A GLOBAL COMPARISON OF CORPORATE VALUE ADJUSTMENTS TO NEWS OF CYBER-ATTACKS

Karen M. Hogan *

* Department of Finance, Haub School of Business, St. Joseph's University, the USA
Contact details: St. Joseph's University, 5600 City Avenue, Philadelphia, PA 19131-1395, the USA

How to cite this paper: Hogan, K. M. (2020). A global comparison of corporate value adjustments to news of cyber-attacks. *Journal of Governance & Regulation, 9*(2), 34-44. http://doi.org/10.22495/jgrv9i2art2

ISSN Print: 2220-9352
ISSN Online: 2306-6784

Received: 21.02.2020
Accepted: 08.05.2020

JEL Classification: F2, G1, G14, G32
DOI: 10.22495/jgrv9i2art2

Abstract

The growing threat of cyber breach has become one of the most feared risks corporations around the world are currently dealing with. This paper uses a methodology similar to Hogan, Olson, and Angelina (2020) to analyze global shareholder value effects of cyber breaches from 1990 to 2019 for five major non-US countries. Cumulative Average Returns (CARs) are calculated using the first notice date to periods of up to 90 days post-announcement to compare short-term and long-term effects of cyber breaches on the stock price. Results for this data set show significant negative returns for US corporations in all windows. Unlike its US counterparts, short-term results for non-US countries show no significant changes to price as a result of cyber breach announcements. Long-term results for the aggregate non-US sample show significance only at the (0,30) window. Individual country long-term analysis shows some significance depending on the event windows, but no common patterns are seen among countries. These results point to differences in how news of a cyber breach, by country, is perceived in the market. The results help explain some of the patterns insurance companies have seen in the reticent buying habits of global companies with respect to cyber insurance.

Keywords: Cyber, Breach, Shareholder Value, Global, Insider Information, Insurance, Corporate Strategy, Event Study Analysis

Authors' individual contribution: The Author is responsible for all the contributions to the paper according to CRediT (Contributor Roles Taxonomy) standards.

Declaration of conflicting interests: The Author declares that there is no conflict of interest.

Acknowledgements: The Author would like to thank Advisen Ltd. for providing me with a comprehensive database of cyber data events using both their "Standard Loss Feed Data Set" and access to their "Cyber OverVue" products. The Author would also wish to thank Dylan Vogt for his help with some of the data analysis.

1. INTRODUCTION

According to Eling (2018), although cyber risk, or information security in general, is a classic topic in IT research, relatively few researchers are currently analyzing the topic from a business or an economics perspective. Historically, most of the publically announced cyber data breaches have occurred in North America, but the cyber risk is a growing threat to all companies worldwide regardless of size or country of incorporation. A 2020 study from Allianz Corporation, found that cyber incidents for the first time in history ranked as the number one corporate risk globally with 39% of the 2,700 global risk managers representing over 100 countries in the survey choosing it.[1] The survey highlights the fact that the risk of global cyber incidents has grown

[1] Allianz Global Corporate and Specialty (2020).

exponentially during the past 15 years, along with the dependence on data analytics and IT infrastructure. According to IBM Security (2019) study, the average cost of a data breach in the US increased from $7.91 million in 2018 to $8.19 million in 2019, which is the highest cost globally when compared to other regions. Globally, the average cost of a data breach has increased to $3.92 million.[2]

The main cyber incidents that worry professionals are incidents like IT or cloud outages, data breaches, ransom ware, and business email compromise such as spoofing to name a few. Cyber-attacks can also do major and irrevocable damage to a company's reputation. Equifax saw its own credit rating downgraded in May of 2019 by Moody's. It was the first time that cybersecurity was cited as a reason for an outlook revision. Regulatory and litigation potential are also the result of cyber incidents with record costs for mega breaches such as Equifax's 700 million settlement. Key changes in global regulation with Europe's General Data Protection Regulation (GDPR), the passing of new privacy laws in US states such as California, and privacy changes in Australia, are increasing both the financial and operational stakes for firms doing business globally. These changes apply to firms of all sizes, fields, and geographic locations. As a result, cyber risk is important to all countries regardless of their corporate domicile.

Amir, Lev, and Livne (2018) find US firms that withhold information regarding cyber breaches are subject to a larger decline in the price of their stock than those who disclose the breach more quickly. The evidence is consistent with managers not disclosing negative information below a certain threshold and withholding information on the more severe attacks. Hogan, Olson, and Angelina (2020) document a downward trend in the overall short-term and long-term stock reactions to cyber breaches as compared with earlier studies. While interesting, the authors do not discuss any differences between countries with regard to returns. In addition, they do not look at global industry-related or other characteristics that could point to differences in cyber breach return behaviors for countries outside of the US. Since cyber breaches are not exclusively a US phenomenon, this study looks at disentangling those events to determine differences that might exist between corporate country domains. These differences could point to priorities regarding cyber readiness that may vary from country to country.

If cyber events in foreign countries were causing significant changes to firm value then corporations would try to mitigate that risk. Eling and Wirfs (2019) find that breaches are global phenomena and document that a specialized market for cyber insurance has emerged as one way for companies to mitigate cyber risk on firm value. However, they also note that outside the US, cyber insurance products are little used. Rational risk management policies would only incorporate the cost of insurance if the benefits of coverage outweighed the cost to the firm. The lack of interest or knowledge in cyber insurance outside the US could be due to the lack of shareholder value effects non-US companies experience compared to their US counterparts.

This paper looks to investigate the global shareholder value effects of cyber breaches from the period 1990 to 2019 to elucidate any differences in the short-term and long-term returns between the US and other major countries around the world. Event study methodology using the public first notice date (FN) for all publically traded companies that have experienced a global cyber event with at least 100 affected individuals per event will be analyzed to determine if other countries see the same type of price movements documented for US firms over time. To the author's knowledge, this is the first paper that has analyzed the shareholder effects of cyber breach by country. This research will do a descriptive analysis of country-specific characteristics, which include time, industry, type of data breach, type of data compromised, and the current country breach frequency and severity index to give a detailed picture of the differences that occur by country.

