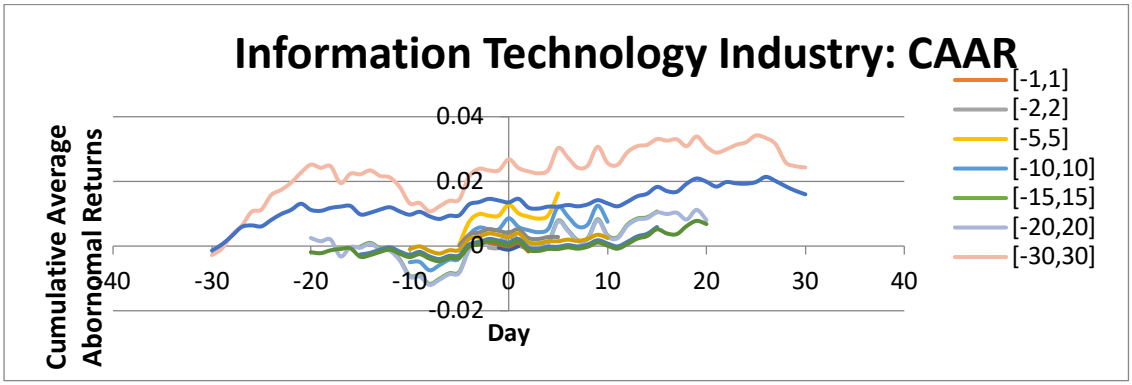

Figure 1c: Industry Level Analysis: Cumulative reactions of Stocks - Information Technology Sector

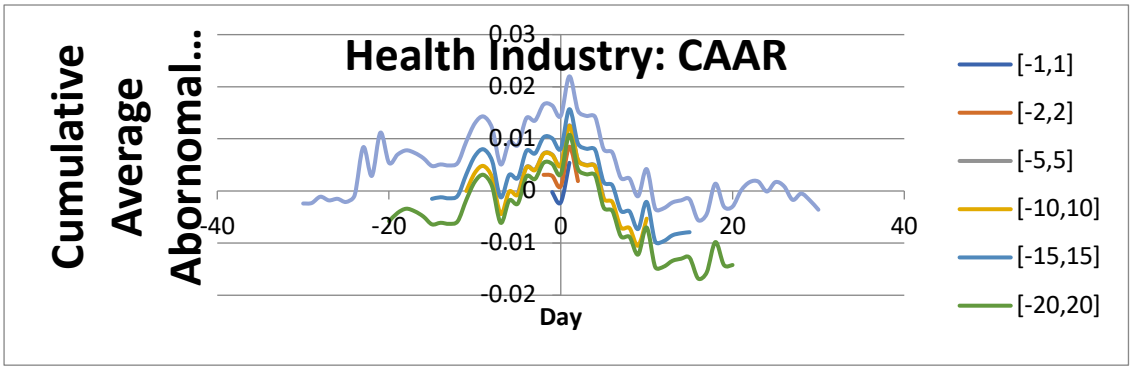

Figure 1d: Industry Level Analysis: Cumulative reactions of Stocks - Health Sector

Panel A and Panel B of Table 1 present the cross-section and industry level analyses, respectively. The test statistics of our cross-section analysis show that markets do not significantly react to cyberattacks for all the event windows except [-30,30] where Generalized

Sign Z, that adjusts for cross-section correlations, shows a marginal cumulative market reaction. For industry level, the analysis offers three main results. Firstly, there is no evidence of a cumulative firm reaction to cyberattacks for all the estimation windows for the industrial, information technology and health sectors. Secondly, for the retail sector, only the generalized Z test shows that the firms marginally reacted cumulatively over the [-20, 20] event window. For the financial sector, there is a strong evidence of cumulative reaction to cyberattacks for [-1, 1], and the reactions disappear for relative longer event windows.

The outcome of the analysis implies the following: Firstly, studying the cumulative effects of cyberattacks on prices of listed firms using event study methodology without grouping the firms into various sectors may not be informative. Secondly, firms in the financial sector tend to react cumulatively to cyberattacks over a 3-day period than firms in other sectors. Furthermore, there is not much reaction to the stock values of technology firms in terms of public announcement of a cyberattack. This may be due to the fact that such firms usually have tools and techniques to respond quickly to counteract the potential impact of such event.

