Review of Economics & Finance
Submitted on 01/01/2018
Article ID: 1923-7529-2018-03-93-08 Daniel Castillo, and Joseph Falzon

An Analysis of the Impact of WannaCry Cyberattack on Cybersecurity Stock Returns

Daniel Castillo, CFA (Correspondence author)
Faculty of Economics, Management and Accountancy, University of Malta
Banking & Finance, Room 219, Humanities B (FEMA), Msida, MALTA
Tel: +356 2340 3478 Email: daniel.castillo@um.edu.mt
Homepage: https://www.um.edu.mt/fema

Prof. ***Joseph Falzon***
Faculty of Economics, Management and Accountancy, University of Malta
Banking & Finance, Room 221, Humanities B (FEMA), Msida, MALTA
Tel: +356 2340 2391 Email: joseph.falzon@um.edu.mt
Homepage: https://www.um.edu.mt/fema

***A*bstract:** This research examines the impact of the WannaCry cyberattack, considered to be the defining event for cyber threats, on stock returns of companies operating in the cybersecurity industry on the first trading day after the event. The aim is to ascertain whether the reaction of stock prices on this day could be classified as abnormal and which direction they follow. The expectation is for a demand shift for the products and services offered by these firms and consequently stock markets should reflect this new information in equity prices. Literature has mostly focused on natural catastrophes and lately on man-made catastrophes like terror attacks. This study explores the emerging area of cyberattacks which could develop into catastrophic situations. Event-study methodology is employed for the analysis of this specific event and results clearly indicate that WannaCry had a positive effect on the equity returns of cybersecurity companies and cybersecurity investment vehicles.

Keywords: WannaCry Cyberattack; Ransomware; Stock returns; Event-study; Cybersecurity industry

JEL Classification: G11, G14, G15, G22

1. Introduction

Stock prices tend to respond vigorously to events considered to be potentially cataclysmic as investors try to quickly make up their minds on investment decisions in short timeframes. Events studied so far in the literature are mostly focused on natural catastrophes and lately man-made catastrophes like terror attacks. This study explores the new area of cyberattacks which could develop into catastrophic situations if the attacks have a global reach and exploit widespread security weaknesses. The focus is the global ransomware attack named WannaCry which started on Friday, May 12, 2017. To the best of the authors' knowledge this study is the first to consider the specific impact of cyberattacks.

The aim of this paper is to analyse the equity price response of companies involved in the cybersecurity industry on the first trading day after the event to ascertain whether the reaction in stock prices on this day could be classified as abnormal and consequently which direction they follow. This paper first analyses the response of two exchange traded funds (ETFs) explicitly formed to invest in cybersecurity stocks. It then examines the impact on 43 individual worldwide cybersecurity related companies. This study is an analysis of a single event which can be considered as a defining moment for cyberattack threats – from the advent of WannaCry, governments, companies and individuals raised the priority of dealing with cybersecurity topics to the top spot.

Results in this research clearly indicate that WannaCry had a positive effect on the equity returns of cybersecurity companies and of associated investment vehicles.

2. Literature Review

On Friday, May 12, 2017 a ransomware attack named WannaCry, was launched on worldwide computer systems exploiting a security gap in computers running Microsoft operating systems which have not been updated with a security patch designed to address this precise weakness. It is estimated that the attack infected over 300,000 computers in 150 different countries before it was eventually stopped (Lawrence and Robertson, 2017). Affected users were asked to pay a ransom of between $300 - $600 in bitcoin to decrypt their files and systems which were professionally encrypted by the attack (ibid.). Some of the high-profile victims included the UK's National Health Service, FedEx, Renault, Nissan, Russian Central Bank, Russian Interior Ministry, Petrobras, Telefonica, Deutsche Bahn and many others (Navetta *et al*. 2017). A cyber apocalypse was only avoided accidentally when Markus Hutchins, a young cybersecurity expert based in England found a hidden weakness in the cyberattack which stopped the further propagation of WannaCry (ibid.).