A proprietary data set obtained from Advisen Ltd., the leading insurance data, media, and technology provider for the commercial property and casualty insurance market is used to obtain information on data breaches from 1990 to 2019. The resulting cyber event information for public global corporations trading on US exchanges is merged with historical pricing data as stored in the Center for Research in Security Prices (CRSP) research asset pricing database and then run through event study software, Eventus, to calculate the appropriate cumulative abnormal returns (CARs). The CARs are then analyzed, using various event windows from day -1 up to +90, to determine differences in market reactions to cyber news events between countries.

The results highlight some major differences that exist when comparing cyber events in the US to other major countries around the world. The US still makes up at least 95% of the known breaches, but the risks among other major countries are growing. While the absolute number of reportable yearly events differs significantly between the US and other major non-US countries, the relative distribution of events appears to follow a similar pattern around the world with publicized global cyber events peaking in 2017. An industry breakout by country highlights major industry differences between the US and some non-service dominated countries. Current cyber risk frequency and severity indices show similar results for many of the countries with the exception of Japan, which has significantly higher current frequency and severity results associated mainly within the manufacturing industry. The popular method of breach for all countries tended to focus mainly on external malicious breach. The relative distribution of compromised data source was similar between the US and its major non-US counterparts, with about half the compromised data resulting from server breaches.

Event study analysis highlights major differences that exist with respect to the CARs for

[2] IBM Security (2019).

the short-term and long-term analysis between the US and other global countries. As expected, US short-term and long-term CARs follow similar results seen in other studies that show cumulative negative abnormal returns. However, these results are smaller than seen in some of the original studies and more in line with those seen in more recent studies such as Amir et al. (2018) and Hogan et al. (2020). This reduction in the magnitude of the CAR could possibly highlight the desensitization of the market to cyber-attacks or the result of increased spending by companies related to cyber readiness. Surprisingly, when looking at major non-US cyber events for firms who are also traded on exchanges in the US, the short-term CARs for event windows spanning (-1 to 5) for all countries, regardless of aggregation of the data, do not show any significant cumulative abnormal price changes positive or negative to news of a cyber event, implying, that the market perceives the news of a cyber breach differently depending on the country of the domain.

Analyzing the long-term results with event windows including (-1 to 90 days) between the US and major non-US firms' highlights differences with shareholder effects there as well. Long-term global results show the US reporting significantly monotonic negative CARs of up to – 1.06% for day 90 and other non-US firms showing only significant results at the window (0, 30) of -1.59%. Varied results are reported for the individual smaller samples for each country in the long term, with large variations in CARs between the countries ranging from a significant -14.94% for the (0,90) day window in the Netherlands to a significant overreaction of 3.78% for Japan in the (0,60) event window. However, no country shows the highly significant results in all long-term windows as is seen by the US companies. These results support differing patterns of shareholder value effects in both short-term and long-term event windows to news of a cyber breach for the major non-US corporations than traditionally seen with US companies. Historically, global firms have had less regulation and legal issues related to cyber, which may account for some or all of the differences. Current changes in global cyber regulation in countries outside the US, especially those countries that have industry demographic profiles aligned with the US, may with future research show closer patterns as those currently demonstrated in US firms. This is an area of research for the future.

Additionally, the current lack of short-term shareholder value changes and differing long-term patterns for non-US countries supports the historical lack in current global demand for cyber insurance products for countries outside the US, as observed by Eling and Wirfs (2019) and may point to possible shareholder value pattern changes in the future as those markets develop. This also points to areas of future research.

The remainder of the paper is as follows. Section 2 reviews the relevant literature. Section 3 analyzes the methodology that has been used to conduct empirical research on the cyber breach data and the changes in global stock prices from the announcement date. Section 4 looks at the data results and Section 5 offers some conclusions.

2. LITERATURE REVIEW

As stated previously, Eling (2018) noted that although cyber risk is not a new topic, few researchers are currently analyzing the topic from a business or an economics perspective. Studies on historical stock price changes to cyber breaches have been limited, due to the difficulty with data collection and data reporting methods. Most of the previous studies used hand-collected data with limited sample size or focused on specific types of breaches further limiting sample size. This paper overcomes the low sample size by using a proprietary database of global cyber-attacks that are fact-checked at multiple levels. The scope of the database allows this paper to pull from thousands of events and as a result, the limitation of the number of data points is not an issue. Additionally, the lack of global and US federal standardized reporting requirements has limited true representative events, due to low rates for firm self-reporting. While low self-reporting is a worldwide problem, this research tries to minimize its effect by looking at global firms that trade on the same US exchanges as those US firms in our sample.

Of those papers that specifically looked at firm value, prior research has found either no change or negative change in firm value as the result of a breach (see Campbell, Gordon, Loeb, & Zhou, 2003; Ettredge & Richardson, 2003; Garg, Curtis, & Halper, 2003; Cavusoglu, Mishra, & Raghunathan, 2004; Kannan, Rees, & Sridhar, 2007; Gordon, Loeb, & Sohail, 2010; Gatzlaff & McCullough, 2010; Hilary, Segal, & Zhang, 2016; Sinanaj & Muntermann, 2013; Tanimura & Wehrly, 2015; Amir et al., 2018; Hogan et al., 2020). Also, most prior studies are short-term in nature looking at very short windows around the announcement date or looking for specific forms of breaches such as loss of confidential data, unauthorized malicious breach, or IT data input errors to name a few. This research will look at thousands of data points and cover windows of up to 90 days post announcement. The data will also not be limited to a certain type of cyber breach, thus giving a more representative sample of the market as a whole.

Campbell et al. (2003) examined the stock market reaction to newspaper reports of information security breaches at 38 publically traded US corporations during the period January 1, 1995 to December 31, 2000, which accounted for 43 events. The authors find a highly significant negative market reaction to information security breaches involving unauthorized access to confidential data, but no significant market reaction when the breach does not involve access to confidential data.

Part of the explanation for the small sample sizes in prior studies is not that cyber breaches are a new phenomenon, but instead that companies are reluctant to disclose information for fear that the markets will penalize the company. Hilary et al. (2016) find there is increasing interest in cyber-risk among the general public. However, the disclosure by US listed firms on the topic is rare and boiler-plate. Perhaps as a response to this discrepancy, they argue is the reason the SEC and other regulators historically increased pressure on

registrants. The authors empirically find that the newer regulations did lead to an increase in cyber-risk disclosure but a modest one. Gatzlaff and McCullough (2010) analyze 77 events between 2004 and 2006 involving breached personal information and find a negative reaction between market reaction and firms that are less forthcoming with breach details. Gordon et al. (2010) assess the market value of voluntary disclosures of items pertaining to information security. The authors argue that voluntary disclosures in the annual report filed with the SEC concerning information security allow a corporation to provide signals to the marketplace that the firm is actively engaged in preventing, detecting, and correcting security breaches. This study looked at SEC disclosing and non-disclosing firm years in a cross-sectional pooled model using annualized annual reports filed with the SEC covering the years 2000-2004. The results support the signaling argument that managers will disclose information in a manner with increased firm value.