Table 1: Cross-section and Sector-level Analysis

Window	CAAR Value	Patell Z	Csect T	Generalized Sign Z	StdCSect Z	Generalized Rank Z	Adjusted Patell Z	Generalized Rank T	Skewness Corrected T
Panel A: Cross-Section Analysis									
(-1, 1)	0.000	-0.327	0.024	-0.608	-0.348	-0.743	-0.310	-0.793	0.040
(-2, 2)	-0.002	-0.798	-0.723	-0.403	-0.910	-0.877	-0.756	-0.937	-0.739
(-5, 5)	0.003	0.042	0.636	0.209	0.046	0.108	0.040	0.116	0.669
(-10, 10)	0.003	-0.053	0.419	0.209	-0.054	-0.157	-0.050	-0.168	0.440
(-20, 20)	0.007	0.475	0.766	1.026	0.456	0.447	0.449	0.478	0.786
(-15, 15)	0.006	0.394	0.733	0.617	0.355	0.276	0.373	0.294	0.769
(-30, 30)	0.016	1.182	1.406	1.842**	1.128	1.224	1.120	1.307	1.485
Panel B: Sector-Level Analysis									
Industrial									
(-1, 1)	0.001	-0.377	0.167	-0.015	-0.298	-0.055	-0.374	-0.057	0.221
(-2, 2)	-0.003	-0.889	-0.328	-0.648	-0.930	-1.160	-0.881	-1.187	-0.275
(-5 ,5)	-0.004	-0.567	-0.454	-0.015	-0.635	-0.525	-0.562	-0.537	-0.478
(-10, 10)	-0.005	-0.591	-0.327	-1.280	-0.486	-0.815	-0.586	-0.834	-0.299
(-15 ,15)	-0.011	-0.820	-0.585	-1.280	-0.680	-0.951	-0.812	-0.973	-0.604
(-20, 20)	-0.008	-0.536	-0.429	-0.648	-0.508	-0.844	-0.531	-0.864	-0.432
(-30, 30)	0.011	0.346	0.444	0.617	0.304	0.175	0.343	0.179	0.453
Technology									
(-1, 1)	0.001	0.413	0.125	0.562	0.335	0.050	0.399	0.049	0.171
(-2, 2)	-0.001	-0.340	-0.110	0.115	-0.260	-0.022	-0.329	-0.022	-0.142
(-5, 5)	0.016	0.452	1.139	0.115	0.356	0.798	0.437	0.790	1.236
(-10, 10)	0.007	0.088	0.400	0.562	0.082	0.334	0.085	0.330	0.452
(-15, 15)	0.011	0.032	0.449	0.115	0.034	-0.031	0.031	-0.031	0.554
(-20, 20)	0.008	0.073	0.340	0.562	0.081	0.362	0.071	0.358	0.393