In the finance literature, a lot of research is dedicated to the impacts of natural catastrophic events on insurance stocks (Lamb, 1995; Takao *et al*., 2013; Thomann, 2013; and Hagendorff *et al*., 2015) and on equity markets in general (Worthington and Valadkhani, 2004; Worthington and Valadkhani, 2005; Worthington, 2008; Wang and Kutan, 2013; Ferreira and Karali, 2015; and Valizadeh, 2017). While a growing stream is focusing on the stock market impacts of man-made events like terrorist attacks (Chen and Siems, 2004; Reshetar and Karaman, 2011; and Iatridis *et al*.; 2011). The "large-scale disruption and destruction" (Furedi, 2007 p. 482) caused by such events generally leads to the expectation of negative economic repercussions; however, the debate is still open on whether the adverse implications apply universally or whether there are instances of the gain from loss hypothesis for companies and consequently for stock returns as put forward by Shelor *et al*. (1992).

Focusing on a specific section of the technology industry, this research follows the line of thought of other studies which have analysed the impact of the Paris terror attacks solely on the international defence industry (Apergis and Apergis, 2017) and on airline stock returns following the 11th September attack (Carter and Simkins, 2004). In response to cyberattacks with such global reach, one would expect a demand shift for the products and services offered by these firms and consequently also expect investors to positively reflect this information in equity prices.

While initial evidence indicates that cyberattacks increase stock volatility of companies targeted by cyberattacks (Corbet and Gurdgiev, 2017), the research question tackled by the empirical analysis of this study clarifies the impact on stock returns.

3. Methodology

This study makes use of event-study methodology to understand the impact on financial returns from the occurrence of a specific event. This research makes use of two measures of excess returns to study the impact of WannaCry as outlined by the methodology presented in Brown and Warner (1985). The analysis covers 250 consecutive trading days prior to the day of the event, defined as Day 0, while days -244 to -6 are defined as the estimation period.

The first measure is based on the extraction of excess returns of a security after adjusting for the mean of the same return series:

$$ER_{i,t} = ret_{i,t} - \mu_i \tag{1}$$

$$\mu_i = \frac{1}{239}\sum_{t=-244}^{-6} ret_{i,t} \tag{2}$$

where $ER_{i,t}$ denotes Excess returns of equity i on day t; $ret_{i,t}$ means rate of return of equity i on day t; and μ_i is the arithmetic average of returns in the estimation period.

The second measure is based on the extraction of excess returns of a security after adjusting for the returns based on a market model:

$$ER_{i,t} = ret_{i,t} - \hat{\alpha}_i - \hat{\beta}_i ret_{mrkt,t} \tag{3}$$

where $ret_{mrkt,t}$ denotes rate of return of the market index on day t; and $\hat{\alpha}_i$, $\hat{\beta}_i$ represent the intercept and slope coefficient of the market model estimated respectively, by using Ordinary Least Squares (OLS) over the estimation period.

The decision on the statistical significance or otherwise of the excess returns was done based on the calculation of the following test statistic which follows the t-distribution (ibid.):

$$test\ statistic = \frac{ER_0}{\text{st.}dev\ (ER_t)} \tag{4}$$

$$st.dev\ (ER_t) = \sqrt{\left(\sum_{t=-244}^{t=-6} (ER_t - \overline{\mu}_i)^2\right)/238} \tag{5}$$

$$\overline{\mu}_i = \frac{1}{239}\sum_{t=-244}^{t=-6} ER_t \tag{6}$$

The results of the analysis are presented in the following section.

4. Empirical Analysis

4.1 Data

The study analyses the returns of two cybersecurity ETFs and 43 worldwide cybersecurity companies on the first trading day after the WannaCry cyberattack. The event started developing on Friday 12 May 2017 and continued into the weekend with more information and details of the magnitude being revealed in the mainstream media. The analysis is thus carried out on the first trading day after the weekend, Monday 15 May 2017. The daily data covers the period between May 2016 and May 2017 (250 daily returns) and was obtained from Thomson Reuters Datastream. Part of the empirical analysis requires the estimation of a market model and each company analysed was thus assigned a market index. For the two ETFs and the companies trading in the US stock market, the NASDAQ composite index was selected as it is the most frequently used technology index. Non-US companies were mapped to the main index for that country. The timeseries of daily data were individually adjusted for market holidays on days the stock market is closed. Daily percentage returns were then calculated on the closing prices.