Amir et al. (2018) also look at when information is disclosed to the public. The authors combined two data sources that report daily cyber-attacks to examine data on cyber-attacks from 2010 to 2015. The authors claim that their data suggests that many disclosures on attacks are made after investors discover them. In cases where firms immediately disclosed the cyber-attack, their equity values declined by .33%, on average, in the three days after disclosure and by .72% in the month after disclosure. In comparison, the authors find that the decline in market values was much larger in cases where firms did not disclose the attack and parties outside the firm later discovered it. Their results show a decline in price of 1.47% for three days after discovery and 3.56% in the month afterward. The authors suggest that firms withhold more severe cyber-attacks from investors even though SEC guidelines say that firms must disclose cyber-attacks that materially damage their business. Using market reactions to withheld and disclosed attacks, the authors estimate that managers disclose information on cyber-attacks when investors already suspect a high likelihood (40%) of an attack.

Much in the firm cyber news the past two years has been discussing attacks, which result in a distributed denial of service (DDOS), such as Wannacry and NotPetya. DDOS breaches that deny access to a firm's own computers and servers, usually until a ransom is paid in bitcoin or some other form of cryptocurrency. Ettredge and Richardson (2003) evaluated the stock market reactions to DDOS attacks against well-known Internet firms in Feb 2000. Their research results showed that investors used heuristics in choosing similar firms to those who were attacked and transferred the negative return to those firms as well, even though they were not attacked. Gordon et al. (2010) determined that attacks associated with breaches of availability are seen to have the greatest negative effect on firm value. Cavusolglu et al. (2004) find breach costs are higher for internet firms, but costs are not related to breach type.

Sinanaj and Muntermann (2013) did one of the few studies to acknowledge the corporate domain. They conducted an event study on newly published data breaches to determine the value of reputational effects associated with the breach. The authors evaluated 72 data breach events for various international firms in a variety of industries between 2004 and 2011. Countries represented included firms from the US, Great Britain, Russia, Japan, China, and Germany. According to their data, the authors confirm that the firms experience significant reputational damage attributable to the announcement of the data breach incidents. Tanimura and Wehrly (2015) investigate the reputational market value effects of incidents in which confidential information for a firm's employees and its customers is disclosed. Overall, firms that experience personal information data breaches will experience a significant loss in the market value of the firm's equity, but it is a result of direct costs and not reputational penalties. Unlike this current research, the samples used in these prior studies were small and there was no common market for any of the firms. With thousands of data points and all firms trading on US exchanges, many of the previous limitations have been eliminated.

Hogan et al. (2020), overcome the sample size issue inherent in many of the previous studies, but stops short at extending any results to global firms. This research will fill that void and analyze any differences that may exist up to this point in both short and long-term shareholder value changes to news of cyber breaches. I will also look at detailed cyber related characteristics and how they differ between countries and give ideas of areas where countries may want to expand their cyber corporate risk management practices.

3. RESEARCH METHODOLOGY

Cyber breach data was collected using first notice date from 1990 to 2019 from Advisen Ltd's Standard Loss Feed Data for all global cyber events. First notice date is the public first notification of the event regarding the breach. Data for cyber breaches by country with at least 100 affected individuals per event was organized along with the company GVkey and IID out of the Standard Loss Data Feel Data. Each event is a unique company cyber breach. If the company breach did not affect at least 100 people that event was not included in the dataset for evaluation so that only events that could actually have an effect on the stock price would be used. For example, if Company A was breached and 10,000 individuals records were affected then that one breach would count as one event in the sample. On the other hand, if Company B was affected and only 10 individuals records were affected that cyber breach then that breach would not be included as part of the data set used in this research.

Once the data was collected from Advisen, the GVkey and IID were then converted to Permnos for use in the Center for Research in Security Pricing database (CRSP). The resulting sample of unique cyber events for each country prior to the event study analysis are as follows: US = 3600, Netherlands = 29, Great Britain = 32, France = 28, Canada = 37, and Japan = 36.

The statistical program Eventus was then used to perform standard event study analysis as described by Brown and Warner (1985) to measure the effect of announcements of cyber events on the returns earned by shareholders. This study used first notice date (FN) to calculate Cumulative Abnormal Returns (CARs). Any non-trading day was converted to the next trading day. The estimation period ends 30 days before the event date and is 180 days in length. The US events started at 3,600 cyber breaches including all data necessary to do the event study. Of those 3,600 events 686 unique company cyber events were dropped by Eventus (681 were outside the period available and 5 observations had too few estimation period days) for a resulting US sample size of 2914. The Netherlands original sample of 29 events that met all the criteria for the current event study was reduced by two in running the event study as 2 events had data outside of the period available. Great Britain started with 32 merged security events and 5 events outside the period available were lost. France had 28 merged events and lost 4 due to dates that were outside of the period that was available. Canada started with 37 merged event data and lost 2 events (1 due to event outside of period that was available and 1 due to not enough days for and estimation period). Japan started with 36 events of which 28 were usable (8 events were outside of the period available).

The market model is used to determine the parameter estimates for expected returns.

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \varepsilon_{i,t} \quad (1)$$

where,

$R_{i,t}$ = the rate of return on security *i* for period *t*;

$R_{m,t}$ = the rate of return on the equally weighted CRSP index;

β_i = the slope of the regression line for security *i*;

α_i = the intercept for security *i*;

$\varepsilon_{i,t}$ = the residual for security *i* for period *t*.

The abnormal return for security *i* on day *t*, $AR_{i,t}$, is defined as the difference in the actual return for security *i* for period *t* less the expected return for security *i* for period *t*:

$$AR_{i,t} = R_{i,t} - [\alpha_i + \beta_i R_{m,t}] \quad (2)$$

The estimated market model parameters, α_i and β_i, are obtained by using the pre-estimation, *t* = -30 with a maximum estimation window of 180 days. Cumulative Abnormal Returns (CARs) are computed by adding the daily average abnormal returns for various event windows using an equal weighting scheme.

$$CAR_{w1w2} = \sum_{w1}^{w2} AAR_{w1} \quad (3)$$

where,

AAR_{w1} = Average abnormal return for all securities on day w_1.