(-30, 30)	0.024	0.587	0.712	1.457	0.581	0.858	0.568	0.849	0.837
Retail									
(-1, 1)	0.003	0.722	0.924	0.699	0.917	0.817	0.713	0.818	0.918
(-2, 2)	-0.002	-0.140	-0.437	-0.788	-0.179	-0.489	-0.138	-0.490	-0.450
(-5, 5)	-0.003	-0.365	-0.535	-0.788	-0.459	-0.604	-0.360	-0.605	-0.562
(-10,10)	0.005	0.471	0.517	0.699	0.538	0.827	0.466	0.828	0.503
(-15, 15)	0.015	1.224	0.932	1.442	1.038	1.269	1.209	1.271	0.927
(-20, 20)	0.020	1.098	1.117	1.813**	1.025	1.331	1.085	1.333	1.137
(-30 30)	0.018	0.756	0.775	1.442	0.669	0.932	0.747	0.933	0.778
Health									
(-1, 1)	0.005	0.986	1.295	1.131	1.167	1.103	0.985	1.051	1.394
(-2, 2)	0.002	0.269	0.457	1.131	0.401	0.623	0.268	0.594	0.418
(-5, 5)	-0.001	0.005	-0.166	1.131	0.001	0.612	0.005	0.583	-0.230
(-10, 10)	-0.005	-0.464	-0.390	0.062	-0.449	-0.581	-0.464	-0.553	-0.383
(-15, 15)	-0.008	-0.463	-0.417	0.062	-0.438	-0.209	-0.463	-0.199	-0.438
(-20, 20)	-0.014	-0.608	-0.603	0.062	-0.522	-0.604	-0.607	-0.575	-0.615
(-30, 30)	-0.004	-0.418	-0.168	-0.473	-0.421	-0.271	-0.418	-0.258	-0.151
Financial									
(-1, 1)	-0.008	-2.384***	-4.315***	-3.422***	-4.179***	-4.081***	-2.386***	-4.239***	-3.895***
(-2, 2)	-0.004	-0.779	-1.235	-0.502	-1.102	-1.013	-0.780	-1.053	-1.245
(-5, 5)	0.004	0.445	0.486	0.332	0.397	0.003	0.445	0.003	0.603
(-10, 10)	0.003	0.033	0.247	-0.085	0.023	-0.329	0.033	-0.343	0.324
(-15, 15)	0.006	0.302	0.473	0.332	0.282	-0.122	0.302	-0.127	0.560
(-20, 20)	0.008	0.496	0.567	-0.085	0.483	0.161	0.497	0.167	0.591
(-30, 30)	0.020	1.116	1.179	0.749	1.101	0.881	1.117	0.915	1.229

Notes: ***/** denotes significant at 1 percent and 5 percent, respectively

NO	Ticker	Company Name	Industry	NO	Ticker	Company	Industry
1	BA	Boeing Company	Industrial	50	BBT	BB&T Corporation	Financial
2	CTAS	Cintas Corporation	Industrial	51	COF	Capital One Financial	Financial
3	DAL	Delta Air Lines	Industrials	52	SCHW	Charles Schwab corp.	Financial
4	EFX	Equifax Inc.	Industrials	53	CFG	Citizens Financial Group	Financial
5	GWW	Grainger (W.W.) Inc.	Industrials	54	CME	CME Group Inc.	Financials
6	LMT	Lockheed Martin Corp.	Industrials	55	DFS	Discover Financial Serv.	Financials
7	NOC	Northrop Grumman Corp.	Industrials	56	FITB	Fifth Third Bancorp	Financials
8	RSG	Republic Services Inc	Industrials	57	GS	Goldman Sachs Group	Financials
9	UPS	United Parcel Service	Industrials	58	JPM	JPMorgan Chase & Co.	Financials
10	UTX	United Technologies	Industrials	59	MTB	M&T Bank Corp.	Financials
11	AET	Aetna	Health Care	60	MMC	Marsh & McLennan	Financials
12	ANTM	Anthem Inc	Health Care	61	MS	Morgan Stanley	Financials
13	BAX	Baxter International Inc.	Health Care	62	NTRS	Northern Trust Corp.	Financials
14	CNC	Centene Corporation	Health Care	63	PNC	PNC Financial Serv.	Financials
15	CI	CIGNA Corp.	Health Care	64	PFG	Principal Financial Grp.	Financials
16	CVS	CVS Health	Health Care	65	STT	State Street Corp.	Financials
17	DVA	DaVita Inc.	Health Care	66	STI	SunTrust Banks	Financials
18	HUM	Humana Inc.	Health Care	67	WFC	Wells Fargo	Financials
19	MCK	McKesson Corp.	Health Care	68	AAP	Advance Auto Parts	Retail
20	MDT	Medtronic plc	Health Care	69	AMZN	Amazon.com Inc	Retail
21	PDCO	Patterson Companies	Health Care	70	AN	AutoNation Inc	Retail
22	PKI	PerkinElmer	Health Care	71	AZO	Autozone Inc	Retail
23	DGX	Quest Diagnostics	Health Care	72	BBBY	Bed Bath & Beyond	Retail
24	TMO	Thermo Fisher Scientific	Health Care	73	BBY	Best Buy Co. Inc.	Retail
25	ADBE	Adobe Systems	Information Tech.	74	CBS	CBS Corp.	Retail
26	AAPL	Apple Inc.	Information Tech.	75	CMG	Chipotle Mexican G.	Retail
27	AMAT	Applied Materials Inc	Information Tech.	76	CMCSA	Comcast Corp.	Retail
28	CSCO	Cisco Systems	Information Tech.	77	DLTR	Dollar Tree	Retail
29	CTXS	Citrix Systems	Information Tech.	78	EBAY	eBay Inc.	Retail