4.2 Results and analysis

Tables 1 and 2 below present the results of the analysis while Figure 1 displays the frequency distribution of excess returns.

Table 1. Excess returns of ETFs on Day 0

Investment Channel	Mean Adjusted Returns	OLS Market Model Adj. Ret.
First Trust Nasdaq Cybersecurity ETF (CIBR)	2.51% (2.66)***	2.13% (2.91)***
PureFunds ISE Cyber Security ETF (U-Hack)	3.10% (3.68)***	2.68% (4.00)***
NASDAQ	0.37% (0.51)	n/a

Notes: Figures in brackets represent the test-statistics which follow a t-distribution.
*** shows statistical significance at the 1% level.

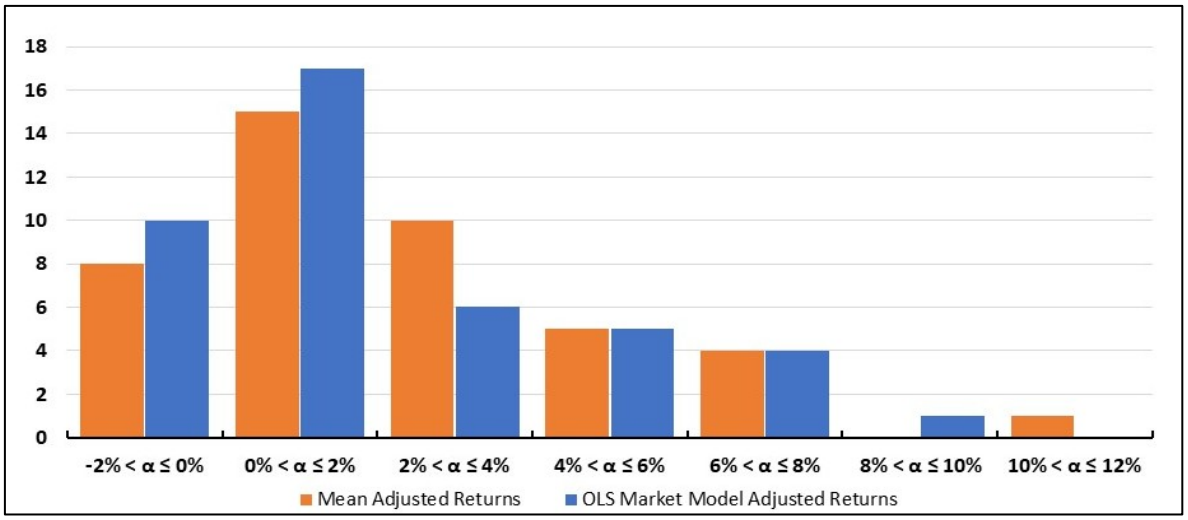

Figure 1. Frequency distribution of Excess Returns

Table 2. Excess returns of individual stocks on Day 0

U.S. Equities	**Mean Adjusted Returns**	**OLS Market Model Adj. Ret.**
A10 Networks, Inc.	1.08% (0.43)	0.53% (0.24)
Akamai Technologies, Inc.	0.79% (0.35)	0.40% (0.19)
Barracuda Networks, Inc.	5.61% (2.04)**	4.89% (2.06)**
Booz Allen Hamilton Holding Corp. Class A	1.20% (0.98)	0.91% (0.84)
Check Point Software Technologies Ltd.	2.47% (2.15)**	2.27% (2.11)**
Cisco Systems, Inc.	2.25% (2.49)**	1.95% (2.83)***
CyberArk Software Ltd.	-1.09% (-0.55)	-1.58% (-0.91)
F5 Networks, Inc.	1.90% (1.11)	1.58% (1.00)
FireEye, Inc.	7.48% (2.47)**	6.92% (2.45)**
Fortinet, Inc.	3.31% (1.71)*	2.87% (1.66)*
Gigamon, Inc.	-0.37% (-0.11)	-0.87% (-0.26)
Imperva, Inc.	2.26% (0.81)	1.81% (0.68)
Itron, Inc.	0.66% (0.37)	0.32% (0.19)
Juniper Networks, Inc.	-0.07% (-0.04)	-0.47% (0.34)
KeyW Holding Corp	5.90% (2.33)**	5.43% (2.31)**
Leidos Holdings, Inc.	0.07% (0.05)	-0.21% (0.17)
ManTech International Corporation	1.88% (1.11)	1.49% (0.98)
Mimecast Ltd.	10.12% (3.15)***	9.69% (3.12)***
MobileIron, Inc	1.59% (0.44)	1.09% (0.32)
Palo Alto Networks, INC	2.76% (1.07)	2.44% (0.97)
Proofpoint, Inc	7.18% (3.07)***	6.59% (3.24)***
Qualys, Inc.	5.03% (2.84)***	4.62% (2.94)***
Radware Ltd.	2.32% (1.45)	1.94% (1.37)