CAR_{w1w2} = Cumulative Abnormal Return for period w_1 to w_2 .

The short-term event windows w_1 includes day 0 and day -1 to allow for possible information leakage and the event window w_2, includes day 1, day 3 and day 5. Long-term windows include w_1 includes day 0 and day -1 and window w_2, includes day 30, day 60 and day 90. Any non-trading date has been converted to the next trading date. The short-term results are calculated using traditional event study analysis with a Patell Z adjustment as is standard to help correct with the fact that the event window abnormal returns are out of sample predictions.

Since most long-term investors don't sell and reinvest every day, long-term calculations are computed with a buy and hold calculation to mimic the more realistic behavior of long-term investors. The buy and hold abnormal returns (BHAR) is defined as the difference between the realized buy and hold return and the expected buy and hold return over the same time period. The buy and hold return of the asset uses geometric compounding. The average buy and hold abnormal return is calculated using an equally weighted portfolio. I limit the number of days for the buy and hold calculations to 90 trading days as long run returns tend to be sensitive to the model and test statistics that are used.[3] The test statistics used is the Patell Z (for the same reasons above) and these results are adjusted using the bootstrap method to adjust for cross-correlation and skewness bias as is common in long-term event studies.[4]

4. DATA AND RESULTS

Table 1 shows the annual distribution of cyber breaches by the country for each year. The results support the market knowledge that historically the majority of all cyber breaches have occurred in North America, with about 95% of them occurring in the US alone. The annual patterns between the US and the rest of the world do support increases in frequency over time regardless of country origin. Both markets show a peak for cyber activity in 2017, which coincides with increasing awareness of the need for cyber risk management as part of the corporate enterprise risk management equation. These results are in line with historical buying habits of global cyber policies with fewer policies written in the global markets. According to experts in the field, this could be a result of the historical lack of regulation regarding privacy in the global markets. With the recent addition of GDPR in Europe and similar regulations in Australia, there has been an increase in activity for these types of products and a growing awareness of the extended negative financial ramifications that can result from cyber breaches.[5]

[3] See Fama (1998) for a discussion on the differences between CARs and BHARs.
[4] See Kramer (2001) discusses the bootstrap method in event studies.
[5] See Morkroft (2019).

Table 1. Break out of US breach activity compared to the rest of the world

Year	*USA Cyber Events*	*% to Total*	*Major Non-US Cyber Events*	*% to Total*
1990s	5	0.14%	0	0.00%
2000	2	0.06%	1	0.62%
2001	3	0.08%	0	0.00%
2002	5	0.14%	0	0.00%
2003	15	0.42%	0	0.00%
2004	5	0.14%	0	0.00%
2005	25	0.69%	0	0.00%
2006	84	2.33%	2	1.23%
2007	94	2.61%	3	1.85%
2008	124	3.44%	7	4.32%
2009	101	2.81%	6	3.70%
2010	97	2.69%	4	2.47%
2011	146	4.06%	6	3.70%
2012	173	4.81%	10	6.17%
2013	287	7.97%	6	3.70%
2014	391	10.86%	27	16.67%
2015	541	15.03%	15	9.26%
2016	595	16.53%	27	16.67%
2017	644	17.89%	33	20.37%
2018	239	6.64%	14	8.64%
2019	24	0.67%	1	0.62%
Total	*3600*	*100.00%*	*162*	*100.00%*

Note: Data collected from Advisen Ltd's Standard Loss Feed Data for all Cyber Category events from 1990 to 2019 by country with more than 99 affected individuals per event and verifiable Permno matches using GVkey and IID. Thus, an event below is defined as a unique cyber breach for a publically traded company with at least 100 affected individuals in each event. Major non-US includes (Canada, Netherlands, Great Britain, Japan, and France). Only countries with more than 28 events including all data variables were used.

Table 2 highlights the compromised data source that was the cause of the cyber breach by US and non-US companies. Similar patterns between all countries in or outside the US show that about 50 to 60% of all breaches are the result of a compromised server. This finding highlights the need for companies of all countries to continue to invest in IT third party services and upgraded networks and firewalls. As important, are more basic services such as employee training to minimize chances of lower-level attempts such as phishing emails, etc. that are often used by bad actors to gain entry into the system with the use of an authentic username and password. A larger percentage of breaches in major non-US countries are the result of website weaknesses than in the US (27.16% vs 11.33%), respectively, perhaps, drawing attention to the possible need of some foreign countries to increase spending on IT cyber corporate digital infrastructure. None of the breaches to the non-US companies was the result of phone or fax communications, while it accounted for over 8% of those in the US. This could be a function of US firms having almost all the publicized cyber breaches prior to 2006 when telephone communication was a more common means of communication than email etc. Of note though, is the more recent attempts of hackers to use phone services for cyber breaches called "deep throat breaches", which happens when voice recognition AI software is used to impersonate the voice of a senior member of the company to trick a staff member with financial authorization to wire money to bogus bank accounts. It is important for firms in all countries to alert their employees of such events and how realistic the bad actors can sound.

Table 2. Source of compromised data

Compromised Data or Access Source Primary	*USA Events*	*% to Total*	*Major Non-US Events*	*% to Total*
Automatic Teller Machine (ATM)	9	0.25%	0	0.00%
CD-ROM	9	0.25%	2	1.23%
Desktop	38	1.06%	1	0.62%
Email	181	5.03%	4	2.47%
Hard Drive (portable)	36	1.00%	3	1.85%
Laptop	214	5.94%	3	1.85%
Other	13	0.36%	0	0.00%
Point of Sale (POS)	70	1.94%	1	0.62%
Printed Records	133	3.69%	3	1.85%
Privacy Laws/Act Violation (State or Federal)	109	3.03%	0	0.00%
Server	1913	53.14%	94	58.02%
Smartphone, Tablet	19	0.53%	1	0.62%
Social Media	37	1.03%	1	0.62%
Software	41	1.14%	2	1.23%
Tape	36	1.00%	1	0.62%
Telephone Communication or Fax Transmissions	307	8.53%	0	0.00%
Thumb Drive	14	0.39%	2	1.23%
Website	408	11.33%	44	27.16%
Unknown	13	0.36%	0	0.00%
Total	*3600*	*100.00%*	*162*	*100.00%*

Note: Data collected from Advisen Ltd's Standard Loss Feed Data for all Cyber Category cases from 1990 to 2019 by country with more than 99 affected individuals per event and verifiable Permno matches using GVkey and IID. Major non-US includes (Canada, Netherlands, Great Britain, Japan, and France). In order to minimize small sample issue, only countries with more than 28 cases including all data variables were used.