30	EA	Electronic Arts	Information Tech.	79	EXPE	Expedia Inc.	Retail
31	FB	Facebook	Information Tech.	80	HBI	Hanesbrands Inc	Retail
32	FIS	Fidelity National Information Services	Information Tech.	81	HAS	Hasbro Inc.	Retail
33	INTU	Intuit Inc.	Information Tech.	82	HD	Home Depot	Retail
34	MU	Micron Technology	Information Tech.	83	K	Kellogg Co.	Retail
35	MSFT	Microsoft Corp.	Information Tech.	84	LOW	Lowe's Cos.	Retail
36	MSI	Motorola Solutions Inc.	Information Tech.	85	M	Macy's Inc.	Retail
37	NFLX	Netflix Inc.	Information Tech.	86	MAR	Marriott Int'l.	Retail
38	NVDA	Nvidia Corporation	Information Tech.	87	MAT	Mattel Inc.	Retail
39	ORCL	Oracle Corp.	Information Tech.	88	MCD	McDonald's Corp.	Retail
40	STX	Seagate Technology	Information Tech.	89	NKE	Nike	Retail
41	TWX	Time Warner Inc.	Information Tech.	90	JWN	Nordstrom	Retail
42	XRX	Xerox Corp.	Information Tech.	91	SPLS	Staples Inc.	Retail
43	AABA	Yahoo Inc.	Information Tech.	92	HSY	The Hershey Company	Retail
44	WU	Western Union Co	Information Tech.	93	MOS	The Mosaic Company	Retail
45	AFL	AFLAC Inc	Financial	94	TRIP	TripAdvisor	Retail
46	AXP	American Express Co	Financial	95	VIAB	Viacom Inc.	Retail
47	AMP	Ameriprise Financial	Financial	96	WMT	Wal-Mart Stores	Retail
48	AON	Aon Inc	Financial	97	WYN	Wyndham Worldwide	Retail
49	BAC	Bank of America Corp	Financial				

5.0 Conclusion

"Cybercrime is a global growth industry. The returns are great, and the risks are low"[2]. Cybercrime is estimated to cost over $400 billion dollars annually to global economy [42]. This figure

[2] Centre for Strategic and International Studies, McAfee

represents only financially quantifiable estimates, yet many companies underestimate the cybersecurity risk they face and how quickly such risk may escalate. Additionally, the actual and total impacts (in terms of cost) of cybercrime activities are never known as many attacks remain undetected and/or unreported. Studies have also shown that stock market reacts strongly to the events of cyberattacks and potential investors continue to monitor such market reactions. For instance, in February 2017, Yahoo had to agree to take a price cut on the original $4.8bn sale of its core business to Verizon, making it one of the first times that the discovery of a cyberattack had resulted in revising an acquisition price [43]. In this paper, an attempt has been made to explore and explain the reaction of stock markets to high-profile cyberattacks in the S&P 500 index firms. In all data involving 97 firms were studied.

The empirical analysis was performed in two ways: cross-section and industry level. The test statistics of the cross-section analysis show that markets do not react significantly to cyberattacks for all the event windows except [-30,30] where Generalized Sign Z, that adjusts for cross-section correlations, shows a marginal cumulative market reaction. For industry level, the analysis offers three main results. Firstly, there is no evidence of a cumulative firm reaction to cyberattacks for all the estimation windows for the industrial, information technology and health sectors. Secondly, for the retail sector, only the generalized Z test shows that the firms marginally reacted cumulatively over the [-20, 20] event window. For the financial sector, there is a strong evidence of cumulative reaction to cyberattacks for [-1, 1], and the reactions disappear for relative longer event windows.