Rapid7, Inc.	2.01% (0.67)	1.33% (0.49)
Science Applications International Corp.	1.71% (1.04)	1.34% (0.91)
Splunk, Inc.	1.26% (0.59)	0.55% (0.34)
Symantec Corp.	2.92% (2.25)**	2.61% (2.27)**
Varonis Systems, Inc.	1.53% (0.80)	1.06% (0.63)
VASCO Data Security International, Inc.	4.63% (1.97)**	4.12% (1.94)*
Verint Systems, Inc.	0.04% (0.02)	-0.32% (-0.20)
VeriSign, Inc.	1.09% (0.79)	0.74% (0.62)
VMware, Inc.	1.36% (1.01)	1.01% (0.87)
Zix Corporation	5.51% (2.79)***	5.15% (2.80)***
U.K. Equities	**Mean Adjusted Returns**	**OLS Market Model Adj. Ret.**
BAE Systems p.l.c.	-0.84% (-0.67)	-0.96% (-0.97)
Experian p.l.c.	-0.60% (-0.58)	-0.71% (-0.90)
Sophos Group p.l.c.	7.07% (3.16)***	6.94% (3.30)***
Ultra Electronics Holdings p.l.c.	-0.24% (-0.18)	-0.35% (-0.31)
Swedish Equities	**Mean Adjusted Returns**	**OLS Market Model Adj. Ret.**
Precise Biometrics AB	-1.09% (-0.27)	-1.13% (-0.29)
Japanese Equities	**Mean Adjusted Returns**	**OLS Market Model Adj. Ret.**
FFRI, Inc.	6.55% (2.07)**	6.71% (2.34)**

Trend Micro, Inc.	1.21% (0.68)	1.32% (0.89)
Dutch Equities	**Mean Adjusted Returns**	**OLS Market Model Adj. Ret.**
Gemalto NV	-0.23% (-0.11)	-0.28% (-0.14)
Finnish Equities	**Mean Adjusted Returns**	**OLS Market Model Adj. Ret.**
F-Secure OYJ	3.68% (1.91)*	3.48% (1.92)*
South Korean Equities	**Mean Adjusted Returns**	**OLS Market Model Adj. Ret.**
AhnLab, Inc.	2.43% (0.57)	2.22% (0.52)
Notes: Figures in brackets represent the test-statistics which follow a t-distribution. ***, **, and * indicate statistical significance at the 1%, 5%, and 10% level, respectively.		

Results show that the two cybersecurity ETFs registered strong statistically significant positive excess returns at the 1% level on the first trading day following WannaCry. Both the size and significance of this finding demonstrate the impact of this worldwide cyber event on ETFs with a specific mandate to invest in the worldwide cybersecurity industry.