Table 3 analyzes the industry breakout of cyber breaches by country and looks at the current frequency and severity of the industries by country. As expected, the two North American countries follow popular services (SER) and finance, insurance, and real estate (FIR) industries as the highest industries with cyber breaches. This highlights the historically popular target of companies that have personal identifying information, personal financial information, and personal medical information. The Netherlands also has the majority of their breaches in the services industry, while Great Britain reports about half of their breaches are in FIR industries. Network security and regulatory compliance are paramount in these countries in order to minimize not only the number of breaches, but also the regulatory fines that could be levied on firms for not keeping customer's data safe. France and Japan show different cyber breach patterns with the majority of Japanese breaches (86.11%) coming from manufacturing (MAN) industries and France's from Transportation, Communication and Utility (TCU) related industries. Companies in these countries need to pay special attention to denial of service attempts and ransom ware Trojans, as these firms tend to be the targets of bad actors, trying to either shut down networks to third party customers or limit output production, in exchange for skyrocketing ransoms. The current frequency and severity scores by industry show that most countries' current frequency and severity of attack scores range between 50 to 60 out of 100. However, Japan ranks highest with a frequency of 76.7 and severity of 70, which shows that the manufacturing industry for this country is at risk for frequent and severe cyber-attacks. This result highlights the growing risk of damage to factories as manufacturing firms have become increasingly reliant on the internet in recent years.

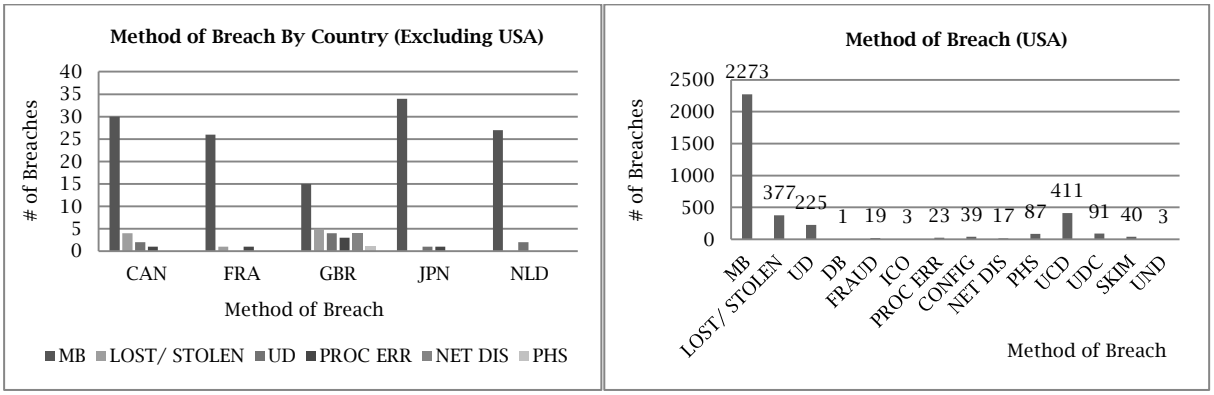
Table 3. Industry breakout of major cyber activity

Country	*MAN*	*TCU*	*RET*	*FIR*	*SER*	*OTH*	*Total*	*FREQ*	*SEV*
Canada	3	3	0	9	21	1	37	56.4	44.2
France	2	24	0	2	0	0	28	60.0	50.1
Great Britain	3	9	0	16	4	0	32	58.8	51.6
Japan	31	1	0	2	2	0	36	76.7	70.7
Netherlands	3	3	0	0	23	0	29	61.6	50.7
United States	377	318	433	591	1801	80	3600	63.5	58.9
Total	*419*	*358*	*433*	*620*	*1851*	*81*	*3762*		

Note: Global analysis of major cyber events by country by SIC. Where MAN = Manufacturing, TCU = Transportation, Communications, Electric, Gas, and Sanitary Service, RET = Retail Trade, FIR = Financial Services, Insurance, and Real Estate, SER = Services, OTH = Other. FREQ = An Advisen LTD. calculated value as of 2019 representing the frequency of cyber events from that country's associated corporate industry events. In general, the analyses seek to compare the loss experience of a company against the average, median, and maximum loss experience of its peer group. SEV = An Advisen LTD. calculated value as of 2019 representing the severity of cyber events from that country's associated corporate industry events. In general, the analyses seek to compare the loss experience of a company against the average, median, and maximum loss experience of its peer group. Both values have a possible score from 1 (least) to 100 (highest) probability.

Figure 1 sheds light on the method of breach by country with 63% of US and 82% of non-US labeled as a malicious breach. The majority of the malicious breaches are external in nature and not committed by those who are directly associated with the company. This country-specific data shows that almost all breaches publicly announced by non-US firms are probably from outside sources. This again highlights the need for firms to have proper training and mitigation services in place to be able to minimize the potential ongoing need to recover from cyber breaches. Consider, for example, a denial of service cyber breach in a Japanese major manufacturing plant. Assume the plant is unable to operate for 2 to 4 weeks. This could lead to third party supply chain issues, as the affected company will lack inventory to sell, possibly, leading to longer term issues for the company as revenue and profits decline, since customers are forced to move to alternative suppliers to address the shortfall in their own supply chains. There is no guarantee that these customers will return once the company recovers, especially if they feel the company was not practicing best practices regarding cyber risk mitigation.

Figure 1. Method of breach by country



Note: The number of public corporation breaches trading on US exchanges during the period 1990 to 2019 with greater than 99 persons affected by the breach; countries with more than 28 breaches or more. Where CAN = Canada, FRA = France, GBR = Great Britain, JPN = Japan, and NLD = Netherlands. The method of breach is MB = Malicious Breach, Lost/Stolen, UD = Unintentional Disclosure, DB = Digital Breach/Identity Theft, FRAUD = Identity – Fraudulent Use/Account Access, ICO = Industrial Controls & Operations, PROC ERR = IT Processing Errors, CONFIG = IT Configuration/Implementation Errors, NET DIS = Network/Website Disruption, PHS = Phishing, Spoofing, Social Engineering, UCD = Unauthorized Contact or Disclosure, UDC = Unauthorized Data Collection, SKIM = Skimming, Physical Tampering, and UND = Undetermined.