Reference

[1] C. Potter and A. Miller, "INFORMATION SECURITY BREACHES SURVEY 2013," Department for Business, Innovation and Skills, London, UK, Technical, Apr. 2013.

[2] P. Institute, "2014 Cost of Cyber Crime Study: United States," Ponemon Institute, Michigan, USA, Research, Oct. 2014.

[3] K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *J. Comput. Secur.*, vol. 11, no. 3, pp. 431–448, 2003.

[4] A. Acquisti, A. Friedman, and R. Telang, "Is there a cost to privacy breaches? An event study," *ICIS 2006 Proc.*, p. 94, 2006.

[5] S. Goel and H. A. Shawky, "Estimating the market impact of security breach announcements on firm values," *Inf. Manage.*, vol. 46, no. 7, pp. 404–410, 2009.

[6] M. Ko and C. Dorantes, "The impact of information security breaches on financial performance of the breached firms: an empirical investigation," *J. Inf. Technol. Manag.*, vol. 17, no. 2, pp. 13–22, 2006.
[7] A. Garg, J. Curtis, and H. Halper, "Quantifying the financial impact of IT security breaches," *Inf. Manag. Comput. Secur.*, vol. 11, no. 2, pp. 74–83, 2003.
[8] J. Binder, "The event study methodology since 1969," *Rev. Quant. Finance Account.*, vol. 11, no. 2, pp. 111–137, 1998.
[9] A. C. MacKinlay, "Event studies in economics and finance," *J. Econ. Lit.*, vol. 35, no. 1, pp. 13–39, 1997.
[10] "^GSPC 2,472.54 -0.91 -0.04% : S&P 500 - Yahoo Finance." [Online]. Available: https://finance.yahoo.com/quote/%5EGSPC?p=^GSPC. [Accessed: 22-Jul-2017].
[11] Gemalto, "Data Breach Database," *Breach Level Index*. [Online]. Available: http://breachlevelindex.com. [Accessed: 05-Jul-2017].
[12] S. Romanosky, R. Telang, and A. Acquisti, "Do data breach disclosure laws reduce identity theft?," *J. Policy Anal. Manage.*, vol. 30, no. 2, pp. 256–286, 2011.
[13] T. Tsiakis and G. Stephanides, "The economic approach of information security," *Comput. Secur.*, vol. 24, no. 2, pp. 105–108, 2005.
[14] A. Garg, J. Curtis, and H. Halper, "Quantifying the financial impact of IT security breaches," *Inf. Manag. Comput. Secur.*, vol. 11, no. 2, pp. 74–83, 2003.
[15] C. Martin, A. Kadry, and G. Abu-Shady, "Quantifying the financial impact of it security breaches on business processes," in *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on*, 2014, pp. 149–155.
[16] R. Telang and S. Wattal, "An empirical analysis of the impact of software vulnerability announcements on firm stock price," *IEEE Trans. Softw. Eng.*, vol. 33, no. 8, pp. 544–557, 2007.
[17] A. A. Yayla and Q. Hu, "The impact of information security events on the stock value of firms: The effect of contingency factors," *J. Inf. Technol.*, vol. 26, no. 1, pp. 60–77, 2011.
[18] K. Kannan, J. Rees, and S. Sridhar, "Market reactions to information security breach announcements: An empirical analysis," *Int. J. Electron. Commer.*, vol. 12, no. 1, pp. 69–91, 2007.
[19] "Yahoo Finance - Business Finance, Stock Market, Quotes, News." [Online]. Available: https://finance.yahoo.com/. [Accessed: 06-Jul-2017].
[20] T. P. Wisniewski, "Empirical Evidence on Economic and Financial Aspects of Intensive Insider Trading," 2004.
[21] S. D. Friedman and H. Singh, "CEO succession and stockholder reaction: The influence of organizational context and event content," *Acad. Manage. J.*, vol. 32, no. 4, pp. 718–744, 1989.
[22] C. Eckel, D. Eckel, and V. Singal, "Privatization and Efficiency: Industry Effects of the sale of British Airways," *J. Financ. Econ.*, vol. 43, no. 2, pp. 275–298, 1997.
[23] A. Telegdy, J. S. Earle, and C. K. Victor Kaznovsky, "Corporate control: A study of firms on the Bucharest Stock Exchange," *East. Eur. Econ.*, vol. 40, no. 3, pp. 6–27, 2002.
[24] I. Otchere, "Do privatized banks in middle-and low-income countries perform better than rival banks? An intra-industry analysis of bank privatization," *J. Bank. Finance*, vol. 29, no. 8, pp. 2067–2093, 2005.
[25] A. Hovav and J. D'Arcy, "The impact of denial-of-service attack announcements on the market value of firms," *Risk Manag. Insur. Rev.*, vol. 6, no. 2, pp. 97–121, 2003.