No impact was determined on the equities of the general I.T. industry as proxied by the Nasdaq index.

At the individual company level, the data reveals that out of the 43 companies analysed, 5 (6) companies experienced positive statistically significant mean-adjusted (OLS market model-adjusted) excess returns at the 1% level. While a further 8 (7) companies had positive statistically significant mean-adjusted (OLS market model-adjusted) excess returns at the 5% level and 2 (2) companies had positive statistically significant mean-adjusted (OLS market model-adjusted) excess returns at the 10% level. Such a result at the individual company level confirms the above finding for ETFs and specifically evidences that investors quickly reacted to the news of this cyber event and positively changed their outlook for companies in the cybersecurity industry.

Having a closer look at the data, it can also be noted that 80% of the companies analysed had positive excess returns on the first trading day after WannaCry. On the other hand, for companies with negative excess returns, none of these were statistically significant even at the 10% level.

The results are robust to a change in the way excess returns are calculated. Significance results are consistent across both methods. The relationship between the size of excess returns and market capitalisation was also analysed but no further insights were derived.

5. Conclusions and Applications

The study discovers significant positive excess returns for the two ETFs specifically formed to invest in cybersecurity stocks and for 15 individual companies which are directly related to the cybersecurity market.

The results outlined in this study have significant applications to retail and institutional investors as they assess the implications of large-scale cyberattacks on portfolio values. Investors with a portfolio exposed to potential losses from cyberattacks, may rethink their asset allocation strategy especially towards investments which may i) mitigate the negative implications, ii)

neutralise them; or iii) gain from the ensuing chaos. A case in point is the (re)insurance industry which is embracing the nascent market of cyber insurance (Merret, 2017) while challenges still exist on the modelling of its risks (Shi, 2017). This means that the understanding of the impact of an event on liabilities (i.e. claims) is in most cases still unknown and contains significant margins of error. With this backdrop, the situation makes it even more important for (re)insurance companies to analyse and design their asset portfolios in a way that their value moves in the opposite direction and better still with higher magnitudes as the uncertainty, disruption and panic from an event increase.

Albeit the results from this study are strongly indicative that cybersecurity related companies or investment vehicles can be a good match for investors who wish to hedge or take an active position in such risks, it is to be said that cautiousness is required before any quick generalisations from such results are made. This is because the pool of similar cyber events with widespread repurcussions are still too small and further analysis is required. The research must be widened to ascertain the source of the weakness that permits the cyberattack in the first place. In the event that one of the studied companies has left an exploitable vulnerability in one of its cybersecurity solutions that initiates an attack, it is unlikely that the significant positive excess returns found in this study will be individually replicated. Notwithstanding, an investment vehicle focused on cybersecurity stocks, similar to the ETFs studied, could potentially still be an attractive addition to a diversified portfolio to lessen any idiosyncratic risk of this kind while protecting from negative repercussions of a cyberattack exposure.

Acknowledgements: The authors would like to thank the anonymous referees to ***Review of Economics & Finance*** for their valuable comments.

References

[1] Apergis, E., and Apergis, N. (2017). "The impact of 11/13 Paris terrorist attacks on stock prices: evidence from the international defence industry", *Applied Economics Letters*, 24 (1): 45-48.

[2] Brown, J. S, and Warner, J. B. (1985). "Using daily stock returns: The case of event studies", *Journal of Financial Economics*, 14 (1): 3-31.

[3] Carter, D. A., and Simkins, B. J. (2004). "The market's reaction to unexpected, catastrophic events: the case of airline stock returns and the September 11th attacks", *The Quarterly Review of Economics and Finance*, 44 (4): 539-558.

[4] Chen, Andrew H., and Thomas F. Siems (2004). "The effects of terrorism on global capital markets", *European Journal of Political Economy*, 20 (2): 349-366.

[5] Chesney, M., Reshetar, G., and Karaman, M. (2011). "The impact of terrorism on financial markets: An empirical study", *Journal of Banking & Finance*, 35 (2): 253-267.