Table 4 shows the CARs for the US, aggregate major non-US, and by country for event windows between (-1 to +5) days. The US companies show an increasing negative short-term CAR in each window from day (0 to 1, 3, and 5). When looking from day (t = -1 to 1, 3, and 5) the CARs are slightly more negative for the US firms, which highlights potential information leakage by the bad actors, insiders with company knowledge, or both. The magnitude of the CARs is relatively small ranging from -17 basis points with the window (0,1) to -25 basis points with the window (-1,5). These results support more recent studies such as Amir et al. (2018) and Hogan et al. (2020), highlighting the possible desensitization of the market to cyber-attacks regarding short-term price changes. Investors are bombarded on a daily basis with cyber breach notifications. It is difficult in the short term to distinguish which breach is really going to be a significant loss for the company, as very little information is available at the time of the announcement. Additionally, increases in cyber insurance purchases, coupled with changes in breach habits by bad actors who have moved into ransom ware as a popular method of breach, may have cut down the out of pocket direct and indirect costs to the firm as some of the costs have been transferred to the insurance industry. About 40% of all firms in the US to date have some type of cyber insurance policy, which helps to soften the costs associated with a breach and should eliminate some of the post cyber announcement stock volatility.

Table 4. Short-term global CARs for companies experiencing cyber events (1990-2019)

US				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+1)	2914	-0.17%	-2.688	0.0036
(0,+3)	2914	-0.20%	-1.800	0.0360
(0,+5)	2914	-0.22%	-1.427	0.0768
(-1,+1)	2914	-0.20%	-2.935	0.0017
(-1,+3)	2914	-0.23%	-2.183	0.0145
(-1,+5)	2914	-0.25%	-1.806	0.0355
Major Non-US				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+1)	141	-0.04%	-0.075	0.5030
(0,+3)	141	0.00%	-0.286	0.4090
(0,+5)	141	0.20%	0.305	0.3200
(-1,+1)	141	-0.02%	0.097	0.4130
(-1,+3)	141	0.02%	-0.127	0.4960
(-1,+5)	141	0.22%	0.394	0.2860
Netherlands				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+1)	27	0.14%	0.110	0.4562
(0,+3)	27	0.47%	0.335	0.3689
(0,+5)	27	-0.07%	-0.346	0.3646
(-1,+1)	27	0.16%	0.240	0.4050
(-1,+3)	27	0.49%	0.416	0.3386
(-1,+5)	27	-0.05%	-0.222	0.4122
Great Britain				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+1)	27	0.22%	-0.272	0.3927
(0,+3)	27	0.10%	-0.615	0.2694
(0,+5)	27	0.96%	0.394	0.3466
(-1,+1)	27	0.20%	-0.124	0.4506
(-1,+3)	27	0.08%	-0.474	0.3179
(-1,+5)	27	0.94%	0.429	0.3338
France				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+1)	24	-0.01%	-0.013	0.4949
(0,+3)	24	-0.23%	-0.542	0.2939
(0,+5)	24	-0.14%	-0.327	0.3720
(-1,+1)	24	0.21%	0.434	0.3321
(-1,+3)	24	-0.01%	-0.14	0.4442
(-1,+5)	24	0.08%	-0.011	0.4956
Canada				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+1)	35	0.01%	0.603	0.2732
(0,+3)	35	-0.10%	0.058	0.4768
(0,+5)	35	0.30%	0.584	0.2796
(-1,+1)	35	0.05%	0.474	0.3179
(-1,+3)	35	-0.06%	0.038	0.4850
(-1,+5)	35	0.34%	0.528	0.2987
Japan				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+1)	28	-0.55%	-0.639	0.2613
(0,+3)	28	-0.21%	0.049	0.4860
(0,+5)	28	-0.11%	0.308	0.3792
(-1,+1)	28	-0.70%	-0.774	0.2194
(-1,+3)	28	-0.36%	-0.152	0.4397
(-1,+5)	28	-0.26%	0.120	0.4524

Note: Cumulative Average Returns (CAR) using standard event study methodology with equal weight using the event date of public first notice for cyber events occurring 1990 through April 2019. N = the number of companies who experienced a cyber event with complete cyber event data. Data was collected from Advisen Ltd's Standard Loss Feed Data for all Cyber Category cases by country with unique company cyber events affecting more than 99 individuals per event and verifiable company Permno matches using GVkey and IID. Each unique company event meeting the criteria would be counted as one event in the data set. Each event's Permnos and first notice date were then used in the Center for Research in Stock Prices data base (CRSP) and the event study program Eventus to obtain the calculations of the company of CARs. Some observations were dropped by Eventus due date outside of period available.

The short-term results for the major non-US firms follow a very different pattern. All windows of the aggregated data for non-US companies show no significant CARs for any of the short-term windows analyzed, implying that on average firms outside the US do not see abnormal negative price reactions to the news that the company has been breached. This result is interesting in that these firms also trade on US exchanges and presumably have some of the same investors purchasing them. Some of the differences might be explained by the differences in cyber breach industry break out for countries like Japan and France. These countries don't follow the traditional US services/FIR pattern where heavy cyber activity is commonplace. However, that would not explain the differences for the countries that do have similar industry patterns to the US. These patterns might be better explained by a difference in regulation or legal activity that has existed up to this point in each country. For example, in Europe privacy regulations are just now becoming a major issue that companies and boards have to incorporate into their business strategy. New regulations such as General Data Protection Regulation (GDPR) now exist, which gives the consumer rights to their own personal data and tries to simplify the requirements for international business in the EU. Firms in the EU who handle any private information as of 2018 have had to make changes to incorporate these new rules. Future reactions to news of non-US cyber events may change, as the industry sees the potential fines that could be levied on companies who are in violations of the new regulations.