[26] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers," *Int. J. Electron. Commer.*, vol. 9, no. 1, pp. 70–104, 2004.
[27] E. Boehmer, J. Masumeci, and A. B. Poulsen, "Event-study methodology under conditions of event-induced variance," *J. Finance. Econ.*, vol. 30, no. 2, pp. 253–272, 1991.
[28] E. F. Fama, "Market efficiency, long-term returns, and behavioral finance," *J. Financ. Econ.*, vol. 49, no. 3, pp. 283–306, 1998.
[29] B. L. Dos Santos, K. Peffers, and D. C. Mauer, "The impact of information technology investment announcements on the market value of the firm," *Inf. Syst. Res.*, vol. 4, no. 1, pp. 1–23, 1993.
[30] D. Kliger and G. Gurevich, "Introduction," in *Event Studies for Financial Research*, Springer, 2014, pp. 1–3.
[31] E. F. Fama, L. Fisher, M. C. Jensen, and R. Roll, "The adjustment of stock prices to new information," *Int. Econ. Rev.*, vol. 10, no. 1, pp. 1–21, 1969.
[32] C. Frank, A. Garg, L. Sztandera, and A. Raheja, "Forecasting women's apparel sales using mathematical modeling," *Int. J. Cloth. Sci. Technol.*, vol. 15, no. 2, pp. 107–125, 2003.
[33] K. S. Im, K. E. Dow, and V. Grover, "A reexamination of IT investment and the market value of the firm—An event study methodology," *Inf. Syst. Res.*, vol. 12, no. 1, pp. 103–117, 2001.
[34] S. J. Brown and J. B. Warner, "Using daily stock returns: The case of event studies," *J. Financ. Econ.*, vol. 14, no. 1, pp. 3–31, 1985.
[35] A. Dymarsky, Z. Komargodski, A. Schwimmer, and S. Theisen, "On scale and conformal invariance in four dimensions," *J. High Energy Phys.*, vol. 2015, no. 10, p. 171, 2015.
[36] J. M. Patell, "Corporate forecasts of earnings per share and stock price behavior: Empirical test," *J. Account. Res.*, pp. 246–276, 1976.
[37] A. R. Cowan, "Nonparametric event study tests," *Rev. Quant. Finance Account.*, vol. 2, no. 4, pp. 343–358, 1992.
[38] B. A. Bloom and L. A. Jackson, "Abnormal stock returns and volume activity surrounding lodging firms' CEO transition announcements," *Tour. Econ.*, vol. 22, no. 1, pp. 141–161, 2016.
[39] J. W. Kolari and S. Pynnonen, "Nonparametric rank tests for event studies," *J. Empir. Finance*, vol. 18, no. 5, pp. 953–971, 2011.
[40] J. W. Kolari and S. Pynnönen, "Event study testing with cross-sectional correlation of abnormal returns," *Rev. Financ. Stud.*, vol. 23, no. 11, pp. 3996–4025, 2010.
[41] P. Hall, "On the removal of skewness by transformation," *J. R. Stat. Soc. Ser. B Methodol.*, pp. 221–228, 1992.
[42] McAfee, "Net Losses: Estimating the Global Cost of Cybercrime," Center for Strategic and International Studies, McAfee, Santa Clara, California, USA, Industry, Jun. 2014.
[43] F.-K. James and H. K. Kuchler, "Cyberattacks lead Yahoo to accept price cut on $4.8bn Verizon deal," Financial Times, U.S.A, Feb. 2017.

Appendix