[6] Corbet, S., and Gurdgiev, C. (2017). "What the Hack: Systematic Risk Contagion from Cyber Events", [Online] Available at SSRN: https://ssrn.com/abstract=3033950 .

[7] Ferreira, S., and Karali, B. (2015). "Do Earthquakes Shake Stock Markets? ", *PLoS ONE*, 10 (7): 1-19.

[8] Furedi, F. (2007). "The changing meaning of disaster", 39 (4): 482-489.

[9] Hagendorff, B., Hagendorff, J., and Keasey, K. (2015). "The Impact of Mega-Catastrophes on Insurers: An Exposure-Based Analysis of the U.S. Homeowners' Insurance Market", *Risk Analysis: An International Journal*, 35 (1): 157-173.

[10] Iatridis, G., Stagiannis, A., Kollias, C. and Mastronikolos, A. (2011). "Empirical Examination of the Impact of Terrorist Attacks – New York, Madrid, London – on Sectoral Stock Returns: cross-stock market study", *Journal of Financial Management & Analysis*, 24 (1): 1-23.

[11] Lamb, R. P. (1995). "An Exposure-Based Analysis of Property-Liability Insurer Stock Values Around Hurricane Andrew", *The Journal of Risk and Insurance Association*, 62 (1): 111-123.

[12] Lawrence, D., and Robertson, J. (2017). "The global hack could have been much, much worse", Bloomberg. [Online]Available at: https://www.bloomberg.com/news/articles/2017-05-18/the-wannacry-global-hack-could-have-been-much-much-worse [Accessed on 7 Jul 2017].

[13] Merret, J. (2017). "Cyber Security", The Journal, August – September 2017, pp. 18-19.

[14] Navetta, D., Segalis, B., Locker., E., and Hoffman, A. (2017). "WannaCry Ransomware Attack Summary", Data Protection Report. [Online] Available at: http://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/ [Accessed on 7 Jul2017].

[15] Shelor , M. R., Anderson, D. C., and Cross, M. L. (1992). "Gaining From Loss: Property-Liability Insurer Stock Values in the Aftermath of the 1989 California Earthquake", *The Journal of Risk and Insurance*, 59 (3): 476-488.

[16] Shi, C. (2017). "Sector Profile: Cyber modelling", *Insider Quarterly*, Issue 62, pp. 20-22. [Online] Available at: https://www.insiderquarterly.com/assets/_files/documents/jul_17/ii__1499271871_IQ_Summer_2017_web.pdf .

[17] Takao, A., Yoshizawa, T., Hsu, S., and Yamasaki, T. (2013). "The Effect of the Great East Japan Earthquake on the Stock Prices of Non-life Insurance Companies", *The Geneva Papers on Risk and Insurance – Issues and Practice*, 38 (3): 449-468.

[18] Thomann, C. (2013). "The Impact of Catastrophes on Insurer Stock Volatility", *The Journal of Risk and Insurance*, 80 (1): 65-94.

[19] Valizadeh, P., Karali, B., and Ferreira, S. (2017). "Ripple effects of the 2011 Japan earthquake on international stock markets", *Research in International Business and Finance*, 41 (C): 556-576.

[20] Wang, L., and Kutan, A. M. (2013). "The impact of natural disasters on stock markets: Evidence from Japan and the US.", *Comparative Economic Studies*, 55 (4): 672-686.

[21] Worthington, A., and Valadkhani, A. (2004). "Measuring the impact of natural disasters on capital markets: an empirical application using intervention analysis", *Applied Economics*, 36 (19): 2177-2186.

[22] Worthington, A. C., and Valadkhani, A. (2005). "Catastrophic Shocks and Capital Markets: A Comparative Analysis by Disaster and Sector", *Global Economic Review*, 34 (3): 331-344.

[23] Worthington, A. C. (2008). "The impact of natural events and disasters on the Australian stock market: A GARCH-M analysis of storms, floods, cyclones, earthquakes and bushfires", *Global Business and Economics Review*, 10 (1): 1-10.