Table 5. Long-term global CARs for companies experiencing cyber events (1990-2019)

US				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+30)	2914	-0.05%	7.049	<.001
(0,+60)	2914	-0.59%	10.257	<.001
(0,+90)	2914	-1.00%	12.937	<.001
(-1,+30)	2914	-0.09%	6.888	<.001
(-1,+60)	2914	-0.64%	10.159	<.001
(-1,+90)	2914	-1.06%	12.869	<.001
Major Non-US				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+30)	141	-1.59%	-1.590	0.0950
(0,+60)	141	-1.49%	-0.134	0.4580
(0,+90)	141	-2.67%	-0.399	0.3670
(-1,+30)	141	-1.59%	-1.199	0.1340
(-1,+60)	141	-1.51%	-0.052	0.4860
(-1,+90)	141	-2.68%	-0.325	0.4000
Netherlands				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+30)	27	-4.19%	-0.777	0.2020
(0,+60)	27	-10.68%	-1.936	0.0090
(0,+90)	27	-14.94%	-1.399	0.0170
(-1,+30)	27	-4.16%	-0.673	0.2140
(-1,+60)	27	-10.73%	-1.880	0.0080
(-1,+90)	27	-14.94%	-1.354	0.0180
Great Britain				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+30)	27	-0.49%	-1.071	0.1930
(0,+60)	27	-1.29%	-1.815	0.0310
(0,+90)	27	-4.46%	-2.791	0.0010
(-1,+30)	27	0.65%	-1.034	0.2030
(-1,+60)	27	-1.41%	-1.758	0.0450
(-1,+90)	27	-4.56%	-2.743	0.0010
France				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+30)	24	-1.24%	-1.05	0.0750
(0,+60)	24	-1.01%	-0.124	0.4740
(0,+90)	24	-2.29%	-0.783	0.1240
(-1,+30)	24	-1.06%	-0.878	0.1020
(-1,+60)	24	-0.82%	-0.011	0.5360
(-1,+90)	24	-2.08%	-0.681	0.1500
Canada				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+30)	35	-0.55%	0.771	0.1370
(0,+60)	35	0.91%	1.697	0.0580
(0,+90)	35	1.77%	2.112	0.0290
(-1,+30)	35	-0.49%	0.827	0.1240
(-1,+60)	35	0.97%	1.736	0.0500
(-1,+90)	35	1.82%	2.145	0.0270
Japan				
Event Window	***N***	***CAR***	***Patell Z***	***p-value***
(0,+30)	28	-1.72%	-1.115	0.1570
(0,+60)	28	3.78%	1.601	0.0650
(0,+90)	28	5.03%	1.594	0.1110
(-1,+30)	28	-1.86%	-1.159	0.1410
(-1,+60)	28	3.60%	1.527	0.0760
(-1,+90)	28	4.88%	1.547	0.1120

Note: Cumulative Average Returns (CAR) using standard event study methodology with equal weight using the event date of public first notice for cyber events occurring 1990 through April 2019. N = the number of companies who experienced a cyber event with complete cyber event data. Data was collected from Advisen Ltd's Standard Loss Feed Data for all Cyber Category cases by country with unique company cyber events affecting more than 99 individuals per event and verifiable company Permno matches using GVkey and IID. Each unique company event meeting the criteria would be counted as one event in the data set. Each event's Permnos and first notice date were then used in the Center for Research in Stock Prices data base (CRSP) and the event study program Eventus to obtain the calculations of the company of CARs. Long-term results Z-scores were adjusted using the boot strap method. P-values are based on a 1-tail nonparametric bootstrap of the indicated test.

Taking a closer look at each country, I find that even when looking at each country individually there are no significant short-term CARs associated with any country in the major non-US group. These results follow could explain the global pattern that has been seen historically for cyber insurance purchases with companies in countries outside the US being slow to jump on the cyber insurance train. With no large changes in value to the firm, there is no real need to mitigate a risk that does not appear to be there.

While it is easy to understand how short-term results in general would be small, longer term results should benefit from the associated time lag, as more information should be available regarding the extent of the breach and its financial ramifications on the firm. Table 5 breaks out longer term results for CARs in aggregate and by country when compared to that of the US. The results were done using a more realistic buy and hold strategy with results adjusted for bootstrapping. Similar to the short-term results, the US CARs for windows up to 90 days from the first notice continue to show highly significantly small negative results in each window with a maximum shareholder value change of -1.06 percent associated with the event window (-1, +90). Long-term results for non-US firms show significance only at the window (0, +30) days of -1.59%. All other windows including the (-1, 30) window were not significant. Again, it shows that aggregate non-US firms are not penalized with decreases in shareholder value in most cases for cyber breaches. A more detailed breakout of each country does show that, depending on the country, there are some significant long-term windows. For example, Netherland shows the highest significant CAR for the window (-1,90) of -14.94%. Most of the companies who have experienced cyber breaches in the Netherlands are in the services industry, an industry, which usually carries a high amount of personal and credit information. This result shows the potential for cyber breaches to be devastating to a firm's financial health globally. Additionally, countries like Great Britain who also have a high percentage of financial services firms, where private information is at a premium, show multiple windows at (60 and 90) days where shareholder value is negatively affected by information related to a cyber breach. Firms in these countries should consider evaluating their current IT expenditures, employee education, insurance, and other cyber mitigation techniques to insure that cyber influence on stock price kept to a minimum. While the small sample sizes for many of the non-US countries would make it difficult to extrapolate results across firms in each country, companies in these countries should be on a heightened awareness to changes in regulatory actions that might shift these return patterns negatively.

5. CONCLUSION

The instances of global cyber breaches have been increasing steadily over the past 15 years. Cyber risk has for the first time been named as the number one risk that companies worldwide are concerned with. This paper compares the characteristics and shareholder value effects of news of a cyber breach between the US and five major non-US countries. The results highlight some commonalities and differences between the US and other major countries globally with regard to cyber breach characteristics. Similar to recent studies by Amir et al. (2018) and Hogan et al. (2020), highly significant small short-term and long-term negative shareholder effects to US only firms as an aggregate are found. These returns to US firms occur regardless of event windows length. The results imply that while investors do equate the uncertainty of the impact of a cyber breach as a negative event, the magnitude of results appear to be much smaller than returns found in earlier studies when sample sizes were very small, mitigation techniques less developed, and regulations were more lax, implying, that education, regulation, and the development of a more mature cyber insurance market may have played a role in this reduction of shareholder volatility for US firms in recent years.

However, given the plethora of mitigation techniques, the result that cyber breaches are still causing negative stock price changes highlights the need for firms to continue to find additional ways of managing the risk that cyber has added to the corporate financial management process. While most breaches in the US occur in either the services or financial services industry, recent increases in denial of service and ransom ware have heightened the need for all industries in the US to become cyber savvy regardless of their size or scope. For example, low tech improvements such as employee training may need to play a larger role than was previously thought to mitigate the chance of email scams and phishing attempts from sabotaging the excellent high tech IT infrastructure that companies may have invested in.

Looking at non-US price reactions to information of cyber events, we see that the historical short-term returns to news of cyber events in major non-US companies, who also trade on the US exchanges, are not significantly different from zero. It is unknown if these differences are the result of less regulation or litigation (board or otherwise) abroad, differences in IT expenditures, differences in perceived wealth of the victims leading to differences in perceived value of lost information in non-US companies, differences in industry patterns requiring different personal and private information storage, or lack of awareness of investors that cyber risks could cause to firms. However, given that the non-US companies are trading on the same exchanges as US firms the last option is the least likely of those posited, as many firms would have similar investors to US firms.

Long-term results for all non-US firms show slightly significant negative returns of about -1.59% at only the (0, 30) day event window. Those returns revert to no significance by day 60, implying that even in the long run it appears cyber risk has not been a historical driver of change to shareholder value for companies outside of the US. However, given the recent regulation of GDPR to European firms, including the potential of a 4% of global revenue fine, it would be premature to believe that these trends of no significance will continue into the future. In fact, when looking at individual country data there do appear to be country-specific firm effects that may be related to the country's specific regulatory, legal, or industry characteristics that are

the result of the variations in returns. Countries like Netherland show that it is possible to have significant negative returns of up to -14% or more by day 90.

Countries that are in industries that handle traditional personal, private, or medical information would most likely be liable for adhering to the increased regulations that those industries are bound to include. These companies need to invest in IT cyber mitigation, as well as, working with third part firms to set up mitigation strategies such as employee training, identifying shortfalls in current cyber policies as bad actors expand their tool box, and incorporating more risk transfer products such as cyber insurance.

As I noted in the introduction, Eling and Wirfs (2019) find that breaches are global phenomena and document that a specialized market for cyber insurance has emerged as one way for the companies to mitigate cyber risk on firm value. They also noted that outside the US, cyber insurance products are little used. Perhaps as was shown by the increased awareness documented on the previously mentioned 2020 Allianz Corporation survey, that global services managers now highlight cyber as the number one corporate risk for this year, this may change. The market for cyber insurance as a mitigation tool might easily catch up to those rates of incorporation found in the US. Given these advances, future changes in shareholder value to news of cyber breaches may come closer to patterns seen in the US, but differences in regulatory and legal standards even within industries, depending on the customer data footprint of the firm, could continue to make return patterns to news of cyber events differ than those seen in the US. Only time and future research will answer this question.

REFERENCES

1. Allianz Global Corporate and Specialty. (2020). *Allianz Risk Barometer: Identifying the major business risks for 2020.* Retrieved from https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf
2. Amir, E., Lev, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies, 23*, 1177-1206. https://doi.org/10.1007/s11142-018-9452-4
3. Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance – Issues and Practice, 40,* 131-158. https://doi.org/10.1057/gpp.2014.19
4. Brown, S. J., & Warner, J. B. (1985). Using daily stock returns (the case of event studies). *Journal of Financial Economics, 14*(1), 3-31. https://doi.org/10.1016/0304-405X(85)90042-X
5. Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448. https://doi.org/10.3233/JCS-2003-11308
6. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 69-104. https://doi.org/10.1080/10864415.2004.11044320
7. Eling, M. (2018). Cyber risk and cyber risk insurance: Status quo and future research. *The Geneva Papers on Risk and Insurance – Issues and Practice, 43*(2), 175-179. https://doi.org/10.1057/s41288-018-0083-6
8. Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research, 272*(3), 1109-1119. https://doi.org/10.1016/j.ejor.2018.07.021
9. Ettredge, M. L., & Richardson, V. J. (2003). Information transfer among internet firms: The case of hacker attacks. *Journal of Information Systems, 17*(2), 71-82. https://doi.org/10.2308/jis.2003.17.2.71
10. Fama, E. F. (1998). Market efficiency, long-term returns, and behavioral finance. *Journal of Financial Economics, 49*(3), 283-306. https://doi.org/10.1016/S0304-405X(98)00026-9
11. Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management and Computer Security Treatment, 11*(2), 74-83. https://doi.org/10.1108/09685220310468646
12. Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review, 13*(1), 61-83. https://doi.org/10.1111/j.1540-6296.2010.01178.x
13. Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly, 34*(3), 567-594. https://doi.org/10.2307/25750692
14. Hilary, G., Segal, B., & Zhang, M. H. (2016). *Cyber-risk disclosure: Who cares?* (Georgetown McDonough School of Business Research Paper No. 2852519). Retrieved from https://ssrn.com/abstract=2852519
15. Hogan, K. M., Olson, G. T., & Angelina, M. (2020). *A comprehensive analysis of cyber data breaches and their resulting effects on shareholder wealth* (Working paper). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589701
16. IBM Security. (2019). IBM: Cost of a data breach report 2019. *Computer Fraud & Security, 2019*(8), 4. https://doi.org/10.1016/S1361-3723(19)30081-8
17. Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce, 12*(1), 69-91. https://doi.org/10.2753/JEC1086-4415120103
18. Kramer, L. A. (2001). Alternative analysis for robust analysis in event study applications. *Advances in Investment Analysis and Portfolio Management, 8,* 109-132. https://doi.org/10.2139/ssrn.278109
19. Morkroft, B. (2019, February 6). The evolution of cyber insurance – Where are we now? *Insurance Business America.* Retrieved from https://www.insurancebusinessmag.com/us/news/cyber/the-evolution-of-cyber-insurance--where-are-we-now-124183.aspx
20. Sinanaj, G., & Muntermann, J. (2013). Assessing corporate reputational damage of data breaches: An empirical analysis. *BLED 2013 Proceedings.* Retrieved from https://aisel.aisnet.org/bled2013/29
21. Tanimura, J. K., & Wehrly, E. W. (2015). The market value and reputational effects from lost confidential information. *International Journal of Financial Management, 5*(4), 18-35. https://doi.org/10.21863/ijfm/2015.5.4